



Univerzitet Singidunum
Departman za poslediplomske studije i međunarodnu saradnju

Napredni sistemi zaštite
Doktorske studije

**Predlog modela zaštite poslovno informacionog
sistema apotekarskih ustanova – studija slučaja**
Apoteka Vranje

- doktorska disertacija -

Mentor:
prof. dr Milan Milosavljević

Student:
Irena Tasić, master

Beograd, 2014. godina

KATALOGIZACIJA

Komisija :

1. Prof. dr. Gojko Grubor, predsednik
2. Prof. dr. Boško Nikolić, član
3. Prof. dr. Milan Milosavljević, mentor i član

ZAHVALNICA

Koristim ovu priliku da se zahvalim mentoru prof. dr. Milanu Milosavljeviću na neizmernoj podršci koju mi je pružio u realizaciji ovog rada.

Takođe izražavam i svoju zahvalnost doc. dr. Gojku Gruboru koji mi je svojim savetima i pomoći omogućio da rad bude realizovan u formi kakav je sada.

Zahvaljujem se neizmerno svojoj porodici, suprugu Srđanu i sinovima Nemanji i Vukašinu koji su topline doma podržavali moj rad na ovom velikom projektu.

KRATAK SADRŽAJ

Ovaj rad ima cilj da otvori put istraživanjima upravljanja rizicima informacionih sistema (i ne samo njih) u sasvim novim i neistraženim domenima. Dokazi i metode u ovom radu prvi put su primenjeni, u ovakvom obliku, na složenom poslovno-informacionom sistemu ZU Apoteka Vranje i predstavljaju mogućnost ulaska u sasvim nove oblasti gde je neophodno da se rizici kompletno kontrolišu. Osim toga rad je kao cilj postavio potragu za nizom postojećih relacija i zakonitosti koji se dodatno dokazuju samom činjenicom da je poslovno-informacioni sistem dovoljno složen i da pokriva teritoriju celog Pčinjskog regiona.

Inače, procesi zaštite integrišu procedure, ljude i alate, motivisane za izvršavanje prakse zaštite i predstavljaju temelje za izgradnju sistema zaštite. Proces zaštite treba neprekidno poboljšavati, zbog generalno slabo razvijene svesti vlasnika, menadžera i korisnika o potrebi zaštite i relativno skupih tehnologija i stručnjaka zaštite.

Ključne reči: informacioni sistem, bezbednost podataka, rizici, upravljanje rizicima

ABSTRACT

This aim of this paper is to enable research in the area of risk management of information systems (and similar systems) within new domains yet to be investigated. The presented evidence and methods were used in this form for the first time in the complex business and information system of the health institution "Apoteka Vranje" illustrating thus the possibility of investigating new areas where risk must be fully controlled. Moreover, the research is aimed at identifying existing relations and rules substantiated by the mere fact that this business and information system is already complex and that it covers the entire Pcinja District region.

In general, protection processes integrate procedures, tools and human facilitators motivated to endorse protection measures and as such are the basis of a protection system. The protection process should be upgraded continuously because of a generally low level of awareness among owners, managers and users regarding the need for protection and relatively expensive protection technologies and professionals.

Keywords: information system, Data security, risk, risk management

INDEKS SLIKA I GRAFIČKIH PRIKAZA

Slika 2.1.	Lokacija SSL protokola u višeslojnoj arhitekturi računarske mreže	8
Slika 2.2.	Tipičan skener za procenu ranjivosti RS – (a) i implementacija u RM – (b)	11
Slika 2.3.	Pingovanje računara u mreži	11
Slika 2.4.	Skeneri ranjivosti računarskih mreža	12
Slika 2.5.	Linearna aproksimacija rasta ranjivosti od 2000-2006	12
Slika 2.6.	Mogućnosti primene NIDPS sistema u računarskoj mreži	17
Slika 2.7.	Fizička i logička distribucija bezbednosnih servisa	38
Slika 2.8.	Arhitektura LSA	42
Slika 2.9.	Proces EFS šifrovanja datoteke	46
Slika 2.10.	Proces dešifrovanja EFS datoteke	46
Slika 2.11.	Arhitektura EFS-a	47
Slika 2.12.	Sadržaj šifrovanog objekta sistema datoteka	48
Slika 2.13.	Osnovni prozor <i>Infigo FTPStress</i> Fuzzer alata	53
Slika 2.14.	Izgled stranice web sajta ZU Apoteka Vranje	56
Slika 2.15.	Logovanje na Web server Telekoma Srbija	57
Slika 2.16.	Opšti statistički podaci	58
Slika 2.17.	Domeni složeni u stablo, podeljeni u zone, svaki opslužuje <i>nameserver</i>	60
Slika 2.18.	Slojevi (i protokoli) za čitač Weba koji koristi SSL	64
Slika 2.19.	Računari u oblaku	72
Slika 2.20.	Šta je <i>Cloud Computing</i> ?	72
Slika 2.21.	Taksonometrija <i>Cloud Computing</i> -a	73
Slika 2.22.	Kako radi <i>Cloud Computing</i>	74
Slika 2.23.	Izgled software-a iStor	77
Slika 2.24.	Trag rukovanja podacima	78
Slika 2.25.	Povezivanje računarskih resursa između apoteka i centralne lokacije u Upravi Apoteke Vranje	81
Slika 2.26.	<i>Local Security Settings</i>	82
Slika 2.27.	<i>Local Security Settings</i>	82
Slika 2.28.	Prikaz korisnika na sistemu	82
Slika 2.29.	Administratorski nalog	84
Slika 2.30.	<i>Backup Operators</i> nalog	84
Slika 2.31.	<i>Local Service</i> nalog	84
Slika 2.32.	<i>Local Users and Groups</i>	85
Slika 2.33.	Grupe korisnika	86
Slika 2.34.	Podešavanja prava korisnika	86
Slika 2.35.	<i>Console Root</i>	87
Slika 2.36.	<i>Console Root 2</i>	87
Slika 2.37.	<i>Console Root – Group Policy</i>	88
Slika 2.38.	Prava pristupa u <i>Hubie</i> -u	90
Slika 2.39.	Pravo pristupa – grupe u <i>Hubie</i> -u	91
Slika 2.40.	Korisnici prijavljenu u <i>Hubie</i> -u	91
Slika 2.41.	Potpuna ovlašćenja	91
Slika 2.42.	Ovlašćenja pravne službe	92
Slika 2.43.	Ovlašćenja radnika službe finansija	92
Slika 2.44.	Ovlašćenja operatera u ograncima	92
Slika 2.45.	Mreža zasnovana na IDPS senzorima: inline raspoređivanje	97
Slika 2.46.	Mreža zasnovana na IDPS senzorima: pasivno raspoređivanje	97
Slika 2.47.	Razmeštanje bežični zasnovanih IDPS senzora	98
Slika 2.48.	NBA IDPS raspoređivanje	98
Slika 2.49.	<i>Host-based</i> IDPS raspoređivanje	99

Slika 2.50.	Praćenje i izveštavanje u realnom vremenu	100
Slika 2.51.	Integrisana topologija	102
Slika 2.52.	Namenska topologija	102
Slika 3.1.	Dijagram toka procesa ocene bezbednosnih rizika	114
Slika 4.1.	Izvod iz zapisnika Upravnog odbora ZU Apoteka Vranje	128

INDEKS TABELA

Tabela 2.1.	Kriptografski algoritmi za komunikaciju sa SSL protokolom	9
Tabela 2.2.	Uobičajeni izvori predznaka incidenta i indikacije	24
Tabela 2.3.	Podsetnik za inicijalna rukovanja incidentom	28
Tabela 2.4.	Kategorije incidenta	29
Tabela 2.5.	Česti TLD-ovi i njihovo značenje	61
Tabela 2.6.	Informacije o radu i kapacitetu saobraćaja Cisco modula detekcije anomalija	100
Tabela 2.7.	Osobine Cisco modula detkcije anomalija	101
Tabela 2.8.	IIS direktorijumske dozvole	104
Tabela 2.9.	Aplikaciona ovlašćenja Execute	105

SKRAĆENICE KORIŠĆENE U RADU

3DES	Triple Data Encryption Standard
ACE	Access Control Entries
ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
A&A	Autentifikacioni i autorizacioni serveri
API	Application programming interface
ASP	Active Server Pages
BCM	Business Continuity Management
BCP	Business Continuity Plan
BGP	Granični gateway protokol
BIA	Business Impact Analiza
BP	Basic Practices
BPM	Business Process Mapping
CA	Certification Authority
CBAC	Context - based access control
CC	Cloud Computing
CERT	Computer emergency response team
CIA	Confidential Integrity Availability
CIRT	Computer Incident Response Team
CIS	Card issuing system
CL2/CL3	Capability Levels
CRL	Certificate Revocation List
CSP	Cryptographic Service Providers
DAC	Discretionary Access Control
DDF	Data Decryption Field
DDoS	Distribuirani Denial of Service
DIR	Certificate directory
DMZ	Demilitarized Zone
DNS	Domain name system
DoS	Denial of Service
DPAPI	Data Protection API
DRF	Data Recovery Field
DRP	Disaster Recovery Plan
DS	Digitalni sertifikat
EAM	Extranet Access Management
eDMS	Electronic Document Management System
EFS	Encrypting File System
ERP	Enterprise Resource Planning
ESS	E - Smart Systems
FedCIRT	Federal Computer Incident Response Team
FIPS	Federal Information Processing Standards
FSRTL	File System Run - Time Library
FTP	File transfer protocol

GAISP	Generally Accepted Information Security Principles
GP	Generic Practices
GUI	Graphic User Interface
HIDPS	Host - based Intrusion Detection and Prevention
HIDS	Host IDS
HIPAA	Zakon zdravstvenog osiguranja o prenosivosti i odgovornosti
HSM	Hardware Security / Storage Module
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
IaaS	infrastructure-as-a-service
ICMP	Internet Control Message Protocol
ICT	Information and communications technology
IDPS	Intrusion Detection and Prevention Systems
IDS	Intrusion Detection Systems
IPS	Intrusion prevention systems
IETF	Internet Engineering Task Force
IIS	Internet Information Services
IKT	Informaciono - komunikacione tehnologije
IP	Internet Protocol
IPS	Intrusion Prevention Systems
ISS	Internet Security Systems
IT	Information technology
KA	Master key
KDC	Key Distribution Center
KEMZ	Kompromitujuće elektro magnetno zračenje
LAN	Local area network
LBAC	Label - based access control
LDAP	Lightweight Directory Access Protocol
LKG/CKG	Local / central key generator
LM	LAN manager
LSA	Local Security Authority
MAC	Mandatory Access Control
NAC	Network Access Control
NAS	Network Access Server
NBA	Sistem analiza ponašanja mreža
NIDPS	Network Intrusion Detection And Protection System
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
NNTP	Network News Transfer Protocol
NOSSS	Native Operative System Security Subsystem
NTFS	New Technology File System
NTLM	NT LAN Manager
OP	Oblast procesa
OS	Operativni sistem
OSPF	Open shortest path first
OTP	One Time Password

PAM	Protocol Analiza Modul
PaaS	Platform-as-a-service
PIN	Personal identification Number
PIS	Poslovno - informacijski sistem
PKCA	PKI Certificate Authority
PKI	Public Key Infrastructure
PKIRA	PKI Registracion Authority
PKR	Public key registration
POP3	Post Office Protocol
PrCA	Professional Certificate Authority
ProDF	Proaktivna digitalna forenzika
PrRA	Professional Registartion Authority
RAID	Redundant Array of Independent Discs
RBAC	Role based AC
RM	Računarska mreža
RRSet	Resource Record Sets
RS	Računarski sistem
SA	Session Key
SaaS	Software-as-a-service
SAM	Security Accounts Manager
SIEM	Security Information and Events Monitoring
SIP9	Session Initiation Protocol
SLA	Saciruty Level Agreement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management protocol
SOA	Servisno orjentisana arhitektura
SOP	Standardne operative procedure
SSH	Secure Shell
SSL	Secure Socket Layer
SQL	Structured Query Language
TCP/IP	Skup protokola razvijen da omogući umreženim računarima da dele resurse putem mreže
TGT	Ticket - Granting Ticket
TLD	Top Level Domain
TLS	Transport Layer Security
TTPS	Trusted Third Party Service
UDP	User Datagram Protocol
UPS	Uninterruptable Power Suply
URL	Uniform Resource Locator
VM	Virtuelne mašine
VPN	Virtual private Network
ZIS	Zdravstveni informacijski sistem
ZU	Zdravstvena ustanova
WAN	Wide area network
www	World Wide Web
XHTML	Extensible HyperText Markup Language
XML	Extensible Markup Language

SADRŽAJ

1.	METODOLOGIJA ISTRAŽIVAČKOG RADA	1
1.1.	Uvod	1
1.2.	Predmet istraživanja	2
1.3.	Ciljevi istraživanja	2
1.3.1.	Naučni cilj	3
1.3.2.	Konkretni cilj	3
1.3.3.	Osnovni problemi zaštite informacija	4
1.4.	Hipoteze istraživanja	5
1.4.1.	Hipotetički okvir – IS ZU Apoteka Vranje „Hubie ERP“	5
1.5.	Metode istraživanja	5
1.6.	Tok istraživačkog rada	6
2.	OSNOVNI ELEMENTI ZAŠTITE RS, RM, WEB APLIKACIJA I CC SISTEMA	7
2.1.	Servis logičke kontrole pristupa računarskoj mreži	7
2.1.1.	Mehanizmi logičke kontrole pristupa RM	7
2.1.1.1.	Logičke mrežne barijere	7
2.1.1.2.	Proksi serveri	7
2.1.1.3.	Web filteri	8
2.1.1.4.	Autentifikacioni protokoli	8
2.1.1.5.	Serveri za autentifikaciju i autorizaciju	9
2.1.1.6.	Smart kartice i kriptografski moduli	10
2.1.1.7.	Ostali autentifikacioni uređaji i protokoli	10
2.1.2.	Zaštita integriteta računarske mreže	11
2.1.2.1.	Skeneri ranjivosti računarske mreže	11
2.1.2.2.	Skeneri telefonskih veza	13
2.1.3.	Mehanizmi za detekciju i sprečavanje upada u mrežu	16
2.1.4.	Mehanizmi za upravljanje log datotekama	17
2.1.5.	Proaktivna digitalna forenzika	18
2.1.5.1.	Virtualno računarsko okruženje	19
2.1.5.2.	Funkcionalni model proaktivne zaštite	20
2.1.6.	Kompjuterski događaj i kompjuterski incident	21
2.1.6.1.	Politike i procedure za upravljanje incidentima	22
2.1.6.2.	Kategorije bezbednosnog kompjuterskog incidenta	22
2.1.6.3.	Nagoveštaj kompjuterskog incidenta	23
2.1.6.4.	Upravljanje kompjuterskim incidentom	26
2.1.6.5.	Upravljanje vanrednim događajem u IKTS	29
i.	Proces planiranja vanrednih događaja	30
2.1.7.	Napadi koji dolaze sa dial-up veze	34
2.1.7.1.	Slučaj direktnog napada	34
2.1.7.2.	Slučaj napada preko telefonske centrale	35
2.1.7.3.	Mrežne tehnike za postavljanje zamke i praćenje traga napadača	35
2.2.	Servisi i mehanizmi zaštite računarskog sistema - NOSSS	38
2.2.1.	Uvod	38
2.2.2.	Mehanizmi zaštite	39
2.2.2.1.	Autentifikacioni protokoli u Windows Server 2003	40
i.	Proces NTLM autentifikacije	40

ii.	Proces Kerberos autentifikacije	41
2.2.2.2.	Log datoteka lozinki u Windows Server 2003 sistemu	42
2.2.2.3.	Šifre na Windows sistemima	43
2.2.2.4.	Ranjivost SAM baze u Windowsu	43
2.2.3.	Karakteristike sigurnosti Encrypting File System-a	45
2.2.3.1.	Šifrovanje i dešifrovanje EFS-a	45
2.2.3.2.	Kriptografski algoritmi u EFS-u	49
2.2.3.3.	Mehanizam oporavka kod EFS-a	49
2.2.3.4.	Potencijalni problemi i rešenja	51
2.2.4.	Međuzavisnost sa drugim kontrolama zaštite	51
2.2.5.	Fuzzer alat	52
2.2.5.1.	Mrežni fuzzer alat	52
2.3.	Web sajt i web hosting	54
2.3.1.	Elementi domena	54
2.3.2.	Web sajt	55
2.3.2.1.	Vrste web sajtova	56
2.3.2.2.	Osnovni pojmovi vezani za web sajtove	56
2.3.3.	Web hosting	57
2.3.4.	Servisi	58
2.3.4.1.	Web servisi	58
2.3.4.2.	Windows servisi	59
2.3.5.	DNS server	59
2.3.5.1.	<i>Root Domain</i>	60
2.3.5.2.	<i>Top Level Domain</i>	61
2.3.5.3.	<i>Second Level Domain</i>	61
2.3.5.4.	Poddomen	61
2.3.5.5.	Zone	61
2.3.5.6.	Redosled ispitivanja	61
2.3.5.7.	<i>Cache Name Server</i>	62
2.3.5.8.	Bezbedni DNS	62
2.3.5.9.	SSL – sloj bezbedne konekcije	63
2.3.6.	Sistem zaštite web transakcija	63
2.3.6.1.	Kriptografski mehanizmi zaštite u troslojnoj arhitekturi	67
2.3.6.2.	Zaštita na aplikativnom nivou	67
2.3.7.	Primer realizacije funkcionalnog modela TTPS provajdera	68
2.3.7.1.	Opšti model TTPS za PKI u ZIS	68
2.3.7.2.	Modelovanje poverenja i sigurnosti TTP servis Provajdera	69
2.3.7.3.	Zakonodavna pitanja	69
2.3.7.4.	Predlozi za realizaciju univerzalnog TTPS provajdera	70
2.4.	<i>Cloud Computing</i>	71
2.4.1.	Šta je <i>Cloud Computing</i> ?	71
2.4.2.	Ko pruža usluge <i>Cloud Computing</i> -a?	72
2.4.3.	Bezbednost u <i>Cloud Computing</i> -u	74
2.4.4.	Uticaj virtualizacije na bezbednost <i>Cloud Computing</i> -a	75
2.4.5.	<i>iStor Secure Data Vault</i>	76
2.4.5.1.	Izuzetna efikasnost i pouzdanost	77
2.4.5.2.	Napredna obrada	77
2.4.5.3.	Pojačana sigurnost	78
2.4.5.4.	Brza offsite zaštita	78

2.4.5.5.	Centralno upravljanje	78
2.4.5.6.	Trag rukovanja podacima	78
2.4.5.7.	Sigurno uklanjanje podataka	79
2.4.5.8.	Isplativa zaštita podataka	79
2.4.5.9.	Ekološki odobren proizvod	79
2.4.5.10.	Podrška 24 sata dnevno, 7 dana u nedelji	79
2.4.5.11.	Dostupan na više načina	79
2.5.	Poslovno – informacioni sistem <i>Hubie</i>	80
2.5.1.	Tehničko-poslovne karakteristike <i>Hubie</i> ERP	80
2.6.	NIST Windows XP sigurnosna podešavanja na računarima	
	ZU Apoteka Vranje	81
2.6.1.	<i>Account Policies</i>	81
2.6.2.	<i>Local Policies</i>	81
2.6.3.	<i>Event Log Policies</i>	83
2.6.4.	<i>Restricted Groups</i>	83
2.6.5.	<i>System Services</i>	83
2.6.6.	Dozvole za pristup podacima	83
2.6.7.	Dozvole za pristup registrima	83
2.7.	Dopunska Windows XP bezbednosna konfiguracija	85
2.7.1.	<i>EFS Data Recovery</i>	85
2.7.2.	<i>User Accounts and Groups</i>	85
2.7.3.	<i>Reviewing Audit Logs</i>	85
2.7.4.	<i>Software Restrictio Policy</i>	86
2.8.	Bezbednosna konfiguracija u Hubi-u	88
2.8.1.	RBAC model	88
2.8.2.	Odnosi sa drugim modelima	89
2.8.3.	Korišćenje i raspolaganje	90
2.9.	Digitalni sertifikati Telekoma Srbija	93
2.9.1.	IBM Sistem za sprečavanje upada	93
2.9.2.	Sistem za detekciju i sprečavanje upada	94
2.9.2.1.	Ciljevi IDPS	94
2.9.2.2.	Klasifikacija IDPS	95
2.9.2.3.	Uobičajene metode za detekciju	95
2.9.2.4.	IDPS arhitektura i komponente	96
2.9.2.5.	Vrste IDPS tehnologija	96
2.9.3.	Cisco sistem zaštite	99
2.9.4.	Microsoft Windows Server 2003 – upravljanje web serverom	103
2.9.5.	HSM	105
2.10.	Autentifikacija u okviru ZU Apoteka Vranje	106
2.11.	Microsoft SQL Server	107
2.11.1.	Kriptografija u SQL Serveru 2003	107
2.11.2.	Šifrovanje u Transact – SQL	108
2.11.3.	Razmatranja	108
2.11.4.	Hijerarhija ključeva	108
2.11.5.	Master ključ SQL Servera	109
2.11.6.	Master ključ baze podataka	110
2.11.7.	Korisnički ključevi	111

3.	ANALIZA REZULTATA	112
	3.1. Analiza rezultata	112
	3.2. Izrada liste preporuka za ostvarivanje ICT bezbednosti	113
	3.2.1. Predlog skupa tehničkih bezbednosnih kontrola za Implementaciju	115
	3.2.2. Predlog skupa administrativnih bezbednosnih kontrola za izradu	121
4.	DISKUSIJA	126
5.	ZAKLJUČCI	132
6.	PREGLED DOBIJENIH REZULTATA	134
7.	PRILOZI	136
	7.1. Prilog 1	136
	7.2. Prilog 2	139
	7.3. Prilog 3	144
	7.4. Prilog 4	148
	7.5. Prilog 5	150
	7.6. Prilog 6	152
	7.7. Prilog 7	153
	7.8. Prilog 8	154
	7.9. Prilog 9	158
	7.10. Prilog 10	161
8.	LITERATURA	163

1. METODOLOGIJA ISTRAŽIVAČKOG RADA

1.1. UVOD

Uz mnoge korisne funkcije koje poseduje savremena računarska tehnologija nastala je negativna pojava koja spada u oblast „kompjuterskog kriminala“. Danas je to vrsta kriminala koja ima najznačajniji i najbrži rast kome treba posvetiti sve veću pažnju.

Shvativši ozbiljnost problema stručnjaci za sigurnost od samog nastanka ove vrste kriminala počeli su da razmišljaju o tome na koji način zaštititi računare i računarske sisteme od zlonamernih korisnika, tzv. hakera. Tražeći adekvatna rešenja razvili su mnoge danas poznate metode zaštite ali su zanemarili jednu bitnu činjenicu, a to je ljudski faktor. Treba napomenuti da se pod sigurnošću sistema smatra mera subjektivnog osećanja ili ubeđenja da je sistem bezbedan, da mu ne pretila nikakva opasnost jer je zaštićen (osiguran) i veruje se da je mala verovatnoća negativnih faktora rizika; u semantičkom značenju to je sinonim za bezbednost sistema.

Stručnjaci za sigurnost sve više shvataju veličinu ovog problema, koja nije u njegovoj kompleksnosti ili ne postojanju rešenja. Bez obzira na eventualnu mogućnost delovanja hakera, cilj osobe odgovorne za sigurnost informacionog sistema jeste da preduzme niz radnji sa ciljem smanjenja ranjivosti sistema i povećanju njegove sigurnosti. Informacioni sistem ne može se u potpunosti zaštititi i to je činjenica koje mora biti svestan svaki korisnik. Radnje odgovornih osoba u cilju povećanja sigurnosti sistema vrlo su individualne zbog individualnosti samih informacionih sistema i stoga se ne mogu definisati univerzalne radnje prema kojima bi se gradila sigurnost sistema. Individualnost je u planiranju sigurnosti i vrlo preporučljiva, jer se na taj način otežava planiranje i izvršavanje napada od strane zlonamernih korisnika.

Sigurnost informacionog sistema je vrlo kompleksna i široka tema u kojoj je jasna jedino činjenica da bez kvalitetnog programa sigurnosti i servisa zaštite sistem nije moguće u potpunosti zaštititi. Kvalitetan program omogućava uspostavljanje sigurnosti na svim kritičnim tačkama sistema, u bilo kojem segmentu sigurnosti, a jedan od najboljih programa za postizanje navedenog cilja zasigurno je definisanje sigurnosne politike.

Misija sistema zaštite je zaštita čiste informacione imovine¹ IKT sistema ZU Apoteka Vranje, kroz izbor, instalaciju i održavanje sistema zaštite na kontrolisanom nivou rizika od pretnji koje ga ugrožavaju.

Proces generičkog metoda analize rizika zahteva akviziciju i procenu sledećih informacija: *osetljivosti informacione imovine* - identifikacija i procena nivoa osetljivosti (ranjivosti) tekućih projektovanih sistema, koje bi mogle biti iskorišćene od strane identifikovanih izvora pretnji; *pretnji* - identifikaciju frekvencije, intenziteta i verovatnoće ispoljavanja potencijalnih izvora pretnji; *identifikaciju i procenu potencijalnog uticaja na poslovne procese ili informacione objekte*, koja se izražava kroz procenu potencijalne materijalne ili nematerijalne štete: *neovlašćeno otkrivanje, izmenu, ili destrukciju podataka* i programa, *ili neraspoloživost podataka i/ili servisa*; *procenu i proračun faktora rizika*, kombinovanjem atributa *vrednosti informacione imovine-A* sa intenzitetom potencijalnih izvora *pretnji-T*, *ranjivostima sistema-V* i *uticaja na poslovanje -U*.

U praksi, zaštitne kontrole sistema zaštite biraju se kao kombinacija atributa **A**, **V** i **T** da se obezbedi **izbalansirana i komplementarna zaštita**, tj. sistem zaštite u kojem su manje efikasne mere i metode zaštite komplementirane sa efikasnijim merama i metodama, a *tehničke* mere zaštite praćene sa *proceduralnim* (upravljačko-administrativnim,

¹ Informacije, hardver, softver, ljudi, okruženje, poslovni procesi i operacije

organizaciono-operativnim) merama i koji zajedno obezbeđuju očekivanu efikasnost sistema zaštite.

Ova metodologija je razvijena na bazi generičke metodologije za analizu rizika - ISO/IEC TR 13335-3 i standarda ISO/IEC 27005, NIST SP 800-30.

ZU Apoteka Vranje ima savremen IKT sistem koji predstavlja donaciju norveške vlade vezanu za uvođenje kompjuterskog informacionog sistema u distribuciji lekova u Srbiji.

Sigurnost IKT sistema, što važi i za IKT sistem ZU Apoteka Vranje, danas se u tehničkom pogledu za relativno malo novca (i puno znanja) može dovesti praktično do savršenstva. Bez obzira na eventualnu mogućnost delovanja hakera, cilj osobe odgovorne za sigurnost informacionog sistema jeste da preduzme niz radnji sa ciljem smanjenja ranjivosti sistema i povećanju njegove sigurnosti.

Za pisanje ovo rada korišćena je implementacija novog IKT sistema ZU Apoteka Vranje i na osnovu toga pristupa se razradi servisa zaštite IKT sistema ZU Apoteka Vranje.

1.2. PREDMET ISTRAŽIVANJA

Naučno istraživanje započinje uviđanjem, postavljanjem i formulisanjem problema. Značenje izraza naučni problem često se određuje kao “znanje o neznanju“. Određivanju značenja izraza „**naučni problem**“ pristupa se sa stanovišta:

a) psihološkog sadržaja problema

- raspolaganje određenom količinom znanja i informacija o nekom predmetu proučavanja
- saznanje nepotpunosti raspoloživog znanja (na tu nepotpunost ukazuje saznanje o logičkom neskladu raspoloživih znanja, o netačnosti, o neodređenosti znanja)
- stremljenje prevazilaženju te nepotpunosti koje se ispoljava kao proces upoređivanja alternativnih pretpostavki s ciljem odgovarajućeg izbora između

b) strukture jezičkog izražavanja problema

Prvi činilac problemske situacije je osnovni, jer neznanje može da se ispolji samo kao saznanje nepotpunosti znanja, što je veoma značajno zato što nas usmerava u traženju merila vrednosti problema.

U ovom radu su razmatrane osobine i funkcija informacionog sistema u Zdravstvenoj ustanovi Apoteka Vranje. Iz dosadašnje prakse je uočeno da ranije korišćeni informacioni sistem, tzv. Clipper nije zadovoljio potrebe ove zdravstvene ustanove. S toga je razmatrana mogućnost novog informacionog sistema kojim bi se ostvarila bolja kontrola i postigao efikasni servis zaštite.

1.3. CILJEVI ISTRAŽIVANJA

Uviđanje vrednog naučnog problema je presudno za razvoj naučnog znanja. Nema oštre granice između uviđanja, **jasnog identifikovanja, postavljanja i rešavanja** naučnog problema, nego je reč o delovima istog procesa. Izabiranje i postavljanje problema u velikoj meri je određeno:

1. „paradigmom“ (Kun)
2. „istraživačkim programom“ (Lakatoš)
3. „istraživačkom tradicijom“ (Laudan)

Ne zasluŹuje svaki problem traganje za rešenjem, pa treba razlikovati:

1. prave od prividnih
2. pravilno postavljene od nepravilno postavljenih
3. vredne od bezvrednih problema

Na osnovu razmatranih iskustava iz teorije i prakse zaštite, a na bazi predmeta istraŹivanja i postavljenih istraŹivačkih hipoteza, definisani su sledeći ciljevni istraŹivanja:

1. Izvršeni pregled i komparativna analiza osnovnih karakteristika, kompatibilnosti i komplementarnosti procesa zaštite i drugih relevantnih modela i standarda procesa zaštite (ISO/IEC 17799, ISO 9000/1, i dr)
2. Definisan Źeljeni nivo procesa zaštite organizacije zasnovan na bazi procesa najbolje prakse zaštite,
3. Analizirani rezultati procesa zaštite i glavni nalazi procesa zaštite u odnosu na Źeljeni nivo zaštite.

Problem koji ima ZU Apoteka Vranje veoma je značajan za razmatranje sa više stanovišta. Sa naučne tačke gledišta potrebno je dokazati da zastareli sistemi tipa Clipper koji se do skoro koristio u ovoj ustanovi ne zadovoljavaju potrebe savremenog poslovanja. Ovi sistemi su totalno nezaštićeni i slabi od spoljnih uticaja i upada pa samim tim i dovode poslovanje cele ustanove u fazu razmatranja uvođenja novog informacionog sistema koji bi pratio nove tehnologije i obezbedio bolju i sigurniju zaštitu njihovih podataka.

Vezano za ovo gledište dolazimo i do društvenog cilja koji ustanovi obezbeđuje bolji rad na nivou jedne organizacije kao što je ZU Apoteka Vranje, sigurnost podataka i poslovanja i smanjenje gubitaka u finansijskom i materijalnom delu.

Inače ovo je konkretan problem „na terenu“ tako da je potrebno sa veoma mnogo pažnje i stručnosti naći odgovarajući informacioni sistem koji bi zadovoljio sve zahteve vezane za ZU Apoteka Vranje, koja je sama po sebi veoma specifična.

1.3.1. Naučni cilj

Ovaj rad ima naučni cilj da otvori put istraŹivanjima upravljanja rizicima informacionih sistema (i ne samo njih) u sasvim novim i neistraŹenim domenima. Dokazi i metode u ovom radu prvi put su primenjeni, u ovakvom obliku, na složenom poslovno-informacionom sistemu ZU Apoteka Vranje i predstavljaju mogućnost ulaska u sasvim nove oblasti gde je neophodno da se rizici kompletno kontrolišu. Osim toga rad je kao cilj postavio potragu za nizom postojećih relacija i zakonitosti koji se dodatno dokazuju samom činjenicom da je poslovno-informacioni sistem dovoljno složen i da pokriva teritoriju celog Pčinjskog regiona.

1.3.2. Konkretni cilj

Kada su u pitanju konkretni ciljevi, ovaj rad ih ima nekoliko:

- Dati moćan alat u istraŹivanju procesa i upravljanja tim istim procesima u složenim sistemima,
- Dati oblik postupanja koji bi morao rezultirati opštim preporukama
- Postići primenu u realnim uslovima rada s rizicima na složenim poslovno-informacionim sistemima, s obzirom da je poznato da PIS *Hubi-e* koriste još neki veliki privredni subjekti pored ZU Apoteka Vranje
- PruŹiti osnove za primenu kompletne prakse na postojećim preporukama, zakskim regulativama i svim vaŹećim standardima.

1.3.3. Osnovni problemi zaštite informacija

Za postavljanje hipoteza i definisanje ciljeva istraživanja u ovom radu razmatrana su opšte prihvaćena i statistički obrađena brojna teoretska istraživanja i iskustva iz prakse zaštite IKT sistema kao i neki novi predlozi zaštite i back-up podataka. Na osnovu prikupljenih podataka i saznanja postavljene su opšta i osnovne hipoteze i definisani ciljevi istraživanja.

Osnovna iskustva, koja su zajednička za skoro sve posmatrane izvore, svakako su nedovoljno razvijena svest o potrebi zaštite, sporo menjanje te svesti i neprihvatanje naprednih tehnologija, čak i u informatički mnogo razvijenijim društvima nego što je ovo naše što povlači nedovoljan broj osposobljenih specijalista IKT zaštite po organizacijama. U prilog tome je i činjenica da je svest o potrebi zaštite definisana kao jedan od 9 fundamentalnih, generalno prihvaćenih principa zaštite (*GAISP – Generaly Accepted Information Security Principlless*), [8] osnovnih gradivnih blokova svake metodologije za razvoj programa i sistema zaštite. Ovome treba dodati i tipično nedovoljan broj stručnih i osposobljenih specijalista zaštite koji bi se borili protiv zloupotrebe IKT sistema u svim poslovnim sistemima.

Relevantni su problemi za upravljanje kvalitetom procesa IKT zaštite, kao što su:

- Višeznačnost koncepta „metrike“ U IKT zaštiti i teškoće u dobijanju kvantitativnih mernih rezultata za objekte IKT zaštite, zbog niske objektivnosti rezultata merenja i problema generalizacije i poređenja rezultata;
- Teškoće u merenju operativnih kontrola zaštite, jer je teško predvideti stvarno funkcionisanje sistema zaštite;
- Sama priroda oblasti IKT zaštite, gde uvek postoji rizik od otkrivanja i iskorišćavanja ranjivosti sistema, kao i
- Konstantan problem ubeđivanja menadžmenta i vlasnika sistema o potrebi zaštite što u našem okruženju predstavlja najveći problem i samim tim je na vrhu liste.

Posledice slabog razvoja svesti o potrebi zaštite korisnika, a posebno menadžera i vlasnika sistema brojne su, a glavne su sporo prihvatanje realnih pretnji i implementacija, uglavnom, skupih i najčešće reaktivnih sistema zaštite, koji reaguju samo na poznate pretnje. Neadekvatna je i borba protiv zloupotreba IKT sistema i rastućeg kompjuterskog kriminala, u poređenju sa brzinom razvoja IKT sistema i sve novijih i sofisticiranijih vrsta pretnji za umrežene sisteme, povezane preko nebezbednog Interneta, [24]. U ovu grupu rizičnih korisnika spada i ZU Apoteka Vranje jer je mrežni sistem koji ona koristi razvijen za ceo Pčinjski region a razmena podataka i prikupljanje podataka na glavni server, koji se nalazi u Vranju, je isključivo preko Interneta. Jedno od skupljih i relativno manje dostupnih rešenja ovog problema je razvoj planiranog, dobro definisanog, dokumentovanog i upravljanog proaktivnog sistema zaštite, koji reaguje na poznate i nepoznate pretnje, [15].

Druga, korisnički prihvatljivija mogućnost usmerena je na dobro definisanje i neprekidno poboljšavanje procesa zaštite. Primenom sistem-inženjerskog i procesnog pristupa organizacije mogu raspoloživim resursima i sa prihvatljivom dinamikom razvijati i progresivno poboljšavati procese zaštite do uspostavljanja optimalnog programa zaštite, [4, 27], i implementirati sisteme najbolje prakse zaštite u kombinaciji sa analizom rizika u realnom okruženju [41, 27] i bezbednim back-upovanjem podataka na sigurno mesto koje bi bilo dostupno danonoćno. U skladu sa realnim ljudskim, finansijskim, tehnološkim i vremenskim resursima, organizacija sama bira polazni nivo procesa zaštite, željene nivoe profila procesa zaštite kojima teži i dinamiku realizacije pojedinačnih projekata za poboljšavanje individualnih procesa (OP), ili grupe procesa zaštite.

1.4. HIPOTEZE ISTRAŽIVANJA

Polazeći od široko prihvaćenih definicija procesa zaštite, kao transformatora ulaznih u izlazne parametre, sa očekivanim povećanjem vrednosti na izlazu i kao integratora metodologije zaštite, tehnologije zaštite i osposobljenosti ljudi, motivisanih za izvršavanje procedura i metoda i upotrebu tehnika i alata zaštite, a uzimajući u obzir relativno visoku cenu tehnologija zaštite i nedovoljnu raspoloživost stručnjaka zaštite, proizilazi da se ovi nedostaci mogu optimalno kompenzovati usmeravanjem pažnje menadžmenta ustanova i organizacija na kvalitet i stalno poboljšavanje procesa zaštite.

1.4.1. Hipotetički okvir – informacioni sistem Zdravstvene ustanove Apoteka Vranje - „HUBIE ERP“

Opšta hipoteza: *Postojeći poslovni IKT sistem bez adekvatne zaštite podataka i informacija ne obezbeđuje zahtevani kvalitet savremenog poslovanja ZU Apoteka Vranje u Internet okruženju i često izaziva materijalne i finansijske gubitke.*

Savremeni IKT sistemi uglavnom poseduju neformalno izvršavane procese zaštite što se moglo videti i na primeru ZU Apoteka Vranje. Ovde se slabo (gotovo nikako) planirala i dokumentovala aktivnost zaštite, delimično ili nikako konfigurisao sistem zaštite u prirodnom OS računarskog sistema (NOSSS), a od komplementarnih alata zaštite najčešće se koristila mrežna barijera (*firewalls*) i antivirusni programi. To je sve iz razloga što su troškovi adekvatne tehnologije zaštite relativno visoki dok je svest o potrebi zaštite vlasnika sistema i korisnika generalno slabo razvijena.

Posebna hipoteza: *Za pouzdan rad IS Apoteke Vranje u Internet okruženju zahteva se sveobuhvatan sistem slojevite zaštite. Savremenim mehanizmima i servisima zaštite postojećeg IKT sistema obezbediće se visok kvalitet poslovanja ZU Apoteka Vranje. Efektivno upravljanje sistemom zaštite IS Apoteke Vranje obezbeđuje se uspostavljanjem politike i pravila zaštite.*

1.5. METODE ISTRAŽIVANJA

ZU Apoteka Vranje predstavlja jednu kompleksnu i složenu celinu tako da je za proučavanje njihovog problema korišćeno više metoda istraživanja. Od opštih metoda korišćena je analiza i ako želimo da budemo još precizniji potpuna ili totalna analiza. Nakon što je izvršena analiza i ceo sistem raščlanjen na delove i proučavan do detalja uvođenjem novog informacionog sistema svi delovi se sklapaju u jednu celinu sa novim sistemom i zajedno čine poslovni informacioni sistem *Hubie* – tako da ovo predstavlja sintezu kao osnovnu metodu istraživanja. Pored ovih metoda korišćene su još i indukcija koja je prelazna metoda od analitičkih ka sintetičkim metodama kao i dedukcija koja je sa indukcijom međusobno povezana i uslovljena i time što u toku naučno – saznanog procesa, kao i procesa revizije, neprekidno prelaze jedna u drugu. Što se tiče statističkih metoda u procesu istraživanja *prva etapa* primene statističke opštenaučne metode, u skladu sa njenim pravilima i procedurom primene, jeste *identifikacija statističke mase*. Uzorkovanje i izrada uzorka čine *drugu etapu* primene statističke metode dok je *treća etapa* prikupljanje podataka. *Četvrtu etapu* u primeni ove metode čini *formiranje statističkih serija*. Formiranje serije podataka spada u fazu sređivanja i obradu podataka. *Peta etapa* jeste *statistička analiza*. Statističke podatke smo sredili u statičke serije i analizirali ih kako bi otkrili strukturu, međusobne uticaje činilaca strukture i dinamiku odigravanja istraživanih pojava odnosno procesa. *Šesta etapa* jeste *tumačenje rezultata*

statističke analize i izvođenje zaključaka. Osnovni zadatak nam je bio izvođenje direktnih i indirektnih generalizacija manjeg ili većeg stepena istinitosti odnosno verovatnoće o pouzdanosti informacije o predmetu. Poslednja, *sedma etapa* u primeni opštenaučne statističke metode jeste konstatovanje određenih pravilnosti u procesima koji su vezani za podešavanje informacionog sistema ZU Apoteka Vranje.

1.6. TOK ISTRAŽIVAČKOG RADA

Tok istraživanja procesa i pisanje samog rada išao je sledećim redosledom:

1. Prvo je predstavljen predmet istraživanja, odnosno poslovno-informacioni sistem ZU Apoteka Vranje
2. Prepoznavanje i izdvajanje glavnih elemenata problematike
3. Sistematizacija i potpuna analiza svih raspoloživih preporuka, zakonskih regulativa i standarda
4. Zatim su postavljeni cilj i zadaci istraživanja
5. Postavljene su opšta i posebna hipoteza na osnovu kojih se biraju
6. Metode istraživanja
7. Nakon izbora metoda istraživanja pristupa se razradi problema kao i načinu regulisanja servisa zaštite IKT sistema ZU Apoteka Vranje
8. Verifikacija hipoteze i
9. Pisanje rada

Identifikovanje stanja: Opšta ocena referenta tehničke podrške je da tekući procesi koje ustanova koristi za uspostavljanje PKI sistema (CA i drugih modula) nisu stabilni i ne zadovoljavaju osnovne principe zaštite.

Tekući procesi su planirani, a tehničke aktivnosti kontrolisane isključivo na nivou tekućeg zadatka, ali se ne koristi u punoj meri sistem indikatora stanja progressa u kontrolnim tačkama (*benchmarking*), ne dokumentuju rezultate kontrole i ne primenjuje se striktno analiza rizika za izvođenje zadatka. Procesu su u operativnoj fazi monitorisani i upravljani, kroz izveštavanje korisnika o incidentima u primeni aplikacija i automatizovanim generisanjem izveštaja o stanju sistema i dostavljanjem putem e-mail poruka na server lokalne mreže ESS. Međutim, organizacija ne planira i ne vrši regularnu analizu indikatora stanja bezbednosti, iako su obezbeđene metrike za prikupljanje ovih podataka, uključujući i log datoteke događaja u operativnoj primeni aplikacija, koje obuhvataju i bezbednosno relevantne događaje.

ESS nema formalno definisane, opisane i standardizovane procese organizacije; nema razvijenu familiju standardnih procesa, niti posebnu biblioteku procesa zaštite ustanove. Osnovni problem su ljudski resursi, jer se popuna stručnim kadrovima planira prema zahtevima za projektovanje, razvoj, implementaciju i integraciju PKI sistema na bazi MS Windows platformi. Politike zaštite izrađene su na nivou ključnih komponenti PKI sistema, ali nije izrađena politika zaštite na nivou ustanove. Takođe nedostaju politika i sistem za upravljanje dokumentacijom.

U Prilozima predložena su neka dokumenta koja bi bila neophodna za formiranje biblioteke procesa zaštite ustanove.

2. OSNOVNI ELEMENTI ZAŠTITE RS, RM, WEB APLIKACIJA I SISTEMA U OBLAKU

2.1. SERVIS LOGIČKE KONTROLE PRISTUPA RAČUNARSKOJ MREŽI

Mrežna infrastruktura obuhvata komunikacionu mrežu, uređaje za povezivanje, matične računare i tačke povezivanja sa mrežom. Uspešan napad na mrežnu infrastrukturu može onesposobiti računarsku mrežu ili je izložiti raznim zloupotrebama. Za efektivnu zaštitu mrežne infrastrukture i računarske mreže treba poznavati tipove potencijalnih napada. Od većine potencijalnih napada na računarsku mrežu osnovna zaštita je kontrola pristupa kritičnim resursima, protokolima i pristupnim tačkama, uključujući fizičku zaštitu i zaštitu konfiguracije uređaja, neprekidni nadzor mrežnog saobraćaja, zaštitu servera, mobilnih uređaja, radnih stanica i uređaja za umrežavanje, NIDPS, zaštitu udaljenog pristupa i zaštitu bežičnih računarskih mreža. Najbitnija komponenta zaštite računarske mreže je PKI, koja obezbeđuje brojne prednosti u odnosu na simetrične sisteme, uključujući uređaje za zaštitu kriptografskih tajni *autentifikacioni i autorizacioni serveri, kripto-moduli, smart kartice, tokeni itd.*

2.1.1. Mehanizmi logičke kontrole pristupa računarskoj mreži

2.1.1.1. Logičke mrežne barijere

Logičke mrežne barijere (*Firewalls*) su uređaji ili konstrukcije uređaja koje nameću politiku LAC između dve računarske mreže ili segmenata računarske mreže. Barijere blokiraju konekcije na bazi politike i rade na nivoima 3 – 7 OSI modela. U TCP/IP modelu slojevi 5,6 i 7 su deo aplikacija, tako da se barijere za blokiranje/dopuštanje baziraju na mrežnom, transportnom i aplikativnom sloju. Barijere generalno kontrolišu saobraćaj na mrežnom nivou, ne prepoznaju protokole koji nisu TCP/IP, pa moraju biti specifično konfigurisane da prepoznaju druge tipove protokola.

Barijere sa uspostavljanjem veze, kontrolom stanja veze i tehnikom filtriranja rutiranih IP paketa od jednog mrežnog interfejsa do drugog, presreću već rutirane pakete na mrežnom sloju i analiziraju informacije o protokolu od slojeva 3 – 7. Takođe, analiziraju informacije o stanju veze, da bi odredile da li pakete treba blokirati ili propustiti.

Barijere na aplikativnom sloju poznate kao aplikativna mrežna kapija (*gateway*) ili *proksi*, ne rutiraju direktno pakete. Dolazne pakete procesuiraju komunikacioni programi i prenose ih aplikaciji koja može da čita određeni protokol na visokom nivou apstrakcije. Pošto nameću kontrole na aplikativnom sloju, proksi barijere su specifične za aplikacije, što znači da svaki put kada se razvija novi protokol za neku aplikaciju, zahteva se novi proksi za zaštitu. U stvarnosti, većina savremenih protokola nemaju proksi barijere, koje ih prate, a proksi serveri se uglavnom koriste za kontrolu standardnih Internet protokola, kao što su FTP ili HTTP.

2.1.1.2. Proksi serveri

Proksi serveri funkcionišu slično aplikativnim *gateway* barijerama. Dok su barijere namenjene za kontrolu mrežnog pristupa dolaznog i odlaznog saobraćaja, proksi serveri su usmereni na kontrolu konekcija koje dolaze iz interne računarske mreže. Proksi serveri zahtevaju autentifikaciju krajnjeg korisnika, vrše restrikciju komunikacija na definisani skup protokola, primenjuju restrikciju kontrola pristupa i loguju kontrolne tragove. Najčešći tip proksi servera u praksi su web proksi serveri, koji se ne koriste samo za

zaštitu. Proksi serveri nisu mehanizmi za zaštitu računarskih mreža i korektnije ih je smatrati višefunkcionalnim mrežnim uređajima, koji implementiraju važnu bezbednosnu funkcionalnost.

2.1.1.3. Web filteri

Web filteri se koriste za kontrolu pristupa internih korisnika web lokacijama, omogućavajući administratoru da selektivno blokira pristup određenim tipovima web lokacija, na bazi lokalne politike zaštite. Koriste se i za kontrolu produktivnosti zaposlenih i sprečavanje pristupa zabranjenim web lokacijama.

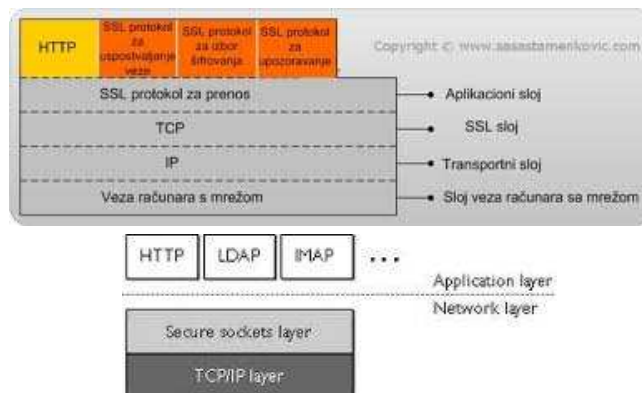
Odluka o blokiranju/dopuštanju pristupa, web filter donosi na bazi konsultovanja instalirane baze podataka o potencijalno problematičnim web lokacijama, koje održavaju i regularno ažuriraju proizvođači. Neki proizvodi poseduju inteligentne agente, koji analiziraju sve posećivane web lokacije i ažuriraju baze podataka. Ovi mehanizmi tipično uključuju mogućnost blokiranja određenih kategorija sadržaja sa web lokacija, restrikcije za određeni period dana, definisanje načina monitorisanja pokušaja pristupa, izdavanje standardnih i kastomizovanih izveštaja i praćenje ponašanja korisnika i poseta lokacijama.

2.1.1.4. Autentifikacioni protokoli

Glavni bezbednosni problem postojećih TCP/IP mreža je lakoća, sa kojom se podaci mogu presresti i analizirati. Zato, svaki mehanizam autentifikacije koji se oslanja na lozinke u otvorenom tekstu ili bilo koja predvidljiva razmena podataka, nije bezbedna u mrežnom okruženju. Zaštita mrežne infrastrukture deo je rešenja ovog problema, ali ne obuhvata mogućnost da neovlašćeni korisnik može koristiti svoju opremu za pristup mreži i aktivirati *snifer* (skener prisluškivač) ili sličan alat za kontrolu saobraćaja u računarskoj mreži. Zato je neophodno ugraditi mehanizme zaštite u sam proces razmene podataka. Uobičajen način, da se ovo uradi, je korišćenje standardnih autentifikacionih protokola [10,18,19,36].

Autentifikacioni protokoli su posebna oblast. Oni se, uglavnom, zasnivaju na konceptu upita – odgovora ili razmene digitalnih sertifikata. Osnovna ideja je da sistem zahteva dokaz o identitetu, a korisnici inicijalno koriste neki drugi mehanizam za razmenu kriptografskih ključeva.

Treba uočiti da autentifikacija nije isto što i uspostavljanje bezbedne sesije i da svaka konekcija, koja ne koristi dodatne mere zaštite može biti kompromitovana. Autentifikacija korisnika uključuje unošenje lozinke preko uspostavljene bezbedne sesije, kao što je SSL (*Secure Socket Layer*) protokol.



Slika 2.1. Lokacija SSL protokola u višeslojnoj arhitekturi računarske mreže [33]

Ovaj metod autentifikacije korisnika često se koristi za pristup web aplikacijama na Internetu. SSL je osnovni protokol za zaštićen prenos lozinke. SSL protokol obezbeđuje autentifikaciju servera klijentu, klijenta serveru i uspostavljanje bezbedne, kriptološki zaštićene, komunikacije između klijenta i servera.

SSL protokol koristi dva podprotokola:

- SSL protokol zapisa poruka (*SSL record protocol*) koji definiše formate poruka za prenos podataka i
- SSL protokol dogovaranja parametara sesije (*SSL handshake protocol*) koji se koristi za razmenu poruka, sastavljenih prema SSL protokolu zapisa poruka, između SSL klijenta i SSL servera kada se među njima po prvi put uspostavlja SSL veza.

SSL protokol podržava više različitih kriptografskih algoritama za međusobne autentifikacije klijenta i servera, razmene digitalnih sertifikata i uspostavljanje tajnih simetričnih ključeva.

Tabela 2.1. Kriptografski algoritmi za komunikaciju sa SSL protokolom

Algoritam	Opis i primena kriptografskog algoritma
DES	<i>Data Encryption Standard</i> - standardni algoritam za šifrovanje podataka
DSA	<i>Digital Signature Algorithm</i>
KEA	<i>Key Exchange Algorithm</i> za razmenu simetričnih ključeva
MD5	<i>Message Digest</i> v. 5, hash funkcija i algoritam za digitalno potpisivanje
RC2 i RC4	<i>Rivest Ciphers</i> simetrični kriptografski algoritmi koje je razvio <i>Ron Rivest</i>
RSA	Asimetrični algoritam za šifrovanje i autentifikaciju
RSA key exchange	Algoritam za razmenu simetričnih ključeva kod SSL protokola zasnovan na RSA algoritmu
SHA-512	<i>Secure Hash Algorithm</i> , hash funkcija dužine 512 bita
Triple-DES	DES algoritam primenjen tri puta nad istim podacima

Autentifikacioni SSL protokoli dopuštaju napad ubacivanjem čoveka u sredinu i uticaj na većinu servera na Internetu. Ranjivost omogućava da se napadač ubaci u SSL protokol na komunikacionom putu. Pri tome ni web server ni web pretraživač ne mogu otkriti da je sesija oteta. Ranjivost dolazi u standardu protokola (formalno poznat kao TLS – *Transport Layer Security*). Većina SSL implementacija je ranjiva na neki način. Scenario napada uključuje korisnika koji plaća online račune, banku koja koristi protokole zasnovane na web servisima i druge aplikacije kao što su mail serveri, serveri baze podataka itd. Sve biblioteke SSL protokola treba bezbednosno popraviti.

2.1.1.5. Serveri za autentifikaciju i autorizaciju

Autentifikacioni i autorizacioni (A&A) serveri obezbeđuju centralizaciju upravljanja procesom autentifikacije – verifikacije identiteta i autorizacije – pridruživanja skupa privilegija autentifikovanim entitetima.

Serveri za A&A obezbeđuju odgovarajuće servise za više klijenata u klijent-server arhitekturi. Uređaj poznat kao server mrežnog pristupa – NAS (*Network Access Server*) prima vezu od PSTN i nakon autentifikacije korisnika i primene neke restrikcije, dopušta konekciju na zahtevani host. Za ove funkcije NAS može koristiti lokalnu bazu podataka ili, što je češće – servise A&A servera [13].

Korišćenje servera za A&A značajno povećava bezbednost pristupa udaljenih korisnika, ali stvarni nivo bezbednosti dostiže se u zavisnosti od primenjenog metoda

A&A. Međutim, čak i sa vrlo bezbednom implementacijom, tehnike A&A ne štite podatke, koji se izmenjuju između korisnika i internog računarskog sistema, kada se veza jednom uspostavi. Zato treba ići korak dalje i implementirati zaštitni protokol između krajnjeg korisnika i odgovarajućeg terminala iza NAS. Ovo rešenje štiti poverljivost podataka i integritet same sesije.

Za web aplikacije, sa zahtevom za visoki stepen skalabilnosti, razvijen je EAM (*Extranet Access Management*) programski paket koji obezbeđuje servise A&A u ektranet okruženju.

2.1.1.6. Smart kartice i kriptografski moduli

Autentifikacioni uređaji obezbeđuju korisniku neki fizički identifikator, koji se zahteva za uspešan proces autentifikacije. Većina poznatih uređaja za autentifikaciju spada u kategoriju smart kartice i biometrijskih uređaja i tokena.

Za visoku bezbednost računarske mreže, u prvom redu, koriste se smart kartice i kriptografski moduli za zaštitu kriptografskih tajni. Sa aspekta fizičkih karakteristika, postoje tri glavne klase smart kartica: kontaktne – zahtevaju fizički kontakt sa čitačem kartica, bezkontaktne – kapacitivno ili induktivno spregnute sa čitačem kartica i kombinovane kartice – obezbeđuju oba načina rada [14].

Za visoku bezbednost računarske mreže, u prvom redu, koriste se smart kartice i kriptografski moduli za zaštitu kriptografskih tajni. Iako su objavljene bezbednosne ranjivosti smart kartice (napadi diferencijalnom analizom i optičkom indukcijom greške), smart kartice se generalno smatraju bezbednim okruženjem za skladištenje kriptografskih ključeva i drugih poverljivih informacija korisnika.

Smart kartica za skladištenje kriptografskih tajni korisnika, štiti pristup podacima sa zahtevom za unošenje personalnog identifikacionog broja – PIN (*Personal identification Number*) ili nekog biometrijskog parametra (otisak prsta, retine oka, šake i sl.) za otključavanje interfejsa, čime se implementira dvoslojna ili troslojna, jaka autentifikacija, koja od korisnika zahteva višekratnu identifikaciju i verifikaciju identiteta. Korisnik nema pristup samom ključu u smart kartici i ne može da ga otkrije drugom licu, optužujući pri tome da je to uradio neko drugi. Smart kartice su dobar izbor za zaštitu kriptografskih tajni korisnika, ali nisu pravi izbor za operacije na serverskoj strani.

Na serverskoj strani bolja opcija je skladištenje ključeva na tzv. HSM (*Hardware Security/Storage Module*). U ovoj oblasti važan standard je NIST FIPS 140-1 i 2 koji pokriva ukupno jedanaest oblasti dizajna i implementacije kriptografskih modula. Standard se koristi za rangiranje bezbednosnih uređaja na četiri bezbednosna nivoa zaštite (1 – najmanji, 4 – najveći). Kriptografski moduli se rangiraju na osnovu serije zahteva za derivirane testove (DTR) [31].

Elektronsko poslovanje donosi praktično neograničen broj klijenata, što zahteva veću skalabilnost aplikacija i kriptografskih rešenja zaštite. Za bolje performanse kriptografskih aplikacija koriste se kriptografski akceleratori – specijalizovani HSM, koji kombinuju bezbedno skladištenje ključeva sa jakom kriptozastitom.

2.1.1.7. Ostali autentifikacioni uređaji i protokoli

Biometrika obuhvata tehnike provere otiska prsta, geometrije ruke, mrežnjače i DNK, prepoznavanje govora, lica i facijalne termografije. Svi mehanizmi zaštite pristupa računarskoj mreži uvek su kompromis između potreba za zaštitom i potrebe za komfornim pristupom regularnih korisnika. Kriterijumi za izbor biometrijskih tehnika mogu biti različiti, kao što su: performanse i pouzdanost, pogodnost za primenu, kompleksnost

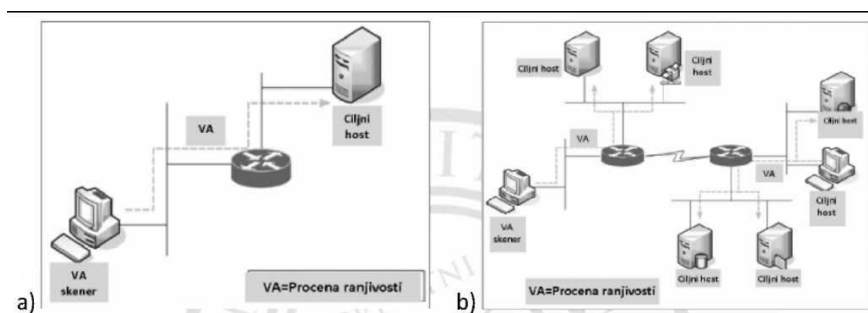
korisničke upotrebe, sposobnost korisnika, korisnička prihvatljivost, troškovi nabavke i sl. Iako se preporučuje biometrijska autentifikacija korisnika, ovu primenu prate brojni problemi: visoka cena, korisnička neprihvatljivost, visok stepen grešaka, nemoguća autentifikacija uređaja, neotpornost na napade i dr.

Tokeni se dele na: uređaje za bezbedno skladištenje kriptografskih informacija i priručne uređaje za autentifikaciju. Prvi su alternativa smart karticama. Drugi su opremljeni sa malim displejem i tastaturom i generalno se ne moraju povezivati na radnu stanicu. Uređaj se konfiguriše sa autentifikacionim serverom pre izdavanja prava pristupa korisniku, kada server i token razmene kriptografske tajne.

2.1.2. Zaštita integriteta računarske mreže

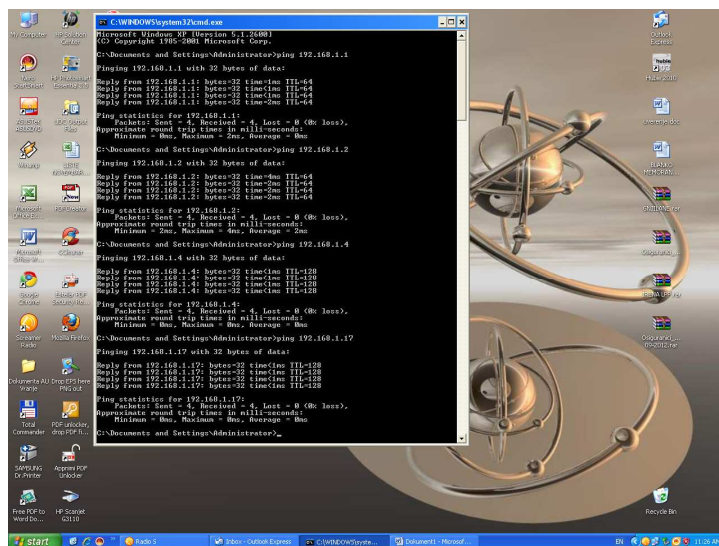
2.1.2.1. Skeneri ranjivosti računarske mreže

Skeneri zaštite integriteta računarskih mreža po konceptu su slični skenerima zaštite računarskih sistema, s tim da se otkrivaju ranjivosti računarske mreže.



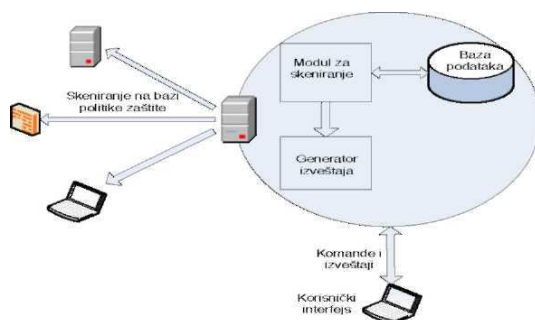
Slika 2.2. Tipičan skener za procenu ranjivosti RS – (a) i implementacija u RM – (b) [15]

Najjednostavniji skener ranjivosti računarske mreže samo mapira uređaje povezane u računarsku mrežu, koristeći jednostavni probni ICMP (*Internet Control Message Protocol*) eho signal, poznat kao ping.



Slika 2.3. Pingovanje računara u mreži

Na višem nivou su jednostavni alati koji mogu mapirati portove, pingujući individualne TCP ili UDP portove na detektovanim hostovima. Ovi alati mogu mapirati mrežu i identifikovati koji su mrežni servisi operativni. Komercijalni alati, iako koriste manje više iste tehnike, znatno su moćniji, jer sadrže baze podataka sa poznatim ranjivostima. Mrežni skeneri su bazirani na sličnim principima, kao i host orijentisani tj. upoređuju aktuelnu konfiguraciju računarske mreže i hostova sa predefinisanim referentnom konfiguracijom i izveštavaju o otkrivenim razlikama. Generalno, skeneri računarskih mreža obezbeđuju više vrsta informacija, ali sa manje detalja od skenera računarskih sistema. Arhitektura skenera ranjivosti računarske mreže uključuje *modul za skeniranje, bazu podataka sa definicijama poznatih ranjivosti, modul za generisanje i prezentaciju izveštaja i korisnički interfejs*. Modul za skeniranje implementira politiku zaštite, koja omogućava prilagođavanje procesa skeniranja zahtevima okruženja, skenira računarsku mrežu, otkriva i poredi tekuće ranjivosti sa poznatim iz baze podataka i daje podatke na izlazu. Rezultati se prikazuju preko korisničkog interfejsa za izveštavanje.

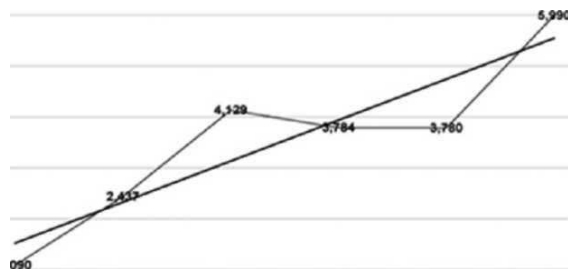


Slika 2.4. Skeneri ranjivosti računarskih mreža [15]

Efektivnost skenera računarske mreže zavisi od sličnih faktora kao i skeneri računarskih sistema: *ažurnosti baza podataka* poznatih ranjivosti; *lokacije skenera* u topologiji računarske mreže u odnosu na uređaje, koji mogu blokirati mrežni saobraćaj (barijere, rutere...), što se mora pažljivo planirati; *adekvatnost politke skeniranja* i *efkasnost procesa korekcije*, koji sledi po otkrivanju ranjivosti. Poslednji faktor je najvažniji, jer bez otklanjanja uzroka ranjivosti računarske mreže proces skeniranja nije završen. Za procenu ranjivosti računarske mreže koriste se brojni alati.

Analitičar zaštite ili menadžer, na osnovu ovih rezultata, mogu brzo proceniti podložnost poznatim bezbednosnim ranjivostima.

Od 1995. do 1999. godine, javno je objavljeno samo 1.506 ranjivosti, a samo u 2000. - 1.090. Koristeći podatak iz 2000. godine kao osnovu od kojih su mereni relativni nivoi porasta ranjivosti, od 2005. godine zabeležen je porast od preko 500 ranjivosti godišnje [26].



Slika. 2.5. Linearna aproksimacija rasta ranjivosti od 2000-2006 [26]

Na slici br. 2.5. prikazane su otkrivene ranjivosti u periodu od 2000. do 2006. godine, sa linearnom aproksimacijom rasta prema jednačini:

$$y=805,6x + 716,6$$

gde je:

y- procenjeni broj ranjivosti za datu godinu,

x- procenjeni vremenski period (npr. 2000=1, 2001=2, 2006=7), 805,6 - nagib i 716,6 - y-intercept.

Na bazi ovog trenda procenjen je rast ranjivost za 2006. i 2007. godini na 6.353 i 7.158, respektivno.

2.1.2.2. Skeneri telefonskih veza

Skeneri telefonskih veza su komercijalni razvoj hakerskih alata tzv. *war dialing* programa, koji se koriste za identifikovanje potencijalnih ranjivosti sistema preko telefonske linije. Konceptualno su sasvim slični skenerima ranjivosti računarskih mreža; biraju seriju telefonskih brojeva, vrše određeni broj bezbednosnih provera, izveštavaju o rezultatima i na taj način prave bezbednosnu mapu telefonskog sistema organizacije, dok skeneri ranjivosti računarske mreže mapiranjem IP adresa prave mapu uređaja lokalne mreže.

Telefonski skeneri detektuju ranjive puteve u računarskoj mreži organizacije koji su pristupačni sa javne telefonske mreže (PSTN). Posebno oni detektuju neovlašćene i nepoznate modeme prisutne na LAN-u i koji mogu prihvatiti dolazne pozive. Principi rada telefonskih skenera zasnivaju se na kombinaciji tehnika probe (pingovanja) i prepoznavanja zahteva za izveštavanje (*prompts*) o ranjivostima na nivou operativnog sistema i na nivou aplikacija (npr. udaljeni pristup sistemu bez passworda).

Pošto se kontrola modema često vrši kroz proceduralna rešenja (mada postoje programi za automatsku detekciju modema), telefonski skeneri značajno povećavaju stopu detekcije neovlašćenih modema automatizacijom procesa detekcije.

Postojeći komercijalni programi veoma su sofisticirani i poseduju čitav spektar opcija konfiguracije, koje omogućavaju operateru da prilagodi skeniranje specifičnim zahtevima. Posebno je značajna fleksibilnost koja obezbeđuje specifikaciju brojeva koje treba skenirati, sa mogućnošću unošenja pojedinačnih ili grupnih brojeva za skeniranje. Skeneri se mogu programirati za rad u određeno vreme dana, predefinisati sa logičkim ograničenjima samog procesa skeniranja (zaustavljanje ponovnog biranja posle određenog broja pokušaja korišćenja sekvencijalnog ili slučajnog biranja i definisanje perioda između dva biranja).

Određeni alati podržavaju različite modove rada dopuštajući operateru da bira između pasivne identifikacije računarske mreže koji odgovara na poziv ili agresivnijeg pokušaja proboja. Poslednji način rada uključuje pokušaj pogađanja kombinacije korisničkog imena/pasvorda i razvoj kompleksnog scenarija proboja kojeg određuje tip detektovanog programa.

Postoje rešenja za distribuirano skeniranje udaljenom instalacijom birača pod kontrolom centralne upravljačke stanice, kao i šifrovane komunikacije između centralne i udaljenih distribuiranih komponenti. Ovo omogućava paralelno skeniranje.

U većini slučajeva telefonski skeneri poseduju jednostavan GUI (*Graphic User Interface*) i proizvode nekoliko različitih tipova izveštaja kao i mogućnost prilagođavanja tipa izveštaja korisniku (kustomizacije).

Koncepcija rešenja:

- Postavlja se između MTK i telefona
- Na MTK – A/D konverzija 8kHz, 8 bita po odmerku
- Kompresija govora vokoderom AMBE1000 (od 2400 do 9600 b/s)
- Digitalna zaštita na bazi GPSN, signal procesor TMS320C5410
- Modemski prenos V.34, V.80

Blok šema:

Tehničke karakteristike:

- Digitalna K3 na bazi PSN
- Zaštita od KEMZa
- Unos K3 podataka preko RS232 porta
- Napajanje (7.5V do 14 V):
 - ✓ iz spoljašnjeg izvora (10V do 14V)
 - ✓ iz akumulatora 12V ± 10%
 - ✓ iz interne baterije (7.5V)
- potrošnja manja od 600 mA

Organizacija ključeva:

- više radnih ključeva (mreže)
- rezervni ključevi za svaku mrežu
- važenje jednog UK – mesec dana
- vektor pristupa i radna mreža
- automatski izbor radnog UK prema mreži pozvanog učesnika
- smena ključeva . iz menija uređaja
- brisanje ključeva – u slučaju opasnosti

Instaliranje:

- postavlja se između MTK i telefona
- koristi se postojeći MTK
- dodaje se jedan kabal do telefona
- povezuje se izvor za napajanje
- uključi se uređaj i iz menija se bira tip telefonskog aparata
- završeno je instaliranje
- nova instalacija – samo kada se uređaj nosi na drugi tip telefona

Upotreba:

- telefonska veza se uspostavlja otvoreno
- uključi se napajanje na uređaju
- jedan od učesnika vrši prelazak u zaštićeni režim rada
- čeka se uspostavljanje sinhronizacije
- zaštićena veza – svetli zeleni LED
- raskid veze – asinhrono

Sistem menija:

Tri nivoa:

- Korisnik – osnovni podaci i samotestiranje
- Operater – reset podataka, instaliranje, izbor brzine, blokiranje rada
- Administrator – održavanje, dozvola pristupa, unos i izbor K3 podataka

Postoje inicijalne (fabričke) lozinke, mogu se menjati na uređaju.

Pravci razvoja:

- Integracija čitača SMART kartica
- Na SMART kartici: deo algoritma i ključevi. Omogućava se personalna identifikacija.
- Prenos podataka
- Zaštita na bazi slučajnih nivoa

Zaštićene komunikacije:

- Mreža – konfiguracija uređaja (procesori, kontroleri, terminali...)
- Međusobno povezani u cilju obrade i razmene informacija
- Veza može biti raznovrsna: žičana, bežična, satelitska, mikrotalasna, multipleksirana, ...
- Mreža: heterogene strukture
- Pristupna tačka i korisnik

Vrste:

- Tipovi šifrovanih komunikacija:
 - ✓ *Link encryption* (zaštita veze)
 - Šifrovane su nezavisno veze između dve tačke mreže
 - Za svaku vezu koristi se različit ključ K
 - Pogodno jer se distribucija ključa radi između tačaka T1 i T2, a ne T3
 - Potreban je veliki broj ključeva
 - Informacija postoji kao otvorena na tački T2, što je nepoželjno za T1 i T3
 - Ovakav vid enkripcije je transparentan za korisnika (ne zna da li se vrši šifrovanje)
 - To su sistemi koji standardno rade 24 časa
 - Sistemi su automatski sa automatskom resinhronizacijom u radu
 - Šifrovanje se vrši nezavisnim uređajima koji praktično prekidaju vezu između dve tačke
 - Povezuju se na linijske uređaje
 - Kod svake tačke treba da postoji nezavisni uređaj za enkripciju
 - ✓ *Point to point* (tačka - tačka)
 - Princip sličan kao kod link enkripcije
 - Osnovni uređaji mreže održavaju sinhronizaciju u sistemu
 - Moduli za šifrovanje ne prekidaju vezu, već su postavljeni paralelno sa uređajima
 - Postoje različiti ključevi za pojedine deonice u mreži
 - Šifrovanje informacija na putu od A do B se otvara na tranzitnim tačkama (T2)
 - Moraju postojati nezavisni uređaji ili moduli koji se povezuju na linijske uređaje
 - ✓ *End to end* (s kraja na kraj)
 - Informacija se šifrue na celom prenosnom putu od učesnika A do B
 - Omogućava se da svaki od učesnika ima različite ključeve za drugog učesnika
 - Informacija se ne otvara na prenosnom putu

- Postupak je identičan ako na prenosnom putu postoji više tačaka T ili ih nema
 - Šifrovanje – nezavisnim uređajima
 - Uređaji enkripcije su potrebni samo negde
-
- Odnosi performansi i cena sistema
 - Informacije koje se razmenjuju u mreži sadrže podatke i heder
 - Heder sadrži informacije o rutiranju, broj poruke, izvor informacije, start stop
 - Kod link enkripcije se štiti i heder, a kod enkripcije s kraja na kraj i tačka-tačka
 - Šifrovane ili otvorene poruke se mogu mešati (informacija u hederu)
 - Maksimalno je ako se sve šifruje
 - Ako je heder otvoren omogućava se praćenje saobraćaja (*traffic analysis*)
 - Ovo se otežava ako se linija drži konstantno aktivnom
 - Link enkripcija ima prednosti ako je potrebno štititi mali broj (određen) linkova, na primer u telekomunikacijama
 - Enkripcija s kraja na kraj je pogodnija ako se zahteva veliki broj zaštićenih linkova
 - Enkripcija s kraja na kraj je cilj, jer nema otvaranja poruke
 - Privatna kriptografija, namenjena širokom krugu korisnika
 - Nadšifrovanje: enkripcija s kraja na kraj se dodatno kriptuje sistemom tačka-tačka
 - Enkripcija u realnom vremenu:
 - ✓ Brzina podataka na liniji
 - ✓ Hardverska osnova za realizaciju
 - ✓ Kompleksnost algoritma enkripcije
 - Enkripcija u *off-line* režimu:
 - ✓ Vreme obrade nije kritično
 - ✓ Mogu se koristiti dugački ključevi
 - ✓ Naknadno slanje kriptovane poruke
 - Hardverska naspram softverske realizacije
 - Npr. NASA svoje proizvode realizuje samo hardverski
 - Hardverske realizacije su brže
 - Softverske su fleksibilnije
 - Realizacija u hardveru (uređaju) obezbeđuje i fizičku zaštitu
 - VLSI čipovi za realizaciju algoritama
 - Navedeni tipovi imaju svoje prednosti i mane (ključevi, zaštita, integritet, bezbednost, transparentnost itd.)
 - Posmatra se komunikaciona mreža sa svojim tačkama i učesničkim pristupima

2.1.3. Mehanizmi za detekciju i sprečavanje upada u mrežu

Detektori upada u računarski sistem – IDS (*Intrusion Detection Systems*) koriste se za prepoznavanje indikacija nekog pokušaja upada i da upozore korisnika ili izvrše korektivne akcije. Savremeni koncept IPS (*Intrusion Prevention Systems*) sistema omogućava, pored funkcija IDS, određene vrste inteligentnih zamki za napadača (tipa ćupa meda – *hony pot*), kojima skreću njihovu pažnju i izučavaju osobenosti u cilju preventivne zaštite od sledećeg napada.

Postoje dve velike klase IDS sistema:

- Mrežni IDS ili NIDS i
- Host IDS ili HIDS.

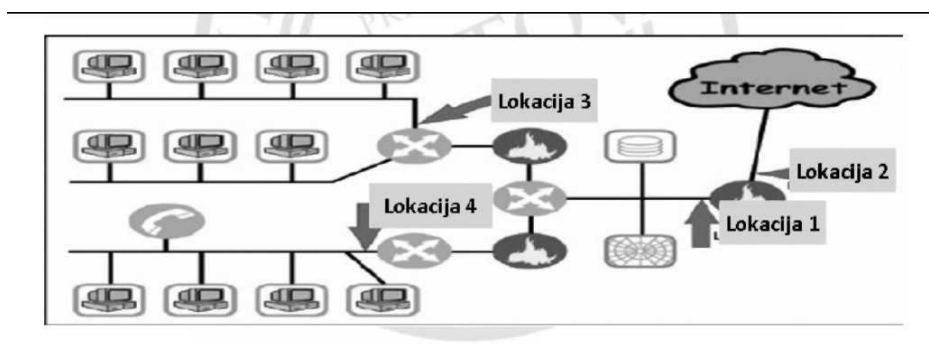
Oba sistema analiziraju podatke o događaju na znakove upada, ali se razlikuju načini na koji to rade i tipovi informacija koje procesuiraju.

IDS sistemi se, takođe, mogu klasifikovati prema principima detekcije na:

- Sisteme koji koriste tehniku detekcije na bazi potpisa i
- Složene detektore anomalija.

Prvi upoređuju log datoteku poznatih potpisa napada sa stvarnim, dok drugi traže anomalije prema obrascima koje koriste sistemi.

Mrežni sistemi za detekciju (NIDS) i sprečavanje upada (NIPS) – NIDPS, u većini slučajeva rade na 2. sloju OSI modela. Programska rešenja u NIDPS stavljaju mrežnu karticu u promiskuitetni režim rada, privilegovanu operaciju na većini NIDPS sistema, koja daje pristup mrežnom saobraćaju u realnom vremenu. Na sličan način rade i analizatori mreže i sniferski programi. NIDPS sistemi su komplementarni HIDPS sistemima po mogućnosti prijema i analize informacija, ali ne i po protokolima koji nisu na raspolaganju HIDPS sistemu. Pošto rade na mrežnom sloju, NIDPS detektuju sisteme nezavisno od operativnog sistema i omogućavaju zaštitu velikog opsega krajnjih platformi [1,31].



Slika 2.6. Mogućnosti primene NIDPS sistema u računarskoj mreži [31]

NIDPS program može igrati važnu ulogu u upravljanju malicioznim kodovima, tako što se može konfigurisati da prepozna određene potpise i preduzme neke predefinisane akcije, posebno u periodu između inicijalnog napada i raspoloživosti prve definicije malicioznog koda. NIDPS program, takođe, može biti konfigurisan da sprečava prolaz inficiranih objekata izvan organizacije, što je koristan mehanizam za sprečavanje širenja malicioznih programa na druge hostove izvan organizacije. Odgovor NIDPS sistema može biti identifikacija i logovanje događaja, neka aktivna protivmera ili kombinacija ove dve. Pasivna tehnika upozoravanja uključuje izveštavanje o problemu na ekranu monitora, generisanje SNMP (*Simple Network Management protocol*) alarma, aktiviranje mobilnog telefona i sl. Aktivne mere zaštite treba pažljivo implementirati, pošto mogu izazvati prekid servisa posebno u slučaju lažnih pozitiva, jer ukidaju konekcije u interakciji sa barijerom.

2.1.4. Mehanizmi za upravljanje log datotekama

Mehanizmi za upravljanje log datotekama koriste se da obezbede selektivan pristup log datotekama kontrolnih tragova bezbednosno relevantnih događaja. U okruženju sa različitim platformama, ovi mehanizmi pomažu osetljivi proces skupljanja i kombinovanja login informacija sa različitih platformi, što omogućava administratoru da prati napade ili sumnjive događaje koji pogađaju više od jednog hosta. Pošto većina savremenih

operativnih sistema obezbeđuje log informacije, mehanizmi za upravljanje log datotekama koriste se za obezbeđenje zaštite svim slojevima softvera u računarskom sistemu.

Izvlačenje relevantnih podataka iz kontrolnih log datoteka u srednjim i velikim organizacijama, veoma je složen i vremenski zahtevan posao. Obično nije problem samo skupljanje informacija, mada dobro treba razmisliti koje događaje upisivati u log datoteke za svaku datu aplikaciju. Pod pretpostavkom da je ovo učinjeno korektno, postoje brojni problemi za korišćenje informacija sadržanih u log datotekama:

- Obično postoji veliki obim podataka koje treba analizirati;
- Zahtevana su jasna pravila koja indiciraju koje podatke treba analizirati proaktivno, a koji podaci se analiziraju reaktivno, samo kao odgovor na sumnjiv incident;
- Zahteva se smeštanje informacija kontrolnih tragova u kontekstu brojnih platform da bi se pratile sumnjive aktivnosti koje se šire kroz mrežu.

Mehanizmi za upravljanje log datotekama smanjuju problem obima podataka kontrolnih tragova, obezbeđujući filtriranje podataka, na osnovu implementiranog skupa pravila za selekciju podskupa podataka izvan skupa podataka od interesa. Nedostaci filtracije log podataka su višestruki:

- a) Neke važne informacije mogu se potpuno odstraniti tako da ne učestvuju u analizi.
- b) Kako se podaci istog tipa predstavljaju na različitim platformama, mehanizmi za upravljanje log datotekama moraju biti dovoljno inteligentni da ih prepoznaju. Idealno bi bila standardizacija reprezentacije kontrolnih tragova (što je i cilj *COAST Audit Trail Reduction Group-e*), što bi omogućilo administratorima da vrše analizu, a ne da interpretiraju sirove podatke.
- c) Potrebno je da se log datotekama označavaju tragovi koji su namenjeni za proaktivnu ili reaktivnu analizu.
- d) U većini sistema vreme časovnika različitih platformi samo je približno sinhronizovano. Postoje protokoli za automatsku sinhronizaciju časovnika na različitim platformama, ali oni nisu uvek implementirani u mrežama. Problem sinhronizacije časovnika može uticati na procese konsolidacije hronologije napada, kao i na podatke prezentirane filterima log podataka.

Većina savremenih rešenja samo delimično rešava ove probleme. Većina alata za analizu log datoteka web lokacija danas su sofisticirani i složeni, ali nisu usmereni na bezbednosne događaje, nego na informacije koje se odnose na posete klijenata lokaciji.

2.1.5. Proaktivna digitalna forenzika

Savremeni proaktivni sistemi za detekciju i sprečavanje upada u sistem, kao što je u gore navedenom tekstu obrađeno, obezbeđuju inteligentnu tehniku za hvatanje napadača poznatu kao ćup meda (*honeypot*). Ove tehnike omogućavaju „zarobljavanje“ hakera u napadnutom sistemu, nakon utvrđivanja njegovog prisustva.

Sada ćemo da predložimo korišćenje virtualizovanog računarskog okruženja za potrebe eliminisanja štete nastale u fazi incidenta i obezbeđivanja podataka potrebnih za proces digitalne forenzičke analize. Proaktivna digitalna forenzika (ProDF) predstavlja proširenje standardne forenzičke istrage čiji je osnovni cilj da se organizacija pripremi za digitalnu forenzičku istragu (internu ili kriminalnu) a u našem slučaju za testiranje otpornosti sistema na napad, i to pre nego što se napad dogodi.

Proaktivna digitalna forenzička istraga (ProDF) obezbeđuje neophodne procese, procedure, tehnologije i sveobuhvatne digitalne dokaze. Neophodno je razmotriti sledeće ciljeve proaktivne digitalne forenzičke istrage:

1. Spremnost za digitalnu forenzičku istragu
2. Poboljšanje upravljačke strukture IT i *Information Security* u organizacijama
3. Poboljšanje Info Sec/IT performansi sa korišćenjem odgovarajućih alata digitalne forenzike za poboljšanje efektivnosti i efikasnosti u organizaciji.

2.1.5.1. Virtualno računarsko okruženje

Savremene virtualizacione tehnologije omogućavaju kreiranje kompletnog virtualnog umreženog računarskog okruženja na standardnim računarskim platformama. Koncept virtualnih mašina omogućava izvršavanje više nemodifikovanih operativnih sistema na jednom računaru, a noseći softver za virtualizaciju omogućava umreženje virtualnih mašina različitim topologijama.

Pored ušteda na hardveru, u osnovne prednosti virtualnih računarskih okruženja spadaju fleksibilnost, skalabilnost i brz oporavak sistema. Virtualizovana računarska okruženja mogu se jednostavno povezati sa realnim računarskim okruženjem organizacije, u ovom slučaju ZU Apoteka Vranje. Ova karakteristika je veoma značajna jer omogućava migriranje napada sa realnog na virtualno računarsko okruženje. Tačka u kojoj će se migracija izvršiti trebala bi da bude *firewall* sistem kroz koji napadač pokušava da pristupi realnom okruženju organizacije. Odluka o preusmeravanju napadača u virtualno okruženje samo je posledica uspešnog prepoznavanja da je u pitanju napad a ne regularan mrežni saobraćaj. Ona se može doneti na osnovu zaključka IDS/IPS sistema ali su mogući i jednostavniji koncepti.

Kritičnu tačku predloženog sistema čini ruter odnosno IDS/IPS sistem. Ovaj sistem ima zadatak da na osnovu dostupnih parametara zahteva sa spoljne mreže utvrdi da je u pitanju napad a ne regularan zahtev. U situaciji ZU Apoteka Vranje gde imamo rad sa protokolima namenjenim za udaljenu administraciju računara (*Remote Desktop*, SSH i sl.) veoma lako se mogu dovesti u sumnju zahtevi za ove i druge protokole koji se izvršavaju na serveru u realnoj internoj mreži organizacije. S druge strane, u opisanoj situaciji i zahtevi pod HTTP protokolom mogu se preusmeriti u virtualizovano računarsko okruženje, i to upravo ka virtualizovanim instancama web servera na kojima su namerno napravljeni bezbednosni propusti (koji odgovaraju identifikovanim tipovima napada) sa svrhom da prikupljaju podatke o cilju, izvoru i karakteristikama napada. Uspešno prepoznavanje napada i preusmeravanje napadača u virtualno okruženje predstavlja izolovanje potencijalne faze incidenta.

Značajno pitanje odnosi se na bezbednosne politike vezane za upravljanje virtualnim okruženjem. Tim dokumentima moraju se jasno definisati, pre svega sledeći aspekti primene predloženog rešenja:

- Proces i nadležnost u uspostavljanju virtualnog okruženja
- Segmenti i stepen poklapanja virtualnog okruženja sa realnim
- Setovi i ažurnost podataka koji se kopiraju u virtualno okruženje

Pravilnim razvojem bezbednosnih politika koje se odnose na upravljanje virtualnim okruženjem, i njihovom adekvatnom primenom, doprinosi se postizanju cilja – izolovanje faze incidenta, eliminisanje štete koja je u njoj izazvana, i prikupljanje adekvatnih podataka za potrebe digitalne forenzičke analize.

2.1.5.2. Funkcionalni model proaktivne zaštite

Metod proaktivne zaštite obuhvata mehanizme zaštite na više nivoa, sa različitim brzinama reakcije i tačnosti, sa većom ukupnom efikasnošću, redukovanim operativnim rizikom i znatno nižim troškovima razvoja, rada i održavanja. Koncept sistema DPP zaštite nudi novi proaktivni pristup, u kojem se zaštita realizuje kombinacijom baza znanja, vrhunske tehnologije za proaktivnu zaštitu, procesnog pristupa i pojednostavljenog rešenja sistema zaštite. [35,22,24]

Baze znanja vodećih obaveštajnih mreža CIRT i CERT prikupljaju podatke o pretnjama i ranjivostima sistema i obezbeđuju ažuran bilten podataka (*X-Press Updates*) u kojem se objavljuje oko 45% ranjivosti aktuelnih sistemskih programa u svetu ili 3 puta više od ostalih.

Vrhunska tehnologija višeslojne proaktivne zaštite obezbeđuje automatizaciju ciklusa zaštite sa elementima ekspertnih sistema, a tipično obuhvata [22,24] :

- Uređaj za zaštitu (*Protection Engine*) koji sadrži IDPS i Modul za reagovanje na incidente i obezbeđuje nelinearnu zaštitu i upravlja sa IDPS,
- Uređaj za zaštitu lokacije (*Site Protector*) koji obezbeđuje komande i centralizovano upravlja događajima i mehanizmima zaštite u računarskim mrežama i računarskim sistemima,
- Integrator sistema (*Fusion System*) koji vrši obradu signala, obezbeđuje prepoznavanje obrazaca i analizira uticaje DPP napada,
- Modul za ažuriranje (*X-Press Updater*), koji automatski ažurira bazu podataka sa podacima CERT/CIRT timova.

DPP Protection Engine obezbeđuje realizaciju mehanizama DPP zaštite, a ugrađuje se u sva rešenja IBM ISS kao što su: skeneri sistema zaštite, IDPS (tipa *RealSecure 10/100*, *RealSecure Gigabit Network*, *realSecure_Nokia*, *RealSecure_Crossbeam*, *PreventiaA...*), softversko-hardverski sistemi za sprečavanje napada (*PreventiaG*), višefunkcionalni uređaji za zaštitu (*PreventiaM*), IDPS servera (*Real Secure server*) i IDPS radne stanice (*Real Secure Desktop*) [22,24]

Procesni pristup zaštiti i pojednostavljeni proces zaštite, bitne su komponente koncepta proaktivne DPP zaštite. Borba protiv nepoznatih pretnji zahteva brzo reagovanje na tek otkrivenu iskoristivu ranjivost, pre nego je neka pretnja iskoristi. Rešenja DPP zaštite koriste jedinstveni mehanizam „virtuelne zakrpe“ (*Virtual Patch*) za automatsko fiksiranje poznatih i potencijalnih ranjivosti sistema. Na primer *Ibm/ISS Preventia* radi tako što obezbeđuje privremeni zaklon ili „virtuelne bezbednosne popravke“ za zaštitu u nultom danu; sprečavaju iskorišćenje ranjivosti od poznatih i nepoznatih pretnji; ne oslanjaju se na definicije AVP, eliminišu potrebu bitnih popravki, otklanjaju rizik štete od popravki i omogućavaju primenu popravki u toku održavanja sistema i uobičajenih napada.

Ovaj mehanizam omogućava organizaciju da trenutno, u realnom vremenu, zaštititi sistem od poznatih i nepoznatih napada, često znatno ranije od zvaničnog generisanja i objavljivanja popravki za nivo ranjivosti sistema.

Proces proaktivne zaštite počinje sa trenutkom otkrivanja/objavljivanja ranjivosti sistema. Zatim sledi generisanje napada, koji može iskoristiti otkrivenu ranjivost sistema, ali obavezno ne mora. Konačno, generiše se i aplicira nova bezbednosna popravka za otklanjanje ove iskoristive ranjivosti. Iako je vreme od otkrivanja do iskorišćenja ranjivosti promenljivo, popravka se često aplicira tek kada je šteta već naneta, zbog *potrebnog vremena za manuelnu popravku distribuiranih ranjivosti, raspoloživosti popravki za nove ranjivosti, tek kada su ranjivosti iskorišćene i sve kraćeg vremena između otkrivanja ranjivosti i njenog iskorišćenja.*

U vremenu od otkrivanja do iskorišćenja ranjivosti, nalazi se prozor proaktivne zaštite. U tački otkrivanja ranjivosti sistema aktivira se *Virtual Patch* proces, aktivira sistem za proaktivnu zaštitu i obezbeđuje zaštitu i bez poznavanja informacije o iskoristivosti te ranjivosti, koja se može generisati znatno kasnije. Dakle, zonu proaktivne zaštite od DPP obezbeđuje *Virtual Patch* proces, koji štiti sistem od nepoznatih pretnji. U stvari, proaktivna zona zaštite proteže se i na zonu pre otkrivanja ranjivosti sistema, što omogućavaju stalni procesi istraživanja i dubokog razumevanja prirode ranjivosti IKTS, sistem ranog upozorenja o otkrivenim ranjivostima (ISS – obično 30 dana pre javnog otkrivanja, a 24 sata ranije od drugih entiteta) i sistem automatskog ažuriranja bezbednosno relevantnih informacija, dobijenih od istraživačkog CERT tima.

Dakle, *Virtual Patch* proces obezbeđuje rezervno vreme do pojave dovoljno ažurne bezbednosne popravke, koja ne zahteva individualno krpljenje i manuelno restartovanje sistema; redefiniše bezbednost sistema tako da se operacije zaštite izvršavaju kao deo normalnog procesa upravljanja promenama IKTS, što omogućava mnogo efektivnije i efikasnije planiranje resursa i brže reagovanje na poznate i nepoznate pretnje.

Proaktivni sistem zaštite, u poređenju sa reaktivnim, postiže rentabilnije vreme analize i upravljanja rizikom, veću tačnost i brzinu otkrivanja i bolje sprečavanje napada. Kako pretnje i ranjivosti rastu, sistem zaštite mora biti brži, precizniji i pouzdaniji. Napadačima je za efektivan napad dovoljna margina greške od svega 1%. Centralna platforma za DPP zaštitu, obezbeđuje znatno bolju zaštitu cele računarske mreže i smanjuje kompleksnost, eliminiše lažne alarme, znatno smanjuje ukupne troškove zaštite i približava se *optimalnom sistemu zaštite*.

Proaktivni sistem zaštite zadovoljava zahteve savremenih trendova zaštite virtuelizovanog okruženja u distribuiranom internet računarstvu (*Cloud computing* - CC), mreža u razvoju, mobilnih uređaja, senzorskih sistema za fizičku zaštitu, alternativnih puteva isporuke mehanizama zaštite, upravljanja rizikom i identitetom [22].

2.1.6. Kompjuterski događaj i kompjuterski incident

Kompjuterski događaj je bilo koje uočljivo dešavanje i sistemski događaj, registrovan u log datoteci u računarskom sistemu ili računarskoj mreži. Kompjuterski incident je događaj sa negativnim posledicama (pad računarskog sistema, zagušenje saobraćaja računarske mreže, eskalacija privilegija i sl.). Upravljanje kompjuterskim incidentom obuhvata sve događaje štetne za bezbednost IKTS. Definicija kompjuterskog incidenta je evoluirala od “bezbednosno relevantnog događaja koji dovodi do gubitka CIA informacija”, do definicije u Internet okruženju – “povreda ili immanentna pretnja za povredu i/ili primenu politike zaštite” [23].

Politika za upravljanje kompjuterskim incidentom, internim ili iznajmljenim kapacitetima, u većini organizacija obuhvata iste ključne elemente: izjavu menadžera o angažovanju; namenu i ciljeve; obim i granice; identifikaciju prirode kompjuterskog incidenta i posledica u kontekstu organizacije; strukturu, uloge i odgovornost interventnog tima; način i formu izveštavanja; prioritete saniranja i metriku performansi kapaciteta za upravljanje kompjuterskim incidentom.

Najčešća podela (koja nije konačna) je, na bazi primarnih kategorija napada, na posledice: odbijanje izvršavanja servisa, napada malicioznih programa, neovlašćenog pristupa, nepropisnog korišćenja IKTS i kombinovanih napada. Neki kompjuterski incidenti mogu se svrstati u više od jedne kategorije. Ova podela je pre osnovno uputstvo za upravljanje kompjuterskim incidentom.

Glavni problem upravljanja kompjuterskim incidentom je donošenje odluke da se incident dogodio, kojeg je tipa i inteziteta i kolika je šteta? Problem je tim teži, što

kompjuterski incident tipično čini kombinacija raznih faktora (kompjuterski incidenti mogu detektovati razna tehnička sredstva sa različitim nivoima tačnosti/pouzdanosti, brojni su potencijalni znaci da se kompjuterski incident dogodio itd.) i potrebno je specifično tehničko znanje i veliko iskustvo za analizu nagoveštaja – predznaka i indikatora kompjuterskog incidenta.

2.1.6.1. Politike i procedure za upravljanje incidentom

Politika upravljanja incidentom u većini organizacija obuhvata iste ključne elemente, bez obzira da li su kapaciteti za upravljanje incidentom interni ili iznajmljeni:

- Izjava menadžmenta o angažovanju,
- Namena i ciljevi politike,
- Obim i granice politike,
- Identifikacija incidenta i njegove posledice u kontekstu organizacije,
- Definisanje organizacione strukture uloga i odgovornosti interventnog tima,
- Zahtev za izveštavanje o određenim tipovima incidenata,
- Prioriteti ili rangiranje težine incidenta,
- Merenje performansi kapaciteta za upravljanje incidentom,
- Način i forma izveštavanja.

Procedure za upravljanje incidentom u formi Standardne operative procedure (SOP), zasnivaju se na Politici upravljanja incidentom i detaljno objašnjavaju specifične aktivnosti tehničkih procesa, tehnike, ček liste i formulare, koje koristi interventni tim. Treba da budu sveobuhvatne i dovoljno detaljne da obezbede prioritetne akcije interventnog tima i smanje greške zbog tempa i pritiska koji prate tipičan proces reagovanja na incident.

2.1.6.2. Kategorije bezbednosnog kompjuterskog incidenta

Incident se može dogoditi na bezbroj načina, pa nije praktično razvijati sveobuhvatne korak-po-korak procedure sa instrukcijama za upravljanje incidentom. Generalno organizacija se može pripremiti sa bilo kojim tipom incidenta, a specifično sa prepoznatljivim tipovima incidenta. U interesnoj zajednici zaštite još uvek nema konsenzusa o najboljoj taksonometriji kompjuterskog incidenta. Među brojnim podelama, korisna je kategorizacija na bazi primarnih kategorija napada, koja nije sveobuhvatna ni definitivna, nego pre osnovno uputstvo za upravljanje incidentom:

- a) Odbijanje izvršavanje servisa (DoS), napadi koji iscrpljuju resurse i sprečavaju ili slabe kvalitet ovlašćenog korišćenja sistema;
- b) Maliciozni kodovi (virusi, crvi, Trojanci i dr.), koje proizvode maliciozni entiteti da inficiraju neki host;
- c) Neovlašćeni pristup, logički ili fizički, nekom objektu IS;
- d) Nepropisno korišćenje usvojene politike prihvatljivog korišćenja IKT sistema;
- e) Kombinovani napad obuhvata dva ili više faktora pretnji koji izazivaju incident.

Neki incidenti mogu se svrstati u više od jedne kategorije, pa interventni tim treba da izvrši dodatnu kategorizaciju (npr., prema mehanizmu prenosa Trojanac za neovlašćeni pristup je kombinovani incident jer se koriste dva prenosna mehanizma) [23,34].

2.1.6.3. Nagoveštaji kompjuterskog incidenta

Najveći izazov u procesu upravljanja incidentom je pouzdano donošenje odluke da li se incident dogodio i, ako jeste, kojeg je tipa i inteziteta i kolika je veličina problema. Ovaj problem je još teži, jer ga tipično čini kombinacija sledeća tri faktora:

- Incidente mogu detektovati razna sredstva sa različitim nivoima tačnosti i pouzdanosti: mrežni i host IDS/IPS sistemi, antivirusni programi i analizatori log datoteka i izveštaji korisnika o problemu
- Potencijalni znaci da se incident dogodio brojni su (napadač koji skenira 10 web servera može generisati nekoliko hiljada IDS alarma)
- Potrebno je specijalističko tehničko znanje i veliko iskustvo za propisnu i efikasnu analizu podataka koji se odnose na incidente.

Nagoveštaji nekog incidenta spadaju u jednu od dve kategorije: predznaci i indikatori [18].

Predznak je nagoveštaj da se neki incident može dogoditi u bliskoj budućnosti. Na primer, IDS senzor može detektovati neobičnu aktivnost skeniranja porta usmerenu na grupu hostova, koja se dešava neposredno pred DoS napad na hostove. Predznaci incidenta mogu biti: log datoteka u web serveru pokazuje korišćenje skenera ranjivosti Web servera, najavljena nova iskoristivost koja pogađa ranjivost mail servera organizacije i pretnja grupe hakera da će napasti organizaciju itd.

Naravno, svaki napad se ne može detektovati kroz predznake. Neki napadi nemaju predznake, dok drugi generišu predznake koje organizacija ne uspeva detektovati. Ako se predznaci detektuju, organizacija ima priliku da izmeni sistem zaštite i ručno ili automatski spreči napad na objekat IKT sistema.

Indikator je znak da se neki incident vrlo verovatno dogodio, ili se upravo događa. Postoji više tipova indikatora incidenta, a tipični primeri su:

- Mrežni IDS alarmira kada je neki bafer preplavljen pokušajima napada na FTP server,
- Antivirusni program alarmira kada detektuje da je host inficiran sa nekim crvom
- Pad web servera,
- Korisnici se žale na spor pristup hostu na Internetu,
- Korisnik naziva kol centar da prijavi preteću e-mail poruku,
- Host registruje promenu auditing konfiguracije u svojoj log datoteci,
- Aplikacija loguje više propalih pokušaja pristupa udaljenog nepoznatog korisnika,
- E-mail administrator vidi veliki broj povezanih e-mail-ova sa sumnjivim sadržajem,
- Administrator mreže uočava neobična odstupanja od tipičnog mrežnog toka itd.

Predznaci i indikatori incidenta identifikuju se korišćenjem više različitih izvora, od kojih su najčešći softverski alarmi zaštite računara, log datoteke, javno raspoložive informacije i ljudi. U tabeli 2.2. prikazani su najčešći izvori indikatora i predznaka kompjuterskih incidenata za svaku kategoriju incidenata.

Tabela 2.2. Uobičajeni izvori predznaka incidenta i indikacije

Prethodnica ili izvor indikacija	Opis
Informacije o računarskom bezbednosnom softveru	
Mrežni i bazni IDS	IDS proizvodi su dizajnirani tako da identifikuju sumnjive događaje i relevantne podatke u vezi sa njima, uključujući i podatke o vremenu kada je napad otkriven, tip napada, izvor i određenu IP adresu kao i korisničko ime (ako je primenljivo i poznato). Većina IDS proizvoda koristi niz napada koji identifikuju zlonamerne aktivnosti, a potpisi su dizajnirani tako da mogu detektovati i najnovije napade. IDS softver često proizvodi lažna upozorenja koja ukazuju na dešavanje zlonamernih aktivnosti, kada ih u stvari i nema. Analitičari treba ručno da potvrde IDS upozorenja bilo bliskim pregledom snimljenih podataka praćenja ili dobijanjem podataka iz drugih izvora.
Antivirusni softver	Kada se otkrije zlonamerni kod, antivirusni softver obično šalje upozorenje domaćinu i centralizovanoj antivirusnoj konzoli. Trenutni antivirusni proizvodi su veoma efikasni u otkrivanju i otklanjanju ili izolovanju zlonamernih kodova a njihovi potpisi se čuvaju do danas. Ovakvo ažuriranje može biti nepogodno za velike organizacije. Jedan od načina da se to prevaziđe jeste konfigurisanje centralizovanog antivirusnog softvera gde svaki domaćin (host) povlači ispravke (<i>updating-e</i>). Zbog variranja antivirusnih proizvoda, neke organizacije koriste proizvode od više proizvođača kako bi obezbedili bolju pokrivenost i veću preciznost. Antivirusni softver treba da bude raspoređen na najmanje dva nivoa: na obodu mreže (<i>firewall</i> , e-mail serveri) i na nivou domaćina (radne stanice, file serveri, klijent softvera).
Datoteka provere integriteta softvera	Incident može izazvati promenu važnih datoteka; softver može da otkrije takvu promenu. Provera radi po principu usitnjavanja algoritama i dobijanja kriptografske kontrolne sume za svaki određeni fajl. Ako je fajl promenjen, postoji izuzetno velika verovatnoća da novoj kontroli neće odgovarati stara kontrolna suma. Redovnim izračunavanjem kontrolne sume i upoređivanjem sa prethodnim vrednostima mogu se detektovati izmene datoteke.
Treća strana monitoring servisa	Neke organizacije plaćaju treću stranu kako bi pratili dostupnost svojih usluga kao što su Web, DNS i FTP serveri. Treća strana automatski pokušava da pristupi svakom servisu svakih X minuta. Ako se ne može pristupiti servisu, treća strana upozorava organizaciju putem telefona, upozorenja na web stranicama ili e-mailovima. Neki servisi za praćenje takođe mogu da otkriju i upozoravaju o promenama u određenim resursima – na primer web stranicama. Iako je praćenje servisa uglavnom korisno sa operativnog stanovišta što takođe može da obezbedi indikaciju DoS napada ili kompromis servera.
Zapisi	
operativni sistem, usluga i aplikacija za logovanje	Zapisi iz operativnih sistema, usluga i aplikacija (posebno u vezi revizije podataka) često su od velikog značaja kada se desi incident. Zapisi mogu da obezbede bogatstvo informacija, kao što su pristupni računi i izvršene radnje. Nažalost, u mnogim slučajevima logovanja ne sadrže nikakve dokaze, jer je evidentiranje ili onemogućeno ili nepravilno podešeno kod domaćina. Da bi se olakšalo efikasno upravljanje incidentom, organizacije

	treba da zahtevaju osnovni nivo logovanja na svim sistemima, kao i veći nivo evidentiranja na kritičnim sistemima. Svi sistemi treba da uključe reviziju i da prijavljuju događaje reviziji, posebno administrativni nivo aktivnosti. Svi sistemi treba da periodično proveravaju da li ispravno funkcioniše evidentiranje (logovanje) i pridržavaju se standarda evidentiranja.
Mrežni uređaj za logovanje	Zapisi iz mrežnih uređaja kao što su <i>firewall</i> i ruteri se obično ne koriste kao primarni izvor indikacije. Iako su ovi uređaji obično konfigurisani da prikažu i blokirane pokušaje logovanja, pružaju malo informacija o prirodi aktivnosti. Ipak, oni mogu biti korisni u identifikovanju trendova (kada je znatno povećan broj pokušaja pristupa određenim portovima) kao i korelaciju događaja detektovanu drugim uređajima.
zamke logovanja	Neke organizacije se bave otkrivanjem incidenata koji su raspoređeni kao zamke za aktivne napadače, tako da mogu da prikupe bolje podatke o predznacima incidenata. <i>Honeypots</i> su domaćini koji nemaju ovlašćene korisnike, drugačiji su od zamke administratora jer nemaju poslovnu funkciju; sve aktivnosti usmerene ka njima smatraju se sumnjivim. Napadači će da skeniraju i napadaju zamke za aktivne napadače, dajući administratoru podatke o novim trendovima i alatima napada, naročito zlonamerni kod. Međutim, zamka za aktivnog napadača je dodatak a ne zamena za pravilno obezbeđivanje mreže, sistema i aplikacija. Ako <i>honeypots</i> treba da koristi organizacija detekcijom upada treba da upravljaju analitičari. Zakonitost <i>honeypotsa</i> nije jasno uspostavljena, dakle organizacija treba pažljivo da prouči pravne posledice pre planiranja bilo kakve zamke raspoređivanja.
Javno dostupne informacije	
Informacije o novim ranjivostima i eksploataciji	U korak sa novim tehnologijama ide i osavremenjavanje otkrivanja incidenata i analizom novih napada. Neke organizacije kao što su FedCIRT, CERT, IAIP periodično pružaju informacije o pretnjama ažuriranjem putem brifinga, web poruka i mailing lista.
Informacije o incidentima kod drugih organizacija	Izveštaji o incidentima koji su se dogodili drugim organizacijama može pružiti obilje informacija. Postoje web sajtovi i mejling liste, gde timovi za odgovaranje na incident i bezbednosni profesionalci mogu da dele informacije i izvođenju i napadima koje su videli. Pored toga, neke organizacije stiču, konsoliduju i analiziraju dnevnike i upozorenja za otkrivanje napada kod mnogih drugih organizacija.
Ljudi	
Ljudi iz okvira organizacije	Korisnici, sistem administratori, mrežni administratori, bezbednosno osoblje i mnogi drugi iz organizacije mogu prijaviti znakove incidenta. Važno je da se provere svi takvi izveštaji. Ne samo da korisnici uglavnom nemaju saznanja da utvrde da li se neki incident dešava, nego čak i najbolje obučeni tehnički stručnjaci greše. Jedan način je da pitate ljude koji daju takvu informaciju kako su oni uvereni da je ta informacija tačna. Snimanjem ove procene zajedno sa informacijama koje mogu da značajno pomognu tokom analize incidenta, mogu da otkriju konfliktni podaci.
Ljudi iz drugih organizacija	Iako neki izveštaji o incidentima potiču od ljudi iz drugih organizacija, treba ih shvatiti veoma ozbiljno. Klasičan primer je haker koji identifikuje ozbiljnu ranjivost u sistemu i obaveštava organizaciju bilo direktno ili javnim najavljivanjem problema. Druga mogućnost je da organizacija može biti kontaktirana izvana sa tvrdnjom da ima napad. Spoljni saradnici takođe

	moгу prijaviti i druge pokazatelje kao što je oštećena web stranica ili nedostupna usluga. Važno je da imate mehanizme koji prate indikatore sa spoljne strane kao i obučeno osoblje koje pažljivo prati ove mehanizme, a to može biti jednostavno kao postavljanje broja telefona i e-mail adrese.
--	--

2.1.6.4. Upravljanje kompjuterskim incidentom

Cilj upravljanja kompjuterskim incidentom je, da se ograniči mogućnost upada u sistem kroz preventivnu zaštitu, testiranje otpornosti sistema na proboj, skeniranje ranjivosti sistema i IDPS, kao i da se obezbedi lakši istražni postupak kada se incident dogodi. Životni ciklus upravljanja kompjuterskim incidentom tipično ima četiri faze [18,23,34] :

1. **Pripremna faza** – u ovoj fazi se preduzimaju preventivne mere za sprečavanje incidenta, obezbeđenje adekvatnog sistema zaštite i uspostavljanje interventnog tima – CIRT kao i pripreme za brzo reagovanje na incident. Primarni ciljevi razvoja kapaciteta za upravljanje kompjuterskim incidentom su: (1) reagovanje na kompjuterski incident, (2) saniranje štete i (3) oporavak sistema. Kapaciteti za upravljanje kompjuterskim incidentom, moraju biti preventivno implementirani i spremni da po potrebi obezbede: brzo reagovanje, koordinaciju aktivnosti tima, izveštavanje o kompjuterskim incidentu, oporavak sistema i sprečavanje ili minimizaciju potencijalne štete. Podaci o kompjuterskom incidentu i korektivnim akcijama se skupljaju i skladište u bazu podataka i analiziraju za formiranje obrazaca ponašanja – profi KI. Proaktivni sistemi zaštite obezbeđuju efikasnu i efektivnu zaštitu od poznatih, ali i nepoznatih dinamički promenljivih pretnji, znatno uspešnije od postojećih reaktivnih sistema zaštite i rentabilniji su od oporavka sistema i otklanjanja štete.

Iako nije odgovoran za sprečavanje kompjuterskog incidenta, CIRT čini glavnu komponentu kapaciteta za upravljanje incidentom. Ekspertska znanja članova tima dragocena su za poboljšanje sistema zaštite i dokazivanje zloupotrebe ili kompjuterskog kriminala. Modeli struktura CIRT za upravljanje kompjuterskim incidentom mogu se svrstati u tri kategorije [25,28]:

- Centralni CIRT, koji upravlja kompjuterskim incidentom u celoj organizaciji, efikasan je za male i veće organizacije sa malom distribucijom objekata IKTS;
- Distribuirani CIRT, koji upravlja kompjuterskim incidentom u logičnim ili fizičkim segmentima organizacije, kao deo jednog entiteta i procesa upravljanja;
- Koordinacioni CIRT, koji savetodavno vodi rad drugog tima.

Dobri kapaciteti za upravljanje kompjuterskim incidentom treba da poseduju nekoliko ključnih karakteristika: razumevanje obima i granica procesa upravljanja i upotrebe kapaciteta, obrazovnu komponentu, sredstava za centralizovano upravljanje (komunikaciju i izveštavanje), specijaliste za primenjene tehnologije i dobre veze sa entitetima koji mogu pomoći u upravljanju kompjuterskim incidentom.

Obim i granice upotrebe kapaciteta za upravljanje kompjuterskim incidentom ne obuhvataju uvek celu organizaciju. Kapaciteti za upravljanje kompjuterskim incidentom obuhvataju tehnologiju, korisnike IKTS i menadžere. Obuka korisnika ima za cilj da se smanji kompleksnost, poveća korisnička prihvatljivost i obezbedi izveštavanje po prioritetima. Centralizovano upravljanje obezbeđuje efikasno i efektivno upravljanje kompjuterskim incidentom, a uspeh zavisi od blagovremenog

izveštavanja. Ako je kompjuterski incident hakerski napad, treba koristiti kriptozštićen sistem za izveštavanje, analizu i čuvanje informacija o identitetu. Tehnologija za upravljanje kompjuterskim incidentom treba da uključuje i specifične forezničke alate od kojih su mnogi raspoloživi na Internetu. Većina interventnih timova formira prenosivi komplet za istragu kompjuterskog incidenta, u kojem se nalazi većina alata [18].

2. **Faza detekcije i analize incidenta** – u ovoj fazi se kao osnovni alati koriste IDPS sistemi za detekciju i sprečavanje povrede sistema zaštite. Preventivni alati obavljaju inicijalnu evaluaciju konfiguracije sistema dok detektorski alati obezbeđuju kontrolu svake neregularne promene stanja u sistemu. Primeri takvih alata su brojni: *Intruder Alert* (ITA), *AXENT Technologies* – detektor napada na platformu, *RealSecure*, ISS – detektor za napade na komunikacije itd. Ovakvi alati prikupljaju informacije o napadu i napadaču, koje su korisne za forezničku istragu i analizu. Dobro upravljanje upadom u IKTS, preventiva je svih potencijalnih problema i omogućava pokretanje istrage o kompjuterskim incidentu. Detekcija i analiza incidenta mogu uvek biti predznaci ili indikatori pojave incidenta, ako su precizni, što nažalost nije uvek slučaj. Međutim, IDPS sistemi proizvode veliki broj lažnih pozitivnih alarma, pa ne znači da se kompjuterski incident dogodio, čak i kada je neki indikator tačan.

Za efektivno upravljanje kompjuterskim incidentom preporučuje se proces korporacijske digitalne forenzičke istrage kompjuterskog incidenta, koji obuhvata faze pripreme i podnošenja zahteva za istragu, akviziciju digitalnih dokaza, identifikaciju incidenta i napadača i forenzičko čuvanje i rukovanje digitalnim dokazima [18].

3. **Faza saniranja posledica kompjuterskog incidenta i oporavak sistema** – ova faza uključuje razvoj metoda za saniranje posledica, najmanje od svih tipova glavnih kategorija kompjuterskog incidenta. Za brže odlučivanje treba dokumentovati kriterijume za određivanje metoda za saniranje kompjuterskog incidenta, koji uključuju:

- potencijalna oštećenja i krađu objekata informacione imovine,
- obavezu čuvanja dokaza za forenzičku analizu i veštačenje,
- raspoloživost servisa,
- vreme i resurse potrebne za implementaciju strategije,
- efektivnost strategije (npr. sanira delimično ili potpuno) i
- vreme trajanja rešenja.

U fazi oporavka, treba eliminisati preostale komponente kompjuterskog incidenta, izbrisati maliciozne kodove i deaktivirati probijene korisničke naloge. Faza oporavka može uključiti: restauraciju sistema iz bekapa, zamenu kompromitovanih datoteka, instalaciju popravki, izmenu lozinki i povećanje zaštite perimetra računarske mreže, rekonfigurisanje sistema logovanja ili monitoringa računarske mreže i forenzičku analizu digitalnih podataka za otklanjanje pravog uzroka kompjuterskog incidenta.

4. **Faza analize iskustva** – iako je ovo najvažnija faza procesa upravljanja kompjuterskim incidentom, često se zanemaruje, a uključuje: tip i vreme kompjuterskog incidenta, ponašanje menadžmenta i zaposlenih, dokumentaciju i adekvatnost procedura, potrebne informacije po izbijanju kompjuterskog incidenta, preduzete akcije za sprečavanje i oporavak, iskustva za rad i korektivne akcije za sprečavanje budućeg, sličnog kompjuterskog incidenta i potrebne resurse za detekciju, analizu i saniranje novog kompjuterskog incidenta. Mali incidenti ne zahtevaju posebnu analizu u ovoj fazi, osim ako ne otkrivaju nepoznati metod

napada. Ako se dogodi ozbiljan napad, uvek je korisno izvršiti detaljnu multidisciplinarnu analizu [18].

Kompletiran izveštaj o analizi kompjuterskog incidenta treba koristiti za obuku, ažuriranje politike i dokumenata, popravku procedura, izradu pojedinačnih analitičkih izveštaja, izradu hronologije događaja iz log datoteka za dokazni postupak itd. Na bazi normativnih zahteva, prethodnih izveštaja i očekivanja od sakupljenih podataka, organizacija odlučuje, koji se podaci o kompjuterskom incidentu čuvaju. Treba sakupljati podatke, relevantne za upravljanje kompjuterskim incidentom i dokazivanje pred sudom.

Podatke, koji se odnose na kompjuterski incident moguće je meriti na više načina:

- Brojem saniranih kompjuterskih incidenata, mere relativnog obima rada, a ne kvaliteta tima, sa odvojenim podacima za svaku kategoriju incidenta; nije posebno vredna jer zavisi od definicije „incidenata“ pa podaci o broju incidenata ne znače mnogo,
- utrošenim vremenom po kompjuterskim incidentu kao: ukupno vreme rada na incidentu, vreme od pojave do saniranja, vreme trajanja svake faze upravljanja i vreme reakcije od inicijalnog izveštaja,
- objektivnom procenom svakog kompjuterskog incidenta, koja određuje efektivnost akcija, npr: pregled logova, obrazaca, izveštaja i druge dokumentacije o incidentu; pregled predznaka i indikatora incidenta, određivanje eventualne štete, određivanje da li je stvarni uzrok incidenta identifikovan, proračun približnog finansijskog gubitka od incidenta i identifikovanje mera za sprečavanje novih sličnih incidenata
- subjektivna procena svakog kompjuterskog incidenta članova interventnog tima i tima u celini,
- periodična revizija programa za upravljanje kompjuterskim incidentom i troškovi čuvanja i zadržavanja dokaza, koji prema nacionalnom zakonu mogu biti: tipično – od jednog meseca do jedne godine, u slučaju sudskog procesa – do kraja procesa, podataka e-pošte – do 180 dana, a podataka o glavnom incidentu – do tri godine.

U tabeli 2.3. prikazana je kontrolna lista koja obezbeđuje glavne korake inicijalnog rukovanja sa incidentom.

Tabela 2.3. Podsetnik za inicijalna rukovanja incidentom

Aktivnost		kompletnost
Detekcija i analiza		
1	Utvrđite da li se incident dogodio	
1.1	Analizirajte predznake incidenta i indikacije	
1.2	Potražite informacije u korelaciji	
1.3	Obavite istraživanja (npr. pretraživači, baze znanja)	
1.4	Čim rukovalac zaključi da je došlo do incidenta, počnite sa dokumentovanjem istrage i prikupljanjem dokaza	
2.	Klasifikujte incident koristeći kategorije (npr. uskraćivanje usluga, zlonamerni kod, nedopušteni pristup, neprikladno korišćenje)	
3.	Pratite odgovarajući spisak kategorija incidenta, a ako se incident ne uklapa ni u jednu od kategorija, pratite generički spisak	

Po završetku analize treba koristiti kontrolnu listu iz tabele 2.4. koja ukazuje na kategoriju incidenta. Ova lista je generička i odnosi se na incidente koji ne pripadaju striktno ni jednoj kategoriji. Kontrolne liste su samo uputstvo za analitičara koje treba slediti u izvršavanju glavnih koraka, a ne precizne procedure.

Tabela 2.4. Kategorije incidenta

Aktivnost		Kompletnost
Detekcija i analiza		
1.	Prioriteti rukovanja incidentom na osnovu poslovnog uticaja	
1.1	Identifikovati resurse koji su pogođeni i očekivanje resursa koji će biti pogođeni	
1.2	Procena tekućih i potencijalnih tehničkih efekata incidenta	
1.3	Pronađite odgovarajuću ćeliju (e) u matrici prioriteta, na osnovu tehničkog efekta i pogođenih resursa	
2.	Prijavite incident odgovarajućim unutrašnjim kadrovima i spoljnim organizacijama	
Suzbijanje, iskorenjivanje i oporavak		
3.	Sticanje, očuvanje, obezbeđivanje dokumenata i dokaza	
4.	Sadržaj incidenta	
5.	Iskorenjivanje incidenta	
5.1	Identifikovanje i ublažavanje svih slabosti koje su eksploatisane	
5.2	Uklanjanje zlonamernog koda, neprikladnih materijala i drugih komponenata	
6.	Oporavak od incidenta	
6.1	Povratak pogođenog sistema za operativno spremno stanje	
6.2	Potvrda da pogođeni sistemi funkcionišu normalno	
6.3	Ako je potrebno, sprovesti dodatni monitoring tražiti buduće aktivnosti	
Aktivnost posle incidenta		
7.	Kreiranje izveštaja praćenja	
8.	Držite kurseve i sastanke	

Kapaciteti za upravljanje kompjuterskim incidentom nalaze se u određenoj međuzavisnosti sa brojnim servisima zaštite: planiranje vanrednih događaja; obuka o zaštiti; upravljanje rizikom i personalna zaštita.

2.1.6.5. Upravljanje vanrednim događajem u IKTS

Planiranje vanrednih događaja uključuje više od samog planiranja evakuacije izvan zone u kojoj je uništen IKT centar organizacije ili drugi kapaciteti IKT sistema organizacije. Plan obuhvata i kako neka organizacija održava kritične IKT funkcije u operativnom stanju u slučaju većih i manjih prekida i nastavlja poslovanje u vanrednim okolnostima.

Za uspostavljanje kapaciteta organizacije za upravljanje vanrednim događajem treba definisati i implementirati proces planiranja vanrednih događaja, uključujući postavljanje što realnijih scenarija i uvežbavanje svih delova organizacije i IKT sistema.

i. Proces planiranja vanrednih događaja

Planiranje vanrednog događaja i nastavljanja poslovanja najsloženiji je deo posla. Kada organizacija odluči kako će nastaviti poslovanje, primena plana je tada relativno lak zadatak.

Proces planiranja vanrednih događaja odvija se u šest faza [8,23]:

1. Identifikovanje funkcija IKTS kritičnih za misiju organizacije osnovni je preduslov za planiranje kontinuiteta poslovanja. Kriterijumi za određivanje kritičnosti poslovanja mogu biti bazirani na vremenu oporavka servisa IKTS, akumuliranom uticaju ili kombinaciji ovih faktora. Posebno je važno identifikovati i proceniti promene, koje vanredni događaj može izazvati u vanradno vreme. Za većinu funkcija IKTS za podršku poslovanja dostiže se tačka u kojoj uticaj vanrednog događaja postaje toliko velik da su bespredmetni pokušaji održavanja kontinuiteta funkcija IKTS. Očigledno, kritične funkcije IKTS treba oporaviti, pre nego što se ova tačka dostigne. U procesu upravljanja vanrednim događajem, vreme je kritičan faktor i važno je što ranije identifikovati implikacije vremena na proces, kao i određivanje prioriteta saniranja posledica. Potpuna redundantnost za svaku kritičnu funkciju, skupa je za većinu organizacija. U slučaju katastrofe, određene IKTS funkcije neće se izvršiti. Ako se odrede prioriteti, povećava se sposobnost organizacije da preživi vanredni događaj [23].

2. Identifikovanje resursa, koji podržavaju kritične IKTS servise, uključuje i identifikovanje vremenskih ograničenja ovih funkcija, tj. da li je resurs potreban stalno ili samo u nekom periodu i efekat neraspoloživosti resursa na misiju ili funkcije IKTS sledeći je korak u planiranju vanrednog događaja. Osnovni problem je što različiti menadžeri vide i identifikuju različite IKT resurse, ili predviđaju interakciju resursa koji podržavaju kritične funkcije, od kojih nisu svi IKT resursi: ljudi, IKT kapaciteti za procesiranje, servisi IKT sistema, podaci i aplikacije, fizička infrastruktura i dokumentacija IKT. Planiranje vanrednog događaja u IKTS treba da obuhvati sve resurse, koji su neophodni da se poslovni proces izvrši. Definisanje neophodnih resursa za suzbijanje posledica vanrednog događaja treba da vrše ona lica koja znaju kako se izvršavaju servisi IKTS i kako objekti IKTS zavise od drugih resursa, kao i druge kritične zavisnosti, pošto svi resursi nisu kritični za izvršavanje najbitnijih poslovnih procesa. Potrebni resursi za podršku kritičnih servisa IKTS za planiranje vanrednog događaja mogu se svrstati u šest glavnih kategorija [28,18]:

- a) Ljudski resursi, najvažniji za svaku organizaciju, obuhvataju administratore, specijaliste zaštite, operatere i korisnike.
- b) Kapaciteti IKTS za procesiranje tradicionalno su prioriteti za planiranje vanrednog događaja. Iako je bekapovanje IKTS glavna aktivnost, važna su i alternativna rešenja, jer kritične zadatke mogu izvršavati lokalne mreže, mini kompjuteri, radne stanice, PC u svim formama centralizovanog i distribuiranog IKT procesiranja.
- c) Aplikacije i podaci IKTS su najkritičnija imovina, jer neposredno podržavaju misiju i tekuće poslovne procese organizacije. Ako se IKT procesiranje izvršava na alternativnom (*back-up*) hardveru, aplikacija mora

biti kompatibilna sa alternativnim hardverom, OS, drugim programima (uključujući verziju i konfiguraciju) i drugim tehničkim faktorima. Potrebno je periodično verifikovati IKT kompatibilnost na primarnoj i rezervnim lokacijama.

- d) Servisi IKTS podržavaju brojne poslovne procese, a najvažniji su komunikacioni (za prenos podataka i glasa) i informacioni servisi (on-line web servisi, e-trgovina, baze podataka, e-bilteni, novinski servisi, privatne baze podataka itd).
- e) Fizička infrastruktura IKTS obezbeđuje radno okruženje, odgovarajuću opremu i alate, neophodne za efektivan rad zaposlenih. IKTS zahtevaju bezbedan radni prostor i sevice, kao što su napajanje električnom energijom, grejanje i hlađenje, a podaci i elektronski mediji zahtevaju fizički prostor za skladištenje.
- f) Dokumentacija i e-evidencija ili obrasci, koje podržavaju većinu servisa IKTS, mogu biti značajni i za legalne potrebe istrage kompjuterskog kriminala. U organizaciji gde su elektronska dokumenta referentna forma, mogu se obezbediti i neprekidno kontrolisati pristupi tim dokumentima.

Plan mera za vanredne događaje treba da obuhvati svaki od napred opisanih resursa.

3. Procena potencijalnih vanrednih događaja u IKTS i njihovih posledica prethodi razvoju scenarija šireg spektra vanrednih događaja. Tipičan scenario treba da uključi odgovore na pitanja za sve relevantne resurse [7,18]:

- a) Ljudski resursi: Mogu li zaposleni doći na posao? Koji zaposleni ima kritična znanja i veštine? Mogu li se zaposleni lako evakuisati na rezervnu lokaciju?
- b) Kapacitet procesiranja: Da li je IKTS ugrožen? Šta se događa ako neki od sistema nije u operativnoj upotrebi? Postoji li lista prioriternih akcija? Koje su komunikacione veze na raspolaganju?
- c) IKT aplikacije i podaci: Da li je ugrožen integritet podataka? Da li je neka IKT aplikacija sabotirana? Može li neka aplikacija raditi na drugoj procesorskoj platformi?
- d) IKT Servisi: Može li IKTS komunicirati sa drugima i kojim sistemima? Mogu li ljudi komunicirati? Koliko dugo (često) su IKT servisi u prekidu? Mogu li se koristiti usluge iznajmljenih udaljenih transakcija?
- e) Fizička infrastruktura IKTS: Imaju li zaposleni mesta, alate i opremu za rad? Mogu li zaposleni zaposeti zgradu za rad i da li postoji funkcionalna infrastruktura radnog okruženja (voda, kanalizacija, ventilacija, grejanje, hlađenje)?
- f) Dokumentacija: Mogu li biti pronađena potrebna elektronska dokumenta i da li su čitljiva?

Razvoj višestrukog scenarija pomaže u razumevanju vrste i obima vanrednih događaja koje plan treba da obuhvati. Važno je ne upasti u zamku razvoja strategije odbrane i planova za svaki pojedinačni scenario.

4. Izbor strategije za upravljanje vanrednim događajem: u evaluaciji rezervne lokacije, neophodno je razmotriti koje su kontrole zaštite instalirane za sprečavanje i smanjenje uticaja vanrednog događaja na IKTS. Pošto ni jedan skup mera i metoda zaštite ne može rentabilno sprečiti sve potencijalne vanredne događaje, u sistemu zaštite treba koordinirati preventivne mere i

aktivnosti za oporavak sistema. Glavna strategija svakog plana za upravljanje vanrednim događajem u IKTS treba da sadrži [2]:

- a) Hitne intervencije – inicijalne akcije za zaštitu ljudskih života i smanjenje štete;
- b) Oporavak sistema – akcije za obezbeđivanje kontinuiteta kritičnih funkcija sistema i
- c) Kontinuitet poslovanja – povratak IKTS u normalni režim rada.

Odnos između oporavka i kontinuiteta rada IKTS je veoma važan. Neke organizacije proces upravljanja vanrednim događajem dele ne hitne intervencije, operacije bekapovanja i oporavak sistema, što nije presudno za uspešno upravljanje vanrednim događajem. Ipak, osnovne funkcije navedenih faza procesa treba da sadrži svaki ozbiljniji plan za upravljanje vanrednim događajem.

Za donošenje odluke o optimalnoj strategiji treba analizirati svaku od kategorija resursa IKTS, opcije oporavka, rentabilnosti i rizika. Težište analize je na oblastima gde nije jasno koja je strategija najbolja[2]:

- a) Ljudski resursi
- b) Kapaciteti za procesiranje IKTS [29]:
 - Primarna lokacija,
 - Hladna lokacija,
 - Vruća lokacija,
 - Redundantna lokacija,
 - Uzajamno bekapovanje,
 - Udaljena iznajmljena transakcija,
 - Hibridni sistemi.

Sistem treba oporavljati prema redosledu zahteva za raspoloživost IKTS kapaciteta za procesiranje. Osnovni kapacitet za oporavak IKTS od vanrednog događaja je bekapovanje podataka i programa izvan primarne lokacije i korišćenje za oporavak IKTS.

- c) Za aplikacije i podatke primarna strategija planiranja vanrednog događaja je regularno bekapovanje i skladištenje na alternativnu lokaciju. U fazi oporavka sistema, oporavljeni podaci zastarevaju za vreme od poslednjeg bekapovanja do pojave vanrednog događaja. Da bi podaci bili korisni, moraju se češće bekapovati. Takođe, da bi oporavljeni IKTS funkcionisao, bitne su usklađenost i ažurnost bekapovanih podataka i sinhronizacija bekapovanih datoteka, uzetih sa različitih delova IKTS u različitim vremenima. Bekapovanje podataka, datoteka i aplikacija kritičan je deo svakog plana za vanredne događaje [5].
- d) Servise IKTS za vanredne događaje mogu obezbediti i TTPS (telekomunikacioni, Internet) provajderi. Primer tehnologije za visoku raspoloživost podataka su RAID (*Redundant Array of Independent Discs*) čvrsti diskovi, koji omogućavaju nastavak rada servera u slučaju kvara jednog diska, bez gubitka podataka. Ovakva raspoloživost podataka zastupljena je u ZU Apoteka Vranje. Druga tehnologija je klaster servera koji deli klijentsko opterećenje i još bolje toleriše otkaze od RAID sistema. Ako otkaze jedan server, drugi preuzima i nastavlja rad. Naravno, ovi sistemi su od male koristi, ako su smešteni na istoj lokaciji. Redundantne servere treba razmestiti na alternativne lokacije i povezati u WAN mrežu. U slučaju prekida električnog napajanja,

raspoloživost podataka, zavisno od kapaciteta, obezbeđuju i izvori neprekidnog napajanja – UPS (*Uninterruptable Power Supply*).

- e) Redundantna fizička infrastruktura za vanredne događaje, kao što su rezervni radni prostor, servisi zaštite, nameštaj i druge potrebe za slučaj vanrednog događaja u IKT sistemu, treba se planirati i ugovarati, iako primarna i rezervne lokacije moraju obezbediti i radni prostor zaposlenih, pored smeštaja IKT opreme. Za premeštanje na rezervne lokacije, treba izraditi procedure za evakuaciju i povratak na primarnu ili novu lokaciju. Zaštita fizičke infrastrukture normalni je deo plana za hitne intervencije.
- f) Dokumentacija, elektronska i papirna uključujući i arhivu, u primarnoj strategiji upravljanja vanrednim događajem obično se bekapuje na magnetne, odnosno optičke i druge medije i skladišti na rezervnoj lokaciji. Papirnu dokumentaciju treba skladištiti na pristupačnoj alternativnoj lokaciji.

5. Implementacija plana za upravljanje vanrednim događajem u IKTS može zahtevati druge pripreme: uspostavljanje procedura za bekapovanje, sklapanje novih i obnavljanje postojećih ugovora za servise, nabavka IKTS opreme, ažuriranje servisa i opreme za bekapovanje, formiranje redundantnih kapaciteta, zamena dotrajale ili zastarele opreme, formalno pripisivanje odgovornosti itd. Važno je održavati pripremu ažurnom, uključujući i dokumentaciju. Za implementaciju plana je najznačajnije: koliko scenarija i verzija plana treba razviti i ko priprema svaku verziju plana pojedinačno?

Oba pitanja treba da kruže u celoj organizaciji tokom implementacije strategije upravljanja vanrednim događajem. Izabranu strategiju i način implementacije treba dokumentovati u politici i procedurama zaštite organizacije. Za male i manje kompleksne IKTS, plan za vanredne događaje može biti deo plana zaštite. Za velike i kompleksne IKTS, plan zaštite može da sadrži kratak pregled plana za upravljanje vanrednim događajem, koji može biti poseban dokument. Dokumentovan plan za vanredni događaj mora biti ažurno održavan u skladu sa promenama i uskladišten na bezbedno mesto. Pisani dokument plana je kritičan faktor u vanrednom događaju i mora biti jasno napisan, razumljiv i na raspolaganju svim zaposlenim. Korisno je uskladištiti ažurne kopije na nekoliko lokacija, uključujući sve rezervne. Obuka zaposlenih za vanredni događaj je obavezna za sve zaposlene i novo-zaposlene. Testiranje plana za vanredne događaje u IKTS treba vršiti periodično, jer plan vremenom zastareva, pa se moraju specifično dodeliti odgovornosti zaposlenim za održavanje ažurnosti plana. Testiranje uključuje reviziju, analizu i simulaciju.

6. Testiranje i revizija strategije upravljanja vanrednim događajima u IKT sistemu Ispitivanje (testiranje) i reviziju plana za vanredne događaje treba vršiti periodično i uvežbavati, pošto uvek ima neka slabost u planu koja se pokaže tokom implementacije i uvežbavanja. Plan vremenom zastareva kako se menjaju resursi za izvršavanje kritičnih IKT funkcija, pa se moraju specifično dodeliti odgovornosti za održavanje ažurnosti plana zaposlenim u organizaciji. Postoji nekoliko vrsta testiranja, uključujući [23,18] :

- Reviziju: može biti jednostavan test za proveru tačnosti dokumentacije plana za vanredne događaje i može se proveriti da li su: svi zaposleni na spisku još uvek u organizaciji i imaju planirane odgovornosti; tačni

telefoni u kući i na radnom mestu, podaci o organizaciji i zgradi, brojevima soba itd.; da li se datoteke mogu izvući iz sistema za bekapovanje i da li zaposleni poznaju procedure za vanredne događaje.

- Analizu: može se izvršiti na celom planu ili delu plana, kao što su procedure za hitne intervencije. Dobro je da analizu vrši lice koje nije radilo u razvoju plana, ali ima dobro radno iskustvo i znanje za obavljanje kritičnih funkcija i upotrebu resursa za podršku. Analitičari slede strategiju plana, tražeći logične ili procesne slabosti u planiranju i intervjuišu funkcionalne menadžere za resurse i druge zaposlene, da bi nadomestili nedostajući ili zamenili nefunkcionalni deo plana.
- Simulaciju krizne situacije: koja obezbeđuje validne informacije o greškama u planu za vanredne događaje i za stvarnu situaciju; uveštavanje procedura za realnu kriznu situaciju i kritične informacije korisne za nastavljavanje poslovanja. Iako simulacija i testiranje mogu biti skupi, što je kritičnija funkcija za koju se simulira vanredni događaj, to je simulacija rentabilnija. Simulacija vanrednog događaja može se izvršiti koristeći rezervnu IKT opremu za oporavak sistema (tzv. vruće testiranje), ili se može izvršiti na papiru (tzv. papirološki test), koji može proveravati ljude i plan, ali ne i IKT opremu. Prednost vrućeg testiranja je što se može smanjiti vreme, povećati broj funkcija koje treba testirati.

2.1.7. Napadi koji dolaze sa *dial-up* veze

Napadi koji dolaze sa *dial-up* veze (telefona) mogu biti lakši za otkrivanje. Postoje dva osnovna napada direktnim biranjem telefona [3]:

- Direktan napada na računar i
- Napad na sistem centrale.

2.1.7.1. Slučaj direktnog napada

Interesantno je koliko slabo u praksi sistem administratori zaštićuju direktno vezane modeme na kritičnim hostovima.

U slučaju nezaštićenog modema na Windows OS mašini moguće je setovati *com port* sa modemom za automatski odgovor. Postoji mnogo programa za udaljeni pristup, kao što su: *PCAnywhere*, *LapLink*, *ReachOut* i stari *CarbonCopy*. Svi ovi programi imaju ograničenu zaštitu lozinkom. Kada je napadač jednom izabrao vaš broj i nalazi se na liniji i računaru, jedina je mogućnost da mu se uđe u trag, angažovanje telefonske kompanije, što podrazumeva uključivanje zvaničnih organa istrage. Tu se mnoge organizacije prelome i prestanu tragati za napadačem. U tom trenutku treba pratiti aktivnost napadača u internoj mreži. Omiljeni trik napadača je postavljanje *snifera* i kupljenje lozinke. Potrebno je odrediti koji nalog je napadač ukrao i upao u telefonski sistem. Zatim treba pratiti trag napadača u mreži i otkriti šta radi. Ovaj proces zahteva uporno proveravanje više log fajlova u serverima mreže.

Neki tipovi softvera za daljinski pristup zahtevaju da host PC bude logovan na lokalnu mrežu (LAN) da bi dopustio legitimnim učesnicima pristup LAN-u. Kada već dobije pristup PC-u, napadač može lutati po LAN-u kao legalni PC korisnik. Ovde log podaci mogu biti od slabe koristi, jer su podaci o legitimnim korisnicima pomešani sa maskiranim napadačima.

Ako je napadnuti računar imao aktiviran sistem logovanja, može se uz pomoć vlasnika računara odrediti kada se neovlašćeni napad dogodio i koristiti to kao polaznu tačku istrage akcija napadača. Iako ova potraga liči na traženje igle u plastu sena, forenzički alati nude moguća rešenja. To su alati za otkrivanje podataka u skrivenim zonama HD (*slak* i nealocirani prostor klastera, *swap* fajlovi i dr.). Može se desiti da ime ili adresa napadača ostane zapisana u ovim zonama. Moguće je, takođe, da se cela *ekskurzija* napadača kroz mrežu pojavi na udaljenom računaru kroz kojeg je napadač pristupio u mrežu (prvo birao telefonom). Ako se napravi *mirror* slika tog računara i analizira, tu je sve što je potrebno za otkrivanje traga napadača u mreži. Čak i kada napadač više nije na mreži, moguće mu je postaviti zamku za sledeći napad. Kada se otkrije napadač na liniji postoji mogućnost da se zadrži dovoljno dugo dok se ne postavi zamka za praćenje traga, prekine veza u kom slučaju treba očekivati da se napadač vrati, ili učini nešto da se napadač uplaši i više nikada ne vrati natrag.

Ako se donese odluka za postavljanje zamke i praćenje traga napadača, kako će se to uraditi zavisi od toga kako je napadač priključen. Ako napadač dolazi sa Interneta, ili spoljne računarske mreže, potrebna je saradnja sa administratorima duž puta kretanja napadača, a ako napadač dolazi preko telefonske linije, potrebna je saradnja sa telefonskom kompanijom.

2.1.7.2. Slučaj napada preko telefonske centrale

U slučaju napada na telefonsku centralu potreban je sudski nalog za postavljanje zamke za napadača (prisluškivanje linije) i praćenje traga napadača. Upoređivanjem vremena pristupa u log fajlu napadnutog računara sa vremenom pristupa u *pen* registru svih dolaznih poziva u telefonskoj centrali, može se otkriti trag napadača. Potpuni sistem zamke i praćenja traga prikuplja informacije koje prolaze telefonskom linijom, kao i izvore poziva.

Postavljanje zamke i praćenje traga u slučaju mrežnog pristupa znatno je teže. U većini slučajeva samo se može nagađati odakle napadač sa Interneta dolazi, pošto „skače“ iz sistema u sistem da bi izbegao detekciju (IDS/IPS). Važno je krenuti u akciju vrlo brzo i uz pomoć neposrednog sistema administratora može se otkriti trag napadača.

Pažljivi napadač uvek proverava da li je administrator mreže na liniji. Jedan od načina da se skrene pažnja sa administratora je uklanjanje svih referenci koje upućuju na administratora, a drugi davanje benignog naloga i maskiranje naloga administratora, kako rade i hakeri. Na primer, vešt napadač obično ulazi u sistem pomoću ukradenog naloga. Kada administrator listira korisnike na liniji (*on line*), napadač vidi samo poznate login podatke. Administrator uvek treba da izbegava logovanje sa konzole u rutu. Ako administrator trenutno izvrši zadatak može se dobro sakriti i posmatrati napadača bez podizanja alarma.

2.1.7.3. Mrežne tehnike za postavljanje zamke i praćenje traga napadača

U traganju za lokacijom napadača na liniji, treba početi sa otkrivanjem IP adrese ili punog imena domena lokacije napadača. Ovim podacima ne treba previše verovati. Ime napadača uglavnom nije stvarno, nego je to samo lokacija na kojoj je ukrao nalog. Podatak treba zapisati kao i sistemsko vreme na napadnutom računaru.

Dalje je potrebno videti šta napadač radi u sistemu, posmatranjem tekućih procesa (u *Task manageru* kod Windows OS). Treba uočiti sve procese koje nije moguće objasniti, a registrovati proces u kojem se sumnja da je napadač u toku.

Posebno treba usmeriti pažnju na skenere (*snifere*), omiljeno sredstvo hakera za traženje lozinke. Vešti hakeri obično preimenuju *snifer*, multipliciranjem instanci *daemon*

ili servisa. Za mnogo više informacija o tome odakle dolazi napadač moraju se primeniti čisto hakerske tehnike sa puno veštine, brzine i pogađanja, zavisno od toga šta se vidi, kao u borbi dva iskusna hakera.

Zatim treba pokušati saznati nešto o sajtu sa koga je napad došao, ako ne o samom napadaču, ono o nalogu koji je ukrao. Odgovarajućim komandama (zavisno od platforme) saznaju se izvorna lokacija, ime i broj telefona administratora lokacije. Može se saznati nešto o ukradenom nalogu sa te lokacije. Ne treba biti iznenađen ako pripada samom administratoru te web lokacije. Ako je administrator kooperativan i sa ovim informacijama može se početi traganje za napadačem rezervnim putem.

Ako je moguće treba izvršiti svaki *online* zadatak sa drugog računara, da se izbegne skretanje pažnje na forenzičarske aktivnosti. Ceo ovaj postupak ne sme da traje više od par minuta. Sve akcije treba zabeležiti, vremena, adrese, korisnička imena i drugo. Međutim postoji čitav skup okolnosti vezanih za napad sa telefonske linije umesto preko Interneta. Za ove aktivnosti potrebno je saradnja i odobrenje nadležnih zvaničnih organa. Generalno svako postavljanje zamke napadaču podleže zakonu o prisluškivanju linija. Kako se *e-mail* smatra „tranzitom“ podataka po žici, to i snifovanje e-pošte pripada tom zakonu. Ako napadnuti IKT sistem ima sistem zaštite koji neprekidno skenira mrežni saobraćaj i skuplja informacije o normalnim aktivnostima, a posebno o neregularnostima, šanse za ulazak u trag napadaču su znatno veće. Ako se ignoriše otkriveni napadač na liniji, posledice mogu biti oštećenje sistema. Drugo, napadač može iskoristiti neki sistem za novi upad u ili izvan tog sistema, što može naneti i druge vrste štete. Uplašiti se i pobeći potpuno je amaterski. Iskusan napadač može otići, ako mu se administrator suprotstavi, ali se sigurno vraća. Ne preporučuje se ulazak u dijalog sa napadačem. To je gubljenje vremena i ništa se ne postiže.

Zamke (zadnja vrata, Trojanci) su mehanizmi koje hakeri ostavljaju na napadnutom računaru, a koji im omogućavaju kasniji povratak, bez nove kompromitacije računara. Ideja je da se zamka postavi na nekoj ulaznoj tački u kompromitovani računar, tako da je administrator ne otkrije i ukloni. Ako administrator otkrije metod originalnog upada, može zatvoriti *rupu* i sprečiti upad napadača. Međutim, dobro skrivanje zamke je izbor napadača. Ovaj mehanizam omogućava napadaču da se bezbrižno vrati kasnije i završi napad, posebno kada je otkriven na liniji.

Potrebno je pratiti razvoj i upoznati se sa brojnim malicioznim metodama i tehnikama hakera za postavljanje zamki, kao i osposobiti administratore da razumeju kako da spreče napadače da se vrate u kompromitovani sistem. Zamke za većinu napadača obezbeđuju nevidljivi povratak u mašinu u najkraćem vremenu, čak i kada administrator pokuša da je obezbedi, na primer promenom svih lozinki i u većini slučajeva izbegavanje logovanja.

U nekim slučajevima hakeri koriste ranjivost (bagove) sistema kao jedine zamke. Tako ranjivost sistema ostaje jedina nedetektovana zamka u sistemu. Zavisno od tipa platforme napadnutog računara razvijen je veliki broj zamki koje se mogu svrstati u brojne, često promenljive kategorije: za *krekovanje lozinke*, „*Rhosts++*“, za *čeksumu i timestamp*, za *login fajlove*, *postavljanje daljinski (telnet)*, za *servise*, *Cronjob*, za *biblioteke*, u *kernelu*, u *fajl sistemu*, na *butabilnom bloku* itd.

Hakeri najčešće žele sakriti programe koje kasnije aktiviraju. To su najčešće krekeri lozinki ili sniferi. Postoji nekoliko metoda skrivanja zamki od kojih su najčešće:

- Promena imena u ime drugog procesa,
- Preimenovanje sniferskog programa u legitiman servis kao u *syslog*, koji se aktivira kad administrator kuca neku komandu, ili gleda koji procesi su aktivni, a pojavi se ime standardnog servisa,
- Modifikovana biblioteka rutina tako da se na komandu ne pokazuju svi procesi,

- Pečovana (zakrpljena) zamka u rutinu koju aktivira prekid rada, tako da se ona ne pojavljuje u tabeli aktivnih procesa i
- Modifikovani kernel tako da se neki procesi ne vide.

Hakeri ne samo da žele sakriti svoj trag u mašini, nego ga žele što je moguće više sakriti i u mrežnom saobraćaju. Ove zamke za mrežni saobraćaj ponekad dopuštaju hakeru da dobije pristup kroz *firewall*. Postoje brojni programi zamki za mrežni saobraćaj koji omogućavaju hakeru da se postavi na određeni broj porta mašine i dobije pristup bez korišćenja normalnih servisa. Pošto mrežni saobraćaj ide preko nestandardnog mrežnog porta, administrator može predvideti hakera u saobraćaju. Ove zamke za mrežni saobraćaj tipično koriste TCP, UDP i ICMP, ali mogu koristiti razne vrste paketa, uključujući i šifrovanu zamku.

Haker može postaviti zamku za TCP *šel* na neki visoki broj porta, po mogućnosti gde *firewall* ne blokira taj TCP port. Često su zadnja vrata zaštićena lozinkom, tako da kada se administrator konektuje na njega, pristup *šelu* se trenutno neće videti. Administrator može tražiti ove veze sa *Netstat* alatom da otkrije koji se portovi slušaju i gde i odakle idu tekuće veze. Ovaj tip zadnjih vrata često omogućava hakeru da probije TCP *Wrapper* tehnologiju. Ova zadnja vrata mogu biti aktivirana na SMTP portu, kroz koji mnogi *firewalls* dopuštaju saobraćaj za e-poštu.

Savremeni proaktivni sistemi za detekciju i sprečavanje upada u sistem obezbeđuju inteligentnu tehniku za hvatanje napadača poznatu kao *ćup meda* ili zamka za aktivnog napadača (*honeypot*). Ove tehnike omogućavaju „zarobljavanje“ hakera u napadnutom sistemu, kada se jednom otkrije. Generalna tehnika zamke za aktivnog napadača obuhvata sledeće aktivnosti:

- Saznati koji nalog haker koristi za pristup sistemu. Ako je nalog ukraden, stvarnom vlasniku dati novi nalog, a ukradeni držati otvorenim. Promeniti prava ukradenog naloga da se ograniče njegove mogućnosti da kreira direktorijume koji sadrže vrlo velike i sumnjive fajlove;
- Ako haker dugo luta sistemom primetiće rekonfiguraciju i postati sumnjičav. Takođe verovatno nije sasvim poznato koja će informacija dovesti u iskušenje hakera da je preuzme (daunloduje);
- Cilj je smestiti hakera u bezopasnu zonu sistema (što je teško učiniti ako haker uđe u rut), dovesti ga u zabludu i navesti na vrlo obimno daunlodovanje. U toku dugog procesa daunlodovanja, izučavati napadača i pokušavati ući u trag izvora napada;
- Iako je vreme dugo, nema garancije da će haker ostati svo vreme u sistemu, može jednostavno preći na drugi kompromitovani računar i tražiti to tamo. Kada haker pronade da je fajl lažan, učiniće virtuelni prekid i gubi mu se svaki trag;
- Drugi problem je što haker može pobeći, alarmiran rekonfiguracijom sistema. Zato je zamka za aktivnog napadača poslednje rešenje;
- Ako se želi sudsko gonjenje napadača u primenu ove tehnike treba uključiti zvanične organe istrage.

2.2. SERVISI I MEHANIZMI ZAŠTITE RAČUNARSKOG SISTEMA - NOSSS

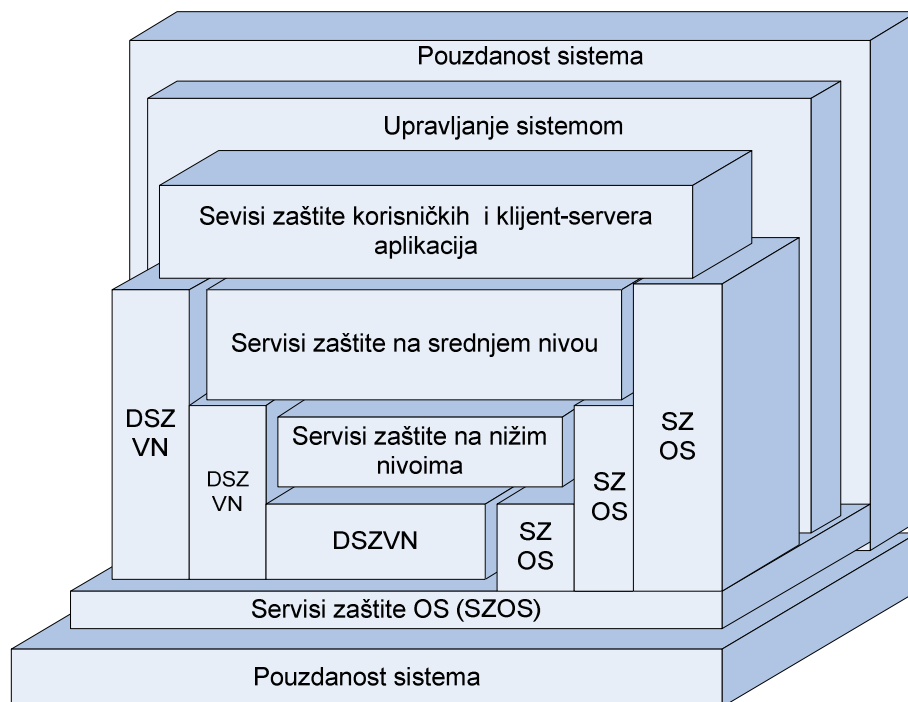
2.2.1. Uvod

Servisi zaštite su funkcije koje izvršava implementirani sistem upravljačkih, operativnih i tehničkih kontrola zaštite ili sistem zaštite u skladu sa programom, politikama i procedurama zaštite. Servisi zaštite su sve one funkcije implementiranog sistema za zaštitu neke računarske mreže (RM) koje taj sistem treba da obezbedi korisnicima ili resursima mreže. Specificiraju se na osnovu funkcionalnih i bezbednosnih zahteva za bezbednosne funkcije, procene pretnji i faktora rizika, poverljivosti sadržaja i procene bezbednosti objekata u mreži.

Mehanizmi zaštite su pojedinačni, individualni algoritmi, ili metodi, ili hardversko-softverski moduli za eliminisanje bezbednosnih problema u mreži. U logičkom smislu, mehanizmi predstavljaju način realizacije servisa zaštite.

Servisi zaštite u distribuiranom IKT sistemu mogu biti distribuirani fizički i logički, u domenama zaštite ili u okviru fizičkih računarskih mreža.

Fizička i logička distribucija bezbednosnih servisa i njihovi odnosi sa drugim servisima sistema prikazani su na slici 2.7. Na slici je prikazano da svi servisi konačno zavise od mehanizama operativnog sistema, a pouzdanost sistema zaštite je ključni element koji obuhvata sve kapacitete zaštite. Upravljanje sistemom je drugi važan aspekt efikasnih mera zaštite.



DSZV- distribuirani servisi zaštite na više nivoa
SZOS -servisi zaštite operativnog sistema

Slika 2.7 Fizička i logička distribucija bezbednosnih servisa

Distribuirani servisi zaštite bazično zavise od pouzdanosti sistema i bezbednosnih servisa operativnog sistema (OS).

2.2.2. Mehanizmi zaštite

Informacioni sistemi sadrže podatke kojima se služe ovlašćeni korisnici i koji služe kako bi korisnicima bilo omogućeno korišćenje sistemom (korisničko ime, lozinka itd.). Budući da takvi podaci ne smeju biti javno dostupni, (moraju biti tajni), ne smeju se menjati bez odobrenja i ne smeju biti nedostupni korisnicima, važno je sprovesti određene korake sigurnosti kako bi navedeni uslovi uvek bili zadovoljeni.

Sigurnosni mehanizam ili mehanizam zaštite (*security machanism*) je mehanizam koji treba da detektuje i predupredi napad ili da sistem oporavi od napada.

Jedan od najkritičnijih delova sigurnosne strategije u organizaciji osigurava sigurnost objekata i nudi pristup odgovarajućim resursima IKT sistema. Da bismo osigurali resurse u organizaciji od malicioznih i neautorizovanih korisnika, i da bismo povećali integritet podataka u organizaciji, veoma je važno izvršiti procenu rizika infrastrukture organizacije i kreirati dokumentovani plan logičke kontrole pristupa - autorizacije i autentifikacije (verifikacije identiteta), koje dozvoljavaju sigurnosnim subjektima (*security principals*) odgovarajući nivo pristupa, različitim resursima IKT sistema, najčešće u zavisnosti od uloge u organizaciji.

Iz razloga što su korisnički nalozi i sigurnosne grupe veoma kritične u procesu efikasne logičke kontrole pristupa, one predstavljaju glavnu formu autentifikacione i autorizacione strategije. Takođe, administrator mora da bude upoznat sa *trust relationship*-om, domenskim funkcionalnim nivoima i osnovnim sigurnosnim subjektima (*security principals*).

Mrežna sigurnost se, između ostalog, zasniva na tri fundamentalna koncepta: autorizacija prava pristupa, autentifikacija i na principu minimuma privilegija.

- **Autentifikacija:** Autentifikacija je proces provere identiteta, nečega ili nekoga, ko pristupa resursima sistema. Autentifikacija obično uključuje korisničko ime i lozinku, mada u nekim slučajevima može uključivati bilo koji predmet za demonstraciju identiteta, kao što su na primer, biometrijski parametri smart kartice, skeniranja mrežnjače, prepoznavanja glasa ili otiska prsta.
- **Autorizacija:** Autorizacija je proces dodeljivanja, identifikovanom korisniku ili procesu, prava i nivoa pristupa objektima (resursima) sistema. Vlasnik resursa, ili neko kome je dodeljena dozvola, određuje da li je korisnik član unapred određene grupe ili poseduje određeni nivo pristupa. Podešavanjem dozvola pristupa na resursu, vlasnik resursa kontroliše, koji korisnici i grupe na mreži mogu pristupati tom resursu.
- **Minimalne privilegije:** Princip minimalnih privilegija (*least privilege*) glasi da administrator mora da dodeli korisnicima samo neophodan nivo privilegija, da bi mogli obavljati svoje radne zadatke. Takođe, potrebno je sprečiti i zabraniti nivo pristupa, koji nije neophodan za obavljanje radnih zadataka, a time se mogu sprečiti maliciozni korisnici da povećaju privilegije i tako ugroze mrežnu sigurnost.

2.2.2.1. Autentifikacioni protokoli u Windows Server 2003

Windows Server 2003 nudi mogućnost autentifikovanja različitih klijentskih operativnih sistema. Da bi ponudili ovu mogućnost i da bi se izvršilo servisiranje ranijih operativnih sistema, Windows koristi dva primarna autentifikaciona protokola: NTLM i Kerberos.

NTLM protokol: Ovaj servis koristi *Challenge-response* mehanizam da autentifikuje korisnike i klijentske kompjutere. Windows Server 2003 podržava sledeća tri metoda *Challenge-response* autentifikacije:

- **LAN manager (LM):** izgradili su ga udruženim snagama *Microsoft i IBM* za korišćenje u *OSI2 i Windows for Workgroups, Windows 95, Windows 98 i Windows Me*. Ovo je najmanje sigurna *Challenge-response* autentifikacija.
- **NTLM Version 1:** Pruža veću sigurnost od **LAN Managera**. Koristi se za povezivanje dva servera, koja rade na *Windows NT Service Pack 3* i ranijim. NTLMv1 koristi 56-bitno šifrovanje da bi zaštitio protokol.
- **NTLM Version 2:** Najsigurnija forma *Challenge-response* autentifikacije. Ova verzija uključuje sigurni kanal da bi zaštitio autentifikacioni proces. Koristi se za povezivanje dva Servera *Microsoft Windows 2000, Windows XO, Windows NT Service Pack 4*. NTLMv2 koristi 128-bitsko šifrovanje da bi zaštitio protokol.

Kerberos: Kao podrazumevani autentifikacioni protokol za *Windows XP Professional i Windows Server 2003*, Kerberos protokol je dizajniran da bude sigurniji i skalabilniji od NTLM kroz velike, raznolike mreže. Kerberos nudi sledeće prednosti od onih, koje nudi NTLM protokol:

- **Efikasnost:** Kada server mora da autentifikuje klijenta, server može da izvrši procenu klijentskih ličnih podataka (*Credentials*), a da pritom ne mora da traži informacije od domenskog kontrolera.
- **Uzajamna autentifikacija:** Vrš se procena identiteta servera i klijenta i na serveru i klijentu.
- **Uprošćava upravljanje poverenjem:** *kerberos* može da koristi tranzitivno poverenje između domena, koji se nalaze u istoj zoni i domena koji su povezani preko zone poverenja.
- **Interoperability:** Kerberos je zasnovan na *Internet Engineering Task Force (IETF)* standardima.

Kerberos autentifikacija se zasniva na specijalno formatiranim paketima podataka, koji su poznati pod nazivom *Tickets*. U *Kerberosu*, ovi *ticket*-i prolaze kroz mrežu umesto lozinki. Ovaj proces dodatno štiti sigurnost mreže.

i. Proces NTLM autentifikacije

Kao što smo ranije pomenuli, NTLM uključuje tri metode *Challenge-response* autentifikacije: *LAN Manager, NTLMv1 i NTLMv2*. Autentifikacioni proces za sve ove metode je isti, ali se razlikuju u nivou šifrovanja. Sledeći koraci demonstriraju nam tok aktivnosti, koje se dešavaju kada se klijent autentifikuje domenskom kontroleru, koristeći NTLM protokole. Klijent i server pregovaraju o autentifikacionom protokolu. Ovo se odrađuje koristeći *Microsoft Negotiate SSP*.

1. Klijent šalje korisničko ime i ime domena ka domenskom kontroleru.

2. Domenski kontroler generiše 16-byte slučajni niz (*random string*) karaktera koji se naziva *Nonce*.
3. Klijent šifrue sa *Hash*-om korisnikove lozinke i šalje ga nazad ka domenskom kontroleru.
4. Domenski kontroler opet dobija *Hash* korisničke lozinke od *Security Account Database*.
5. Domenski kontroler koristi iznos *Hash*-a koji je dobio od *Security Account Database* da bi dešifrovao *Nonce*. Iznos se poredi sa iznosom dobijenim od klijenta. Ako su iznosi identični, klijent će biti autentifikovan.

ii. Proces Kerberos autentifikacije

Kerberos protokol sadrži tri komponente :

- klijent, koji zahteva servis ili autentifikaciju,
- server, koji hostuje servise koje zahteva klijent,
- kompjuter, kojem veruju i klijent i server (u ovom slučaju *Windows Server 2003* domenski kontroler), na kojem radi KDC (*Key Distribution Center*) servis).

Key Distribution Center: KDC održava bazu podataka u kojoj se nalaze informacije o nalogima za sve sigurnosne subjekte (*Security principals*) u domenu. KDC smešta kriptografski ključ, koji je poznat samo sigurnosnom subjektu i KDC-u i poznat je pod imenom *Long-term-key*. *Long-term-key* je isporučen od korisničke Log-on lozinke.

Proces Kerberos autentifikacije:

1. Kada korisnik upiše korisničko ime i lozinku, kompjuter šalje ove informacije za prijavljivanje ka KDC-u. „*Logon*“ informacije (*credentials*) uključuju korisničko ime, nalog domena, preautentifikacione podatke, koji su šifrovani tajnim ključem, koji je dobijen iz korisničke lozinke. KDC sadrži master bazu podataka u kojoj se nalaze jedinstveni *long-term-keys* za svaki subjekat (principal).
2. KDC traži *master key* (KA), koji je takođe dobijen iz korisnikove lozinke. KDC nakon toga kreira dve jedinice: *Session Key* (SA) koji deli sa korisnikom i *Ticket-Granting Ticket* (TGT). TGT uključuje drugu kopiju SA, korisničko ime i datum isteka. KDC šifrue ovu ulaznicu (*ticket*), koristeći svoj *Master Key* (KKDC), koji zna samo KDC.
3. Klijentski kompjuter prima informaciju od KDC-a i startuje korisničku lozinku kroz jednosmernu funkciju sažetka (*One-way hashing*), koja konvertuje lozinku u korisnikov KA. Klijentski kompjuter sada poseduje *Session Key* (SA) i TGT tako da može bezbedno da komunicira sa KDC-om. Klijent je sada autentifikovan u domenu i spreman je da pristupi drugim resursima u domenu koristeći *Kerberos* protokol.
4. Kada *Kerberos* klijent mora da pristupi resursima na server koji je član istog domena, on kontaktira KDC. Klijent će dati svoj TGT i svoj *timestamp* (vremenski pečat) šifrovanog sa *Session* ključem (SA) koji je već ranije podeljen sa KDC-om. KDC dešifruje TGT koristeći KKDC. TGT sadrži korisničko ime i kopiju SA. KDC koristi SA da bi dešifrovao *timestamp*. KDC može da potvrdi da je zahtev došao od korisnika jer samo korisnik može da koristi SA.

5. Nakon toga, KDC kreira par *Ticketa*, jednu za klijenta i jednu za server na kojem se nalaze resursi, kojima klijent mora da pristupi. Svaki *Ticket* sadrži ime klijenta koji zahteva servis, primaoca zahteva, *timestamp*, koji ukazuje na vreme kada je *Ticket* kreiran i vremenski iznos koji ukazuje na količinu vremena kad je *Ticket* validan. Oba *Ticketa* sadrže novi ključ (KAB) koji će biti podeljen između klijenta i servera tako da oni mogu da komuniciraju na siguran i bezbedan način.
6. KDC uzima serverski *Ticket* i šifrjuje ga koristeći *Master Key* (KB). Tada će KDC ugnezditi serverski *Ticket* unutar klijentskog *Ticketa*, koji takođe poseduje KAB. KDC šifrjuje celu stvar koristeći *Session Key*. KDC nakon toga šalje sve ove informacije ka korisniku.
7. Kada korisnik primi *Ticket*, korisnik će prvo dešifrovati ceo paket koristeći svoj SA. Ovaj proces će prikazati KAB klijentu, a *Ticket* serveru. Korisnik ne može da pročita Serverski *Ticket*.

2.2.2.2. Log datoteka lozinke u Windows Server 2003 sistemu

Da bi sprečili da lozinke budu razotkrivene i zloupotrebene, Windows Server 2003 i Windows XP moraju da smeste lozinke na siguran način. Da bi postigli najviši nivo poverljivosti i integriteta za lozinke, lozinke moraju da se smeste na nivou domena u *Aktivnom Direktorijumu*.

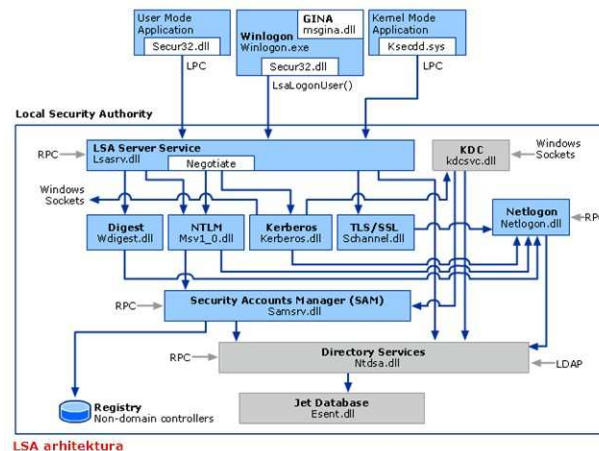
Local Security Authority: Lokalne lozinke su smeštene i održavane u *LOCAL Security Authority* (LSA). LSA je odgovoran za :

1. Upravljanje lokalnim sigurnosnim polisama
2. Autentifikovanje korisnika
3. Kreiranje *Access Token*-a
4. Kontrola i revizija (*Audit*) polisa

LSA tajne (*secrets*): Osetljive informacije smeštene korišćenjem LSA su poznate pod nazivom *LSA secrets*. LSA tajna sadrži:

1. *Trust Relationship* lozinke
2. Korisnička imena
3. Lozinke
4. *Service Account* lozinke
5. *Service Account* imena

Na slici 2.8. prikazana je arhitektura LSA servera.



Slika 2.8. Arhitektura LSA

2.2.2.3. Šifre na Windows sistemima

Lozinke na operativnim sistemima se čuvaju na određenim mestima u odgovarajućim datotekama. Windows XP operativni sistem čuva lozinke u SAM datoteci, u kojoj su upisani heš vrednosti lozinke svih korisnika jednog računara. Datoteka SAM nalazi se na putanji: **C:\Windows\system32\config\SAM**. Sledeći put kada se isti korisnik loguje na sistem, ponovo se računa heš vrednost ukucane lozinke i upoređuje sa hešom koji definiše lozinku, koju je korisnik izabrao na samom početku. Znači, šifre se u obliku heša čuvaju u SAM datoteci, a pri prijavljivanju korisnika na sistem, korisnik upisuje svoju šifru u *login form* i sistem automatski računa heš lozinke koju korisnik trenutno unosi u *login form*. Izračunati heš upoređuje sa hešom koji se nalazi u sistemu, odnosno u SAM datoteci. Ako su heševi identični, sistem dopušta korisniku da pristupi svom nalogu, dok je u suprotnom korisnik obavešten o neispravnosti svoje lozinke.

Šta je glavni problem sa ovom metodom autentifikacije? Vrlo je moguće da postoje dva različita niza karaktera koji će provlačenjem kroz heš funkciju dati isti heš. Ovo je i glavni nedostatak heš funkcija i predstavlja problem kolizije. Pored ovog problema, jedan od najvećih problema koji narušavaju sigurnost šifara uopšte, je ljudski faktor. Šifre zapisane po čitavoj kancelariji, deljenje šifara kolegama sa posla itd. postoje i „Administratori“ mreža i sistema koji greškom ili neznanjem ostave nalog Administrator nezaštićenim, odnosno bez šifre, jer se za svakog korisnika napravi nalog, dok se administratorski nalog zanemaruje usled nekorisćenja.

Kako bi razbili heševe i ukazali na nedostatke pojedinih heš funkcija, kriptanalitičari koriste razne metode, kao što je napad rečnikom. O čemu se radi? Pošto se SAM datoteka čita radi upoređivanja heša unetog na terminalu i onog koji postoji u sistemu, lako je za pretpostaviti da je moguće napraviti posebnu heš vrednost, iako je ona nastala od neke reči, koja nije ista kao šifra korisnika računara, koja odgovara vrednosti u SAM datoteci. Na ovaj način bi u *login formu* pri prijavi na sistem, bilo moguće navesti tu drugu reč kao lozinku i da nas sistem pusti da koristimo nalog kao regularni korisnik, jer obe reči iako različite daju isti heš. Postoje razni alati za spašavanje zaboravljenih lozinke koji radi baš na ovom principu, dakle, čitaju vrednosti heša i koristeći reči i fraze koje su smeštene u bazama tih programa. Kada program dođe do reči ili fraze koja daje isti heš kao onaj u sistemu, smatra se da je šifra razbijena.

2.2.2.4. Ranjivost SAM baze u Windows-u

Ranjivosti SAM (*Security Accounts Manager*) baze u Windows operativnom sistemu dozvoljavaju napadaču ekstrahovanje korisničke lozinke i nedozvoljeno logovanje u sistem pod drugim korisničkim nalogom. SAM baza je obično zaštićena definisanim postavkama u *Windows Registry*-ju, ali ipak neke od procedura, koje se obično pokreću za druge namene, otvaraju korisnicima pristup SAM bazi i podacima u njoj. Primer takve aktivnosti je kreiranje „*Emergency Disc*“, koji je čitljiv svim korisnicima, a sadrži podatke o svim korisničkim nalogima na računaru. Ako uzmemo u obzir činjenicu da je SAM baza podataka zaštićena relativno slabim šifarskim algoritmom, kakav je *LM hash* pod Windows XP operativnim sistemom, dolazimo do iznenađujuće činjenice koliko je lozinka, kao mehanizam za kontrolu pristupa na lokalnoj radnoj mašini, zaista slab mehanizam zaštite od neovlašćenog pristupa podacima.

Ranjivost SAM baze podataka leži u ranjivostima *LM hash* algoritma, te u činjenici da su ovi algoritmi javno publikovani, isto kao i mehanizmi za njihovo razbijanje, te zlonamernom korisniku jedina prepreka do pristupa informacijama ostaje utrošak vremena da nađe uputstvo za napad na korisničke lozinke.

Pomenuti propust Microsoft je registrovao kao sigurnosni propust **ID 859**. Propust u sigurnosti SAM baze, generalno gledano, ogleda se u činjenici da svaki korisnik sa „*Normal User*“ privilegijama može pročitati sadržaj *back-up* SAM baze podataka. Pri tome važno je naglasiti da napadač mora imati lokalni pristup mašini, koju napada, odnosno ovaj napad nije moguće realizovati sa udaljene lokacije.

Baza podataka se puni kreiranjem korisničkih naloga, koji su izvorno u čitavom tekstu. Najpre se kreira polje baze sa sledećim parametrima: *SSID*, *Username*, *Password-Hash*. Pomenuto polje se šifrjuje sistemskim ključem. Kada utvrdimo lokaciju Windows XP operativnog sistema, pristupamo pronalaženju sistemskog ključa kojim je SAM baza šifrovana i koji će se koristiti u dešifrovanju baze. Uzimanje ključa vrši se komandom za pokretanje odgovarajućeg uslužnog alata BKHIVE, na lokaciji gde je pomenuti ključ smešten:

```
#bkhive/mnt/sda1/WINDOWS/system32/config/system/root/mojdirektorijum/mojkljuc
```

Kada imamo ključ, pokrećemo alat za uzimanje SAM baze, koja će nam biti dostupna u svom šifrovanom obliku, te ćemo iskoristiti sada poznati ključ da je dešifrujemo i prevedemo u čist tekst. Za tu namenu koristimo uslužni alat SAMDUMP2:

```
#samdump2/mnt/sd1/WINDOWS/system32/config/SAM/root/mojdirektorijum/mojkljuc>  
/root/mojdirektorijum/ambalaza
```

Rezultat navedene aktivnosti je prikaz i spašavanje baze SAM sa podacima o korisnicima i njihovim *hash*-ovanim pripadajućim lozinkama i ID identifikatorima.

Rezultate stavljamo u */root/mojdirektorijum/ambalaza*.

Da bi smanjili broj iteracija u napadu i koncentrisali se na korisnički nalog koji nam je od interesa, odvajamo vrstu u bazi, koja nam je od interesa, a to je najčešće *Administrator* nalog :

```
#grep-i administrator/root/mojdirektorijum/ambalaza>/root/mojdirektorijum/mojalozinka
```

ili

```
#cat/root/mojdirektorijum/ambalaza>grepadministrator>/root/mojdirektorijum/mojalozinka
```

Nakon toga ostaje nam da primenimo neku od metoda napada na *hash*-ovanu lozinku naloga, čiju lozinku pokušavamo dohvatiti. Najčešće korišćen alat je *John the Ripper*. Korišćenjem komande *locate* može se locirati instalacija pomenutog alata, koji se obično nalazi :

```
/pentest/password/john-1.7.2/run/
```

ili ručno preći na :

```
#cd/usr/local/john-1.7.2/
```

ili

```
/usr/local/john-1.7.2#john-i:lanman/mojdirektorijum/mojalozinka
```

Na ovaj način, korišćenjem inkrementalne metode i algoritma *lanMan* dolazi se do lozinke korisnika u čistom tekstu, koja nam je čitljiva i kojom se može autentifikovati na Windows XP. Isti efekat se može postići i korišćenjem drugih algoritama, kao što su *Dictionary Attack*, *Rainbow Attack* ili *Brute Force* napad, kada se piše:

```
/user/local/john-i:all/root/mojdirektorijum/mojalozinka
```

2.2.3. Karakteristike sigurnosti *Encrypting File System-a*

Od verzije 5.0, NTFS sistem datoteka ima mogućnost šifrovanja objekta sistema datoteka na disku/particiji, putem *Encrypting File System* (EFS). Postoje dve generalne vrste šifrovanja diska: one koje šifruju ceo disk i one koje šifruju samo pojedine objekte sistema datoteka poput datoteka i direktorijuma. U ovaj drugi tip spada EFS.

EFS čuva sadržaj datoteka od uljeza, koji bi mogli steći fizički pristup kritičnim podacima. Šifrovanje putem EFS-a nije dovoljno da obezbedi jedan od sigurnijih ciljeva zaštite integriteta iz CIA (*poverljivosti, integriteta, raspoloživosti informacija*) trojke, jer ne može da spreči nekog napadača da obriše šifrovanu datoteku i na taj način izvrši neautorizovanu modifikaciju. EFS ima sledeće prednosti u odnosu na korišćenje drugih aplikacija za šifrovanje sistema datoteka:

- **Transparentnost.** Transparentan je za korisnike i za sve aplikacije. Jednom kada je datoteka ili direktorijum označen kao šifrovan, biće šifrovan u pozadini bez interakcije sa korisnikom. Korisnik ne mora da pamti neku lozinku da bi dešifrovao podatke.
- **Jaka sigurnost.** Koriste se standardni kriptografski algoritmi poput DES-X, 3DES i AES sa poznatim ranjivostima, manama i prednostima.
- **Zaštita procesa (de)šifrovanja.** Svi (de)šifrovani procesi se izvode u zaštićenom režimu rada operativnog sistema.
- **Mehanizam oporavka.** EFS obezbeđuje mehanizam oporavka podataka, koji je značajan u poslovnom okruženju, jer daje organizaciji mogućnost da dođe do podataka, čak i ako je zaposleni, koji ih je šifrovao napustio kompaniju.

2.2.3.1. Šifrovanje i dešifrovanje EFS-a

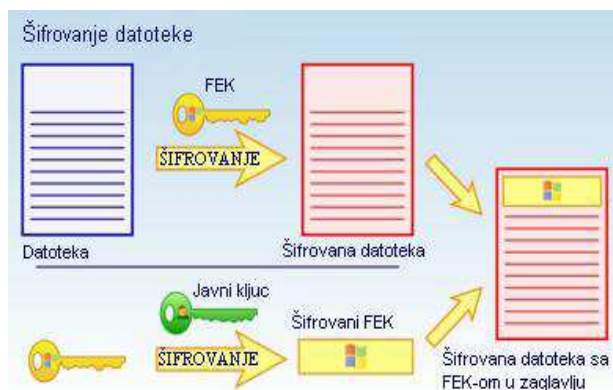
Za uključivanje šifrovanja za neku datoteku ili direktorijum potrebno je uraditi jednu od sledećih akcija:

1. U grafičkom režimu za izabrani objekat u njegovim svojstvima na dijalogu *Advanced Attributes* izabrati opciju *Encrypt contents to secure data*.
2. Dodati objekat u već šifrovan direktorijum.
3. U konzolnom režimu koristiti naredbu *cipher.exe* sa odgovarajućim parametrima.

Šifrovanje se isključuje na isti način, ali u suprotnom smeru.

EFS koristi kombinaciju simetričnog i asimetričnog načina šifrovanja. Razlog zašto se koriste dva različita načina je brzina procesa šifrovanja. Proces šifrovanja jedne datoteke sastoji se od sledećih koraka (Slika 2.9.):

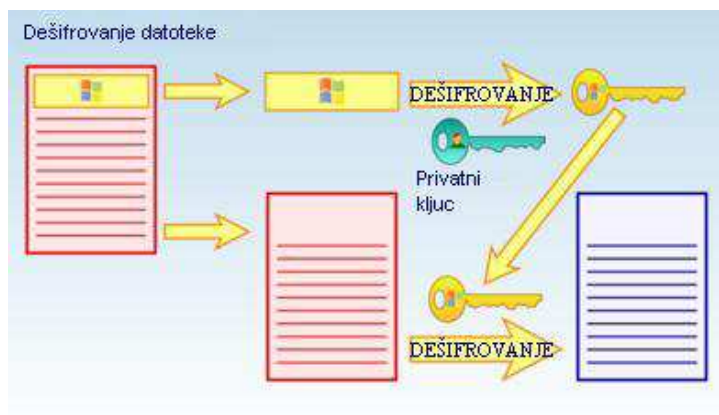
1. operativni sistem pravi jedinstveni simetrični ključ FEK
2. koristeći FEK šifrira se polazna datoteka
3. korisnikov javni ključ će biti upotrebljen za šifrovanje FEK-a
4. konačna šifrovanja datoteka se sastoji od šifrovanog FEK-a i šifrovane polazne datoteke.



Slika 2.9. Proces EFS šifrovanja datoteke

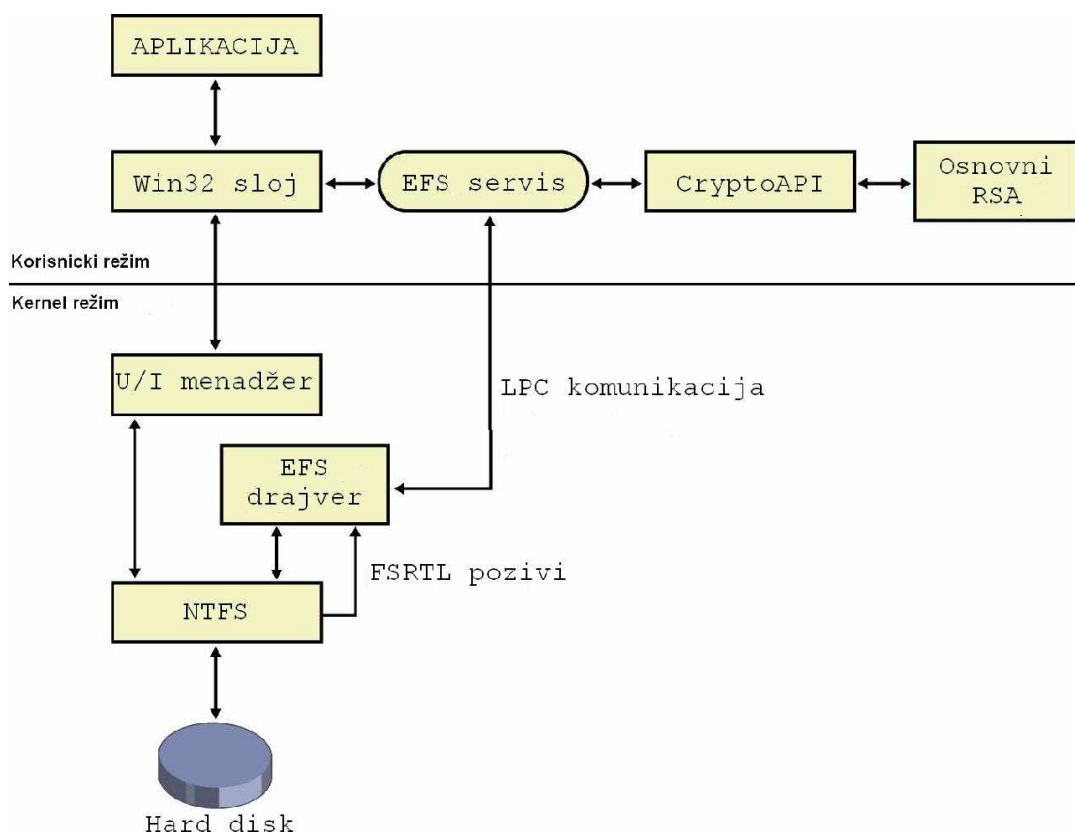
Obrnut proces za jednu šifrovanu datoteku sastoji se od sledećeg (Slika 2.10.):

1. izdvajaju se šifrovani FEK i šifrovani podaci datoteke
2. pomoću korisnikovog tajnog ključa izvodi se dešifrovanje simetričnog ključa
3. sada se FEK koristi za simetrično dešifrovanje da bi se dobila polazna datoteka.



Slika 2.10. Proces dešifrovanja EFS datoteke

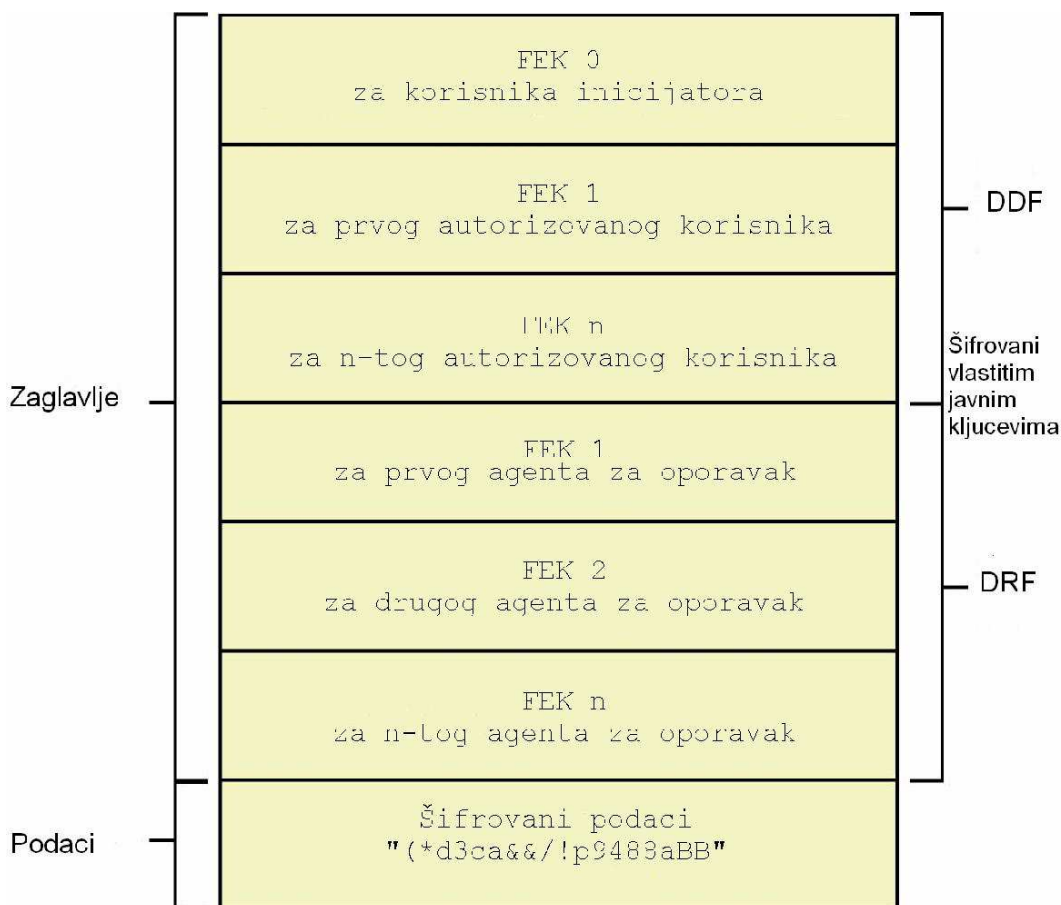
Kao prvi korak šifrovanja, NTFS kreira log datoteku po imenu *Efs0.log* u direktorijumu *System Volume Information*, na istom disku/particiji gde je i datoteka. Onda EFS dobija pristup *CryptoAPI* kontekstu. Uz pomoć njega, EFS generiše FEK.



Slika 2.11. Arhitektura EFS-a

Sledeći korak se sastoji u dobijanju javnog/privatnog para ključeva; ako ne postoji u ovoj fazi (slučaj kada je EFS upotrebljen po prvi put), EFS generiše novi par. EFS koristi RSA algoritam da šifruje FEK.

Onda EFS kreira DDF (*Data Decryption Field*) za trenutnog korisnika tj. za onoga koji je pokrenuo proces šifrovanja, gde postavlja FEK i šifruje ga sa javnim ključem. Ako je agent za oporavak (*recovery agent*) definisan sistemskom politikom, EFS takođe kreira DRF (*Data Recovery Field*) i tu postavlja FEK šifrovan sa javnim ključem agenta. Poseban DRA je kreiran za svakog definisanog agenta za oporavak. Ako postoje korisnici koji imaju pravo na istu datoteku, onda se još pravi odgovarajući broj DDF polja sa šifrovanim FEK ključem na isti način, sa pripadajućim javnim ključevima. Na kraju se dobija struktura podataka kao na slici 2.12.



Slika 2.12. Sadržaj šifrovanog objekta sistema datoteka

Sada je *Efs0.tmp* kreiran u istom direktorijumu u kojem se nalazi datoteka za šifrovanje. Sadržaj originalne datoteke sa otvorenim tekstom (*plain text*) je kopiran na privremeno mesto, te je posle toga original zamenjen šifrovanim podacima. Nakon završenog šifrovanja, privremene i log datoteke su izbrisane.

Nakon što je datoteka šifrovana, samo korisnici koji imaju odgovarajući DDF ili DRF mogu pristupiti datoteci. Ovaj mehanizam je odvojen, ali i upoređan sa uobičajenom kontrolom pristupa putem ACL lista, koje se podrazumevano koriste. Samo korisnik koji može dešifrovati FEK sa svojim privatnim ključem, može pristupiti podacima.

Prvo operativni sistem proverava da li korisnik ima privatni ključ koji koristi EFS. Ako ima, on čita EFS atribut i ide kroz DDF polja tražeći DDF za trenutnog korisnika. Ako je DDF pronađen, koristi se korisnikov privatni ključ koji dešifruje FEK izdvojen iz DDF polja. Koristeći dešifrovani FEK, EFS dešifruje sadržaj datoteke i njega isporučuje aplikaciji koja ga dalje koristi.

FEK nastaje preko generatora slučajnih brojeva i jedinstven je za datoteku. EFS dobija FEK iz statički povezane biblioteke, koja ne može biti zamenjena nekom drugom.

Pošto simetrično šifrovanje ne povećava količinu procesiranih podataka, veličina novostvorene datoteke tako se povećava u minimalnom iznosu. Veličina datoteke izražena u KB ili većim jedinicama nije najčešće ista pre šifrovanja i posle šifrovanja.

2.2.3.2. Kriptografski algoritmi u EFS-u

U EFS-u se koriste razni kriptografski algoritmi i tehnike, poput DES-X, 3DES, AES, RSA, RC4 i jednosmernih *hash* funkcija. Kod Windows XP Professional-a alternativno može da se koristi 3DES, dok je ista verzija, ako ima Service Pack 1 instaliran, sposobna da koristi kao treći algoritam i AES-256 (kao i Server 2003).

EFS koristi bazu podataka *Registry* da odluči koji će simetrični algoritam koristiti od raspoloživih. Ako je vrednost ključa HKLM\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy = 1, onda se koristi 3DES.

A ako ne, onda EFS proverava ključ HKLM\Software\Microsoft\Windows NT\CurrentVersion\EFS\AlgorithmID (ovaj ključ ne mora biti prisutan). Podešavanje da bi podrazumevani simetrični algoritam bio 3DES je izvodljivo iz *gpedit.msc* konzole na putanji *Computer Configuration\Windows Settings\Security Settings\Local policies\Security Options* i politici „System cryptography: Use FIPS compliant algorithms for encryption“.

FIPS (*Federal Information Processing Standards*) broj 140-1 i 2 je standard koji govori o sigurnosnim zahtevima za kriptografske module, izdat od strane američkog NIST-a (*National Institute of Standards and Technology*). Algoritam trostrukog DES-a (triple DES, 3DES), je saglasan sa FIPS 140-1 i 2 objavom standarda.

DES-X je manje poznati simetrični algoritam i predstavlja varijaciju DES algoritma, prethodnog standarda vlade SAD-a. Kao što je poznato da DES nije otporan na napade tzv. Grube sile (*brute-force attack*) zbog male veličine ključa od 56 bita, sa DES-X se probalo popraviti stanje bez značajnijih zahvata u osnovnom pristupu. Predložio ga je Ron Rivest 1984. godine, po sledećoj formuli:

$$\text{DES-X}(M) = K_2 \oplus \text{DES}_K(M \oplus K_1)$$

Gde su M podaci za šifrovanje, K_1 i K_2 dodatni ključevi oba dužine 64 bita a između se koristi operacija ekskluzivnog ILI.

Crypto API je uobičajeno ime za *Microsoft Cryptographic API*, koji obezbeđuje interfejs ka svim kriptografskim operacijama koje zahteva EFS. Podržava i simetrični način kriptografije kao i kriptografiju javnim ključem. Neke od dostupnih operacija su: kreiranje ključeva, razmena ključeva, šifrovanje, dešifrovanje, *hashing*, digitalno potpisivanje, sigurni kriptografski generator pseudoslučajnih brojeva.

Crypto API radi u sprezi sa različitim provajderima kriptografskih servisa - CSP (*Cryptographic Service Providers*), koji su instalirani na operativnom sistemu. CSP-ovi predstavljaju module koji rade stvarni deo šifrovanja i dešifrovanja. Od samog Microsoft-a su instalirani *Basic*, *Enhanced* i *Strong* servisi.

FSRTL (*File System Run-Time Library*) je deo EFS upravljačkog programa koji omogućava otvaranje, čitanje i pisanje za šifrovane datoteke i direktorijume.

2.2.3.3. Mehanizam oporavka kod EFS-a

Proces obnavljanja odnosno oporavka (*recovery*) je sličan dešifrovanju, osim što koristi privatni ključ agenta za oporavak da bi se dešifrovao FEK u DRF, ne u DDF polju. Korisnički nalog koji je vezan za sertifikat agenta za oporavak će izvršiti dešifrovanje datoteke.

Korisnički digitalni sertifikat je stalno smešten na sledećoj putanji:

%USERPROFILE%\ApplicationData\Microsoft\SystemCertificates\My\Certificates

za svakog korisnika, gde je %USERPROFILE% sistemska promenljiva. Sa tog mesta sertifikat se, svaki put kad se korisnik prijavi na sistem, prebacuje u lično spremište sertifikata. Za korisnike koji imaju lutajući (*roaming*) tip profila, sertifikat se nalazi u *Active Directory* bazi podataka domenskog kontrolera te na taj način prati korisnika kada se on loguje na bilo koji računar u domenu. Sadržaj ličnog spremišta sertifikata se može pogledati u *certmgr.msc* konzoli na putanji *Personal\Certificates*. U polju *Intend purpose* za korisnike stoji *Encrypting File System*, a za agenta oporavka stoji *File Recovery*. Sertifikat agenta za oporavak se može videti u i *gpedit.msc* konzoli na putanji *Local Computer Policy \Computer Configuration\ Windows Settings\ Security Settings\ Public Key Policies\ Encrypting File* odakle se može pokrenuti akcija *Add Data Recovery Agent*.

Radi pojačavanja sigurnosti preporučljivo je arhivirati informacije, kao što su ključevi, potpisi i sertifikati. U operativnom sistemu Windows se koristi više formata za ove potrebe, a najčešće su to **.cer** i **.pfx**.

Sistemske servise, koji se brine da ne dođe do neautorizovanog pristupa privatnim ključevima i drugim poverljivim informacijama od strane korisnika, procesa i drugih aplikacija se identifikuje kao *Protected Storage servis* u *services.msc* konzoli, a u *Task Manager*-u, kao *Isass.exe* proces, ne može se ugasiti kao proces. Ako dođe do prestanka rada servisa sistem će se restartovati.

Postoji pet nivoa zaštite koje ima objekat za šifrovanje, a koje transparentno obezbeđuje operativni sistem:

1. EFS koristi FEK ključ kojim štiti podatke objekta
2. FEK ključ se štiti sa javnim ključem korisnika i agenata za oporavak
3. Servis *Protected Storage* upotrebljava korisnikov tzv. *master key* da zaštiti njegov privatni ključ. Privatni ključevi koji će se koristiti za dešifrovanje se nalaze zaštićeni u u %USERPROFILE% \ *Application Data \ Microsoft \ Crypto \ RSA \ User SID* direktorijumu.
4. Isti servis će generisati simetrični ključ izveden od korisnikovih akreditiva, uključujući lozinku, da bi zaštitio *master key*, te se smešta u %USERPROFILE% \ *Application Data \ Microsoft \ Protect \ User SID* direktorijum.
5. Dodatni nivo zaštite je tzv. *system key*, koji može da zaštićuje sve korisničke *master* ključeve.

Uprkos naporima Windows-a da zaštiti ključeve, činjenica je da su sve informacije smeštene na lokalnom računaru, te daju šansu napadačima, koji su dobili pristup hard disku, da otkriju ključeve i da ih upotrebe za dešifrovanje zaštićenih podataka. Ukupna bezbednost bi mogla biti značajno povećana šifrovanjem privatnih ključeva pominjanim sistemskim ključem. Program *syskey.exe* služi da se uključi/isključi ova opcija. Sistemskim ključem se pored *master* ključa šifruju još i lozinke smeštene u lokalnu SAM bazu korisnika, korisnika u *Active Directory* bazi i ostale *Local Security Authority* informacije. Smešta se na hard disk te u tom slučaju nema dodatne interakcije sa korisnikom; ipak postoji mogućnost smeštanja na floppy disketu i na taj način potpunog uklanjanja sa računara. U tom slučaju korisnik mora da ubaci disketu sa sistemskim ključem kada se operativni sistem startuje. Ovu metodu treba koristiti oprezno iz razloga što, u slučaju gubitka diskete, nema način za pristup. Još je moguće koristiti dodatnu lozinku pre logovanja, jer je iz nje izveden sistemski ključ.

2.2.3.4. Potencijalni problemi i rešenja

Privremena datoteka nije izbrisana. Kada EFS šifruje datoteku, kopira njen sadržaj u privremenu, skrivenu datoteku po imenu *Efs0.tmp* u istom tom direktorijumu. Zatim šifruje početni tekst po blokovima i upisuje šifrovane podatke u originalnu datoteku. Nakon tog procesa privremena datoteka je izbrisana. Problem je u tome što EFS jednostavno označava privremenu datoteku kao obrisanu, a ne obriše je fizički sa diska, što čini moguć pristup nezaštićenim podacima veoma lakim koristeći neki od *recovery* softvera niskog nivoa. Rešenje je fizički obrisati slobodni prostor. Čak i ako je pisano preko početnog teksta, mali tragovi magnetita ostaju i tako ostavljaju šansu za čitanje obrisanih podataka uz korišćenje određene forenzičke opreme. Da bi smanjili tu šansu, koristi se komanda *cipher.exe/w*, koja će sav nealocirani prostor da sa tri prolaza prebriše. U prvom prolazu upisuje nule, u drugom jedinice a u trećem pseudoslučajni niz.

Imena datoteka u šifrovanim direktorijumima nisu zaštićena. Zapravo, šifrujući sadržaj direktorijuma automatski podrazumeva da se šifrovanje primenjuje na sve datoteke u direktorijumu, a ne na listu datoteka u direktorijumu. Pošto samo ime može sadržati osetljive informacije, to bi mogao biti sigurnosni propust. Jedno od rešenja bi bilo korišćenje šifrovanih .zip arhiva umesto direktorijuma, koje su u Windows-u tretirane skoro kao i direktorijumi. Na taj način dovoljno je da šifrujemo samo jednu datoteku da bi zaštitili sve podatke.

Posle resetiranja lozinke, ne može se pristupiti šifrovanim objektima. Kada korisnik ima potrebu za brisanjem (*reset*) lozinke, najčešće jer je zaboravljena, to će učiniti administrator. Ovo se takođe događa ako se koriste specijalni alati za brisanje lozinke npr. kada originalni operativni sistem nije aktivan ili dođe do upada sa mreže. *Master key* koji se koristi da bi zaštitio privatni ključ korisnika, je zaštićen sa ključem koji je delom nastao od tada validne lozinke. Ako se lozinka mora obrisati, onda dolazi do toga da se korisnik može logovati, ali ne može uraditi dešifrovanje. Nema rešenja, ali postoji sistemsko upozorenje kada se pokuša uraditi reset lozinke :“ *Resetting this password might cause irreversible loss of information for this user account. For security reasons, Windows protects certain information by making it impossible to access if the user's password is reset*“.

Imamo još neke primere :

- Istekao rok trajanja sertifikata. Iako se EFS sertifikati prave za 10 godina korišćenja, može doći do njihovog isteka. Rešenje – koristiti komandu *cipher.exe/u*.
- Privremene radne datoteke nisu zaštićene. Pri korišćenju npr. Office Word-a, pravi se u direktorijumu gde je dokument koji se obrađuje, privremena datoteka koja nije šifrovana kao što je sam dokument. Rešenje – šifrovati ceo direktorijum.
- Pogrešno ili zlonamerno korišćenje. Rešenje – isključiti mogućnost šifrovanja.
- Postoje još neki dodatni problemi, kao što su nešifrovana virtuelna memorija, hibernacijski režim rada, podaci koji se štampaju, antivirusni program ne može pristupiti svim datotekama i slično.

2.2.4. Međuzavisnost sa drugim kontrolama zaštite

Pošto sve mere i metode zaštite zajedno pomažu da se spreče vanredni događaji u IKT sistemu, praktično postoje međuzavisnosti ove komponente sa svim kontrolama zaštite, a najvažnije su:

- Analiza rizika: obezbeđuje alat za analizu rentabilnosti kontrola zaštite u različitim opcijama planova za vanredne događaje, koristi se za identifikovanje

kritičnih IKT objekata i izbor komponenti zaštite za sprečavanje uticaja potencijalnih pretnji za ove IKT u pripremnoj fazi procesa izrade plana.

- Fizička zaštita IKT sistema i okruženja: preventivno pomaže da se spreče vanredni događaji u IKT sistemu od pretnji kao što su požar, nestanak napajanja, poplava zbog kvara vodovodnih instalacija ili prirodnih katastrofa.
- Upravljanje incidentom: smatra se podskupom vanrednih događaja koji izazivaju tipične pretnje za IKT sistem i mora se obuhvatiti u planu za vanredne događaje.
- Operativne kontrole: periodično bekapovanje datoteka, servisa i aplikacija, sprečavanje incidenata i oporavak sistema od najčešćih pretnji kao što su kvar hard diska ili korupcija datoteka (instaliranje antivirusne zaštite na radnim stanicama), obavezne su operativne mere zaštite u svakodnevnom radu, kao i u planu za vanredne događaje.
- Politike zaštite: neophodne su za izradu i dokumentovanje procesa planiranja vanrednih događaja, eksplicitno dodeljuju odgovornosti svim zaposlenim u procesu zaštite, a posebno u slučaju vanrednog događaja (kompjuterskog incidenta).

Troškovi razvoja i implementacije plana za vanredne događaje u IKT sistemu mogu biti značajni, zavisno od izbora strategije.

2.2.5. Fuzzer alat

Neovlašćenim korisnicima najinteresantnije mete za *fuzzing* su upravo mrežne aplikacije zbog same činjenice da se koriste na Internetu i da su dostupne velikom broju korisnika. To su uglavnom mrežni servisi za popularne protokole kao što su HTTP, FTP, SMTP, POP3, SSH i slični. Broj ranjivosti koje bi se mogle pojaviti u implementaciji nekog protokola eksponencijalno raste sa kompleksnošću odnosno mogućnostima samog protokola. Cilj je napraviti *fuzzer* program koji će sa što manje testova u razumnom vremenskom periodu na što bolji način i što detaljnije testirati sigurnost aplikacije koja se ispituje [5,12].

2.2.5.1. Mrežni fuzzer alati

Mrežni fuzzer alati omogućavaju analizu sigurnosti mrežnih aplikacija, odnosno servisa. Veliki broj sigurnosnih propusta visokog sigurnosnog rizika u brojnim popularnim mrežnim aplikacijama mogu biti otkrivene jednostavnim *fuzzing* testom.

Na slici br. 2.13. imamo prikaz izgleda prozora programa Ftpfuzz kojim se povremeno može prekontrolisati ranjivost naše mreže.

Za ispitivanje sigurnosti određene mrežne aplikacije potrebno je *fuzzer* alat prilagoditi protokolu na kojem se ono zasniva. U svrhu što kvalitetnije analize, potrebno je napraviti dobru specifikaciju protokola i u okvire testa uključiti što više mogućnosti koje pruža ciljna aplikacija.

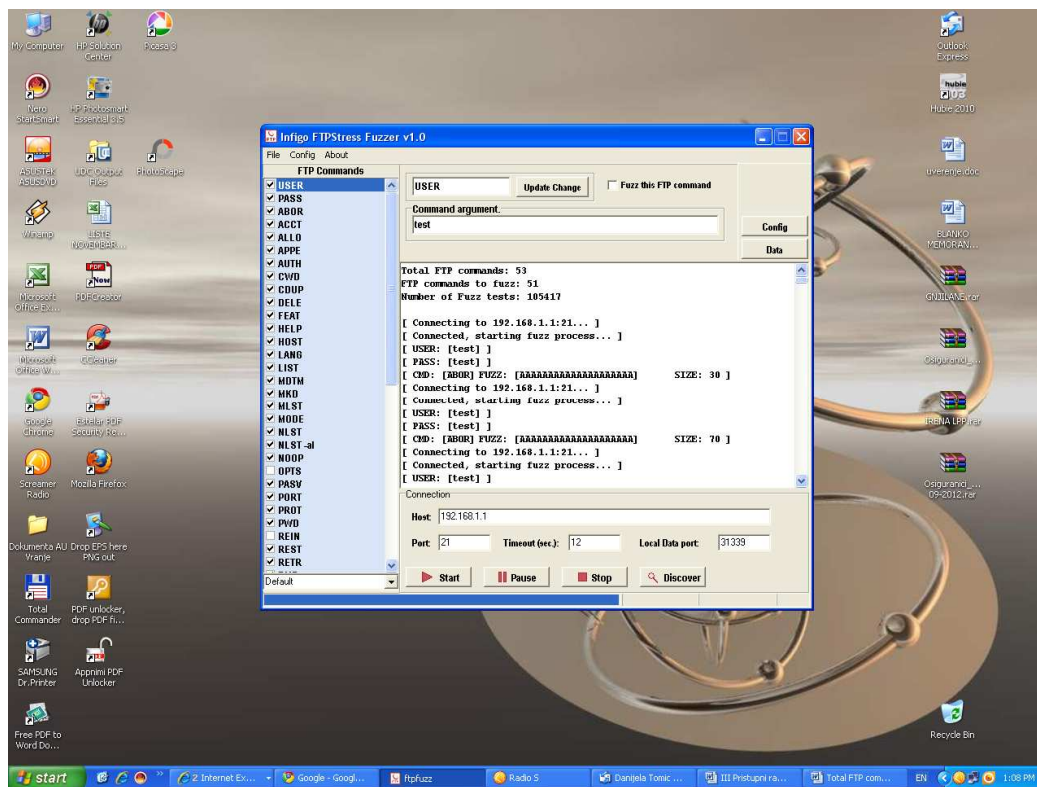
Neovlašćenim korisnicima najinteresantnije mete za *fuzzing* su upravo mrežne aplikacije zbog same činjenice da se koriste na Internetu i da su dostupne velikom broju korisnika. To su uglavnom mrežni servisi za popularne protokole kao što su HTTP, FTP, SMTP, POP3, SSH iako postoje i drugi manje popularni mrežni servisi koji mogu biti zanimljiviji za *fuzzing*.

S obzirom da ove protokole i servise svakodnevno koristi veliki broj korisnika, otkrivanje sigurnosnih ranjivosti u implementaciji tih protokola neovlašćenom korisniku daje veliki izbor ranjivih servera koje može kompromitovati. Kada se radi o *fuzzing* serverskoj aplikaciji, vrlo je bitno pokriti sve komponente protokola koji se testira, jer

izostavljanje implementacije jednog naizgled nevažnog dela protokola može rezultovati propuštanjem otkrivanja opasnih sigurnosnih ranjivosti.

Kako bi se skratilo vreme potrebno za generisanje svih mogućih ulaznih podataka koji mogu pospešiti otkrivanje sigurnosnih ranjivosti, *fuzzer* programi najčešće imaju listu predefinisanih testnih podataka i njihove definisane veličine koje će slati ciljnoj aplikaciji. Lista testnih podataka su uglavnom nizovi znakova (*string*) koji se multipliciraju do definisanih veličina i šalju u ciljnu aplikaciju. Veličina podataka koji se šalju vrlo je važna za proces *fuzzinga*. Previše kratak niz znakova najčešće neće izazvati otkrivanje bezbednosnih propusta, dok će predugačak niz znakova biti odbačen zbog dužine i ranjivost će ostati neotkrivena. Takođe, vrlo je važno da podaci koji se šalju ciljnoj aplikaciji budu u korelaciji sa protokolom koji se testira. Pritom se misli na pojedine specijalne znakove i vrednosti koje su specifične za određeni protokol, odnosno njegovu implementaciju koja se ispituje.

Navedeni alat pokazao se kao veoma uspešan u otkrivanju kritičnih bezbednosnih ranjivosti u velikom broju komercijalnih i besplatnih FTP servera. Testiranje bezbednosnih ranjivosti u serverskom softveru može se podeliti na tzv. *preauth* (ne zahteva prethodnu autentifikaciju korisnika pa je samim tim dosta opasnije) i *postauth* (ovde maliciozni korisnik treba da ima važeće korisnički ime i lozinku) ranjivosti. Dobar *fuzzer* alat trebao bi da ima mogućnost testiranja celog protokola, uključujući i *preauth* i *postauth* faze.



Slika 2.13. Osnovni prozor Infigo FTPStress Fuzzer alata

Na levoj strani glavnog prozora nalazi se lista osnovnih naredbi i ekstenzija FTP protokola.

Na desnoj strani prozora imamo nekoliko polja u kojima su dodatni parametri označene komande:

- Ime naredbe (USER)
- Argument koji naredba prima (test)
- Polje *Fuzz this FTP command* kojim se označava da li će *fuzzing* metoda biti primenjena na ovu komandu. Ukoliko je potvrdni okvir (*checkbox*) uključen, definisani argument komande se ignoriše i menja *fuzzing* vrednostima definisanim u konfiguraciji alata. Ukoliko ovo polje nije označeno, serveru se prosleđuje argument naredbe koji je naveden unutar polja *Command argument*.

Ukoliko server želimo da testiramo za *preauth* ranjivosti, USER i PASS komandama treba uključiti *Fuzz this FTP command* potvrdni okvir. Ukoliko želimo testirati *postauth* fazu komandama USER i PASS potrebno je za argumente staviti važeće korisničko ime i lozinku, kao i isključiti *Fuzz this FTP command* potvrdni okvir.

U donjem desnom uglu glavnog prozora nalaze se podaci o mreži odnosno određena IP adresa, određeni mrežni port na kome se nalazi FTP server, *timeout* vrednosti lokalni data port za prenos podataka. *Timeout* vrednost vrlo je bitna za proces *fuzzinga*, jer je pogrešnim izborom vrednosti moguće zaobići otkrivanje neke bezbednosne ranjivosti ili znatno usporiti *fuzzing* proces. Za testiranje na lokanom računaru optimalna vrednost *timeout* vrednosti je od 4 do 8 u zavisnosti od ponašanja FTP servera.

Fuzzing tehnikom moguće je u vrlo kratkom vremenskom roku otkriti kritične bezbednosne ranjivosti u raznim programskim paketima. Važno je napomenuti da *fuzzing* tehnika, iako lako primenjiva, nije konačno rešenje za otkrivanje svih bezbednosnih propusta prisutnih u nekoj aplikaciji, tako da neke ranjivosti zbog njihove prirode nije moguće otkriti *fuzzingom*.

Fuzzing metoda prvenstveno se odlikuje svojom jednostavnošću i efikasnošću kao i mogućnosti automatizacije što znatno ubrzava postupak otkrivanja bezbednosnih ranjivosti. Metoda je pogodna za veliki broj različitih programskih rešenja i proizvoda i samim tim može se koristiti kao dodatni alat u povremenom proveravanju bezbednosnih ranjivosti računara u mreži ZU Apoteka Vranje.

2.3. WEB SAJT I WEB HOSTING

CC (*Cloud Computing*) i u našoj zemlji ima relativno veliku primenu. Veoma veliki broj kompanija reklamira sebe na internetu na svojim web sajtovima. Samim tim oni zakupljuju domene i prostor na web serverima provajdera, a to je čist primer primene CC-a. ZU Apoteka Vranje ima zakupljen prostor za svoj web sajt na web serveru Telekom Srbije. Web sajt ZU Apoteka Vranje pripada kategoriji visokog nivoa usluga CC softvera u vidu servisa (*software-as-a-service*, SaaS).

2.3.1. Elementi domena

Web adresa se drugačije zove URL (*Uniform Resource Locator*). Ljudi koriste URL-ove da bi pronašli Web lokacije, a računari za to koriste IP adrese. Svaki domen sastoji se iz nekoliko elemenata koji su razdvojeni tačkom. Kao primer iskoristićemo web adresu sajta ZU Apoteka Vranje : <http://www.apotekavranje.rs>.

Ova web adresa sastoji se iz nekoliko elemenata:

- a) **http://** - skraćenica od *Hyper Text Transfer Protocol* – ukazuje na vrstu komunikacije između web pretraživača i servera i ne predstavlja deo samog domena

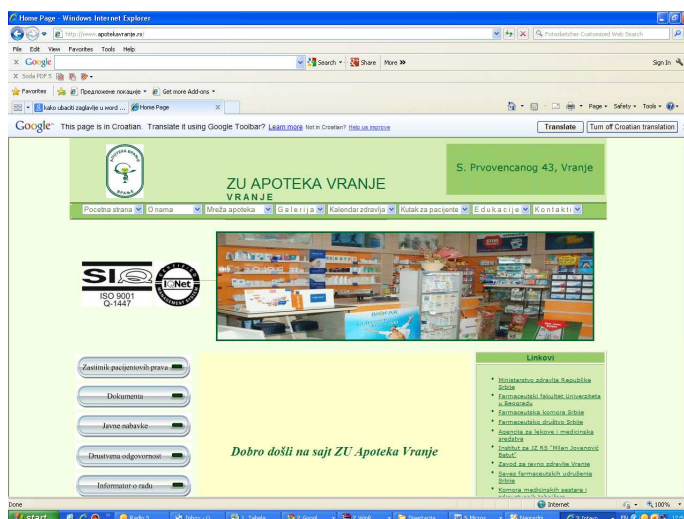
- b) **www** – skraćenica od *world wide web* (svetska internet mreža), predstavlja poddomen i prilikom registracije domena će već biti postavljen od strane domen registra
- c) **apotekavranje** – ime domena; postoji nekoliko pravila kojih se moramo pridržavati prilikom izbora imena domena a to su:
 - Ime domena može sadržati cifre (0-9), slova engleskog alfabeta (a-z) i crtice (-),
 - Dužina imena ne sme biti kraća od 2, niti duža od 63 znaka,
 - Ime domena ne sme imati razmak između reči
 - Ime domena ne sme sadržati crticu na početku i/ili na kraju (npr. www.-apotekavranje.rs ili www.apotekavranje-.rs)
 - Ime domena ne može sadržati dve uzastopne crtice (npr. na trećoj i četvrtoj poziciji = www.apoteka--vranje.rs)
 - Ime domena ne može sadržati slova neengleskog alfabeta :š,č,ć,đ,ž
- d) **rs** (ili com, org, net) – ekstenzija domena.
- e) **/domen-elementi/** - ukoliko se nalazite na bilo kojoj strani web sajta a da to nije naslovna strana, kao krajnji element domena će biti ispisano ime web strane.

2.3.2. Web sajt

Web sajt (en. *Web site*) je grupa web stranica koje čine jednu jednu celinu. Može biti smešten na lokalnom računaru, intranet serveru ili web serveru. Neki su dostupni svim ljudima, a neki imaju ograničen pristup samo članovima ili drugim određenim grupama korisnika. Web sajt može imati svoj internet domen ili poddomen.

Web sajt kompanije je glavni marketinški alat i osnova našeg poslovanja. U isto vreme to je najjeftiniji način reklame koja nam omogućava da na pravi način predstavimo sebe i svoje usluge, prezentujemo svoju delatnost, upoznamo tržište sa svojim brendovima itd. Profesionalni, inspirativni sajt, lak za upravljanje će nas najbolje predstaviti privlačeći mušterije i povećavajući prihode. Sa napretkom tehnologija vezanih za pristup internetu, uvođenjem kablovskih i ADSL operatera, povećao se i prostor za veću količinu podataka koji mogu da budu smešteni i prezentovani na sajtovima. Sada bez problema naš sajt može da sadrži flash animacije, video klipove, kompleksne baze podataka, masivne galerije fotografija. Zapravo, drugim rečima govoreći, sada se na web sajt može postaviti sve što se zamisli.

Međutim, ukoliko će se web sajt koristiti u poslovne svrhe, potrebno ga je prilagoditi za onoga kome će sadržaj biti prevashodno namenjen. Određivanje ciljne grupe, ili targetirane populacije od ključnog je značaja za svaku, dobro osmišljenu, internet prezentaciju.



Slika 2.14. Izgled stranice web sajta ZU Apoteka Vranje

2.3.2.1. Vrste web sajtova

➤ Statički

Statički web sajtovi su oni koji sadrže neke informacije koje se ne menjaju i ne osvežavaju duže vremena, ili nikad dok oni postoje.

➤ Dinamički

Dinamički web sajtovi su oni čiji se sadržaj često osvežava i dopunjava novim informacijama. To su npr. portali sa vestima, forumi, wikipedia i slični web sajtovi, na kojima možete svakodnevno, ili čak svakih nekoliko minuta, naći neki novi sadržaj i nove informacije. Ovakvi web sajtovi su većinom mnogo popularniji i mnogo posećeniji od statičkih.

2.3.2.2. Osnovni pojmovi vezani za web sajtove

- Web stranica je izvor informacija koje možete videti ili pročitati na internetu koristeći internet pretraživač. Najčešće su u HTML ili XHTML formatu i većinom sadrže linkove preko kojih možete posetiti neku drugu web stranicu. Web stranice mogu biti smeštene na lokalnom računaru, intranet serveru ili na web serveru. Većinom su kombinacija teksta i slika i ulepšane su web dizajnom, a neke od njih sadrže i audio ili video fajlove.
- Web server je računar na kojem se nalaze web stranice. Kako je pristup svakom računaru određen portovima (ulazima) koji su predstavljeni brojevima, tako je i pristup web serveru određen portom. Port za pristup web serveru je 80. Svaki server ima IP adresu, tako da kada se posećuje neka stranica, odnosno neki server, zapravo posećuje se adresa kao npr. : 212.200.191.50:80, gde broj 80 govori da se radi o web serveru. Prostor na web serveru može da se zakupi kod davaoca usluga hostinga (posluživanja) stranica. Dakle, prilikom izrađivanja stranica, da bi one bile dostupne na Internetu, potrebno je da se smeste na neki web server. Web serveri obično dolaze u vidu *cluster*a u velikim centrima podataka (eng. *Data*

center). Naravno, moguće je i od običnog računara napraviti web server, ali to nije tako dobro rešenje iz nekoliko razloga. Kao prvo, web stranice smeštene na serveru moraju biti stalno dostupne, što znači da računar mora biti stalno uključen i povezan na Internet. Takođe je potrebno imati statičku IP adresu (iako postoje određene „tehlike“ za instalaciju servera na računar koji nema statični IP). Web server bi trebao imati stalnu IP adresu, kako bi mogli registrovati domen i taj domen usmeriti na dotični IP. Na taj način posetioци ne moraju pamтити adrese (IP) servera već samo adresu kao što je npr. www.apotekavranje.rs.

2.3.3. Web Hosting

Web Hosting je mesto gde se fizički nalaze naše web stranice. Sve web stranice moraju biti smeštene na računaru koji je sve vreme vezan na Internetu tj. Web server, kako bi bile dostupne celom svetu. Mesto za naše web stranice na web serveru prodaju Web Hosting kompanije kod kojih zakupljujemo prostor na serveru na koji se stavlja naš web sajt.

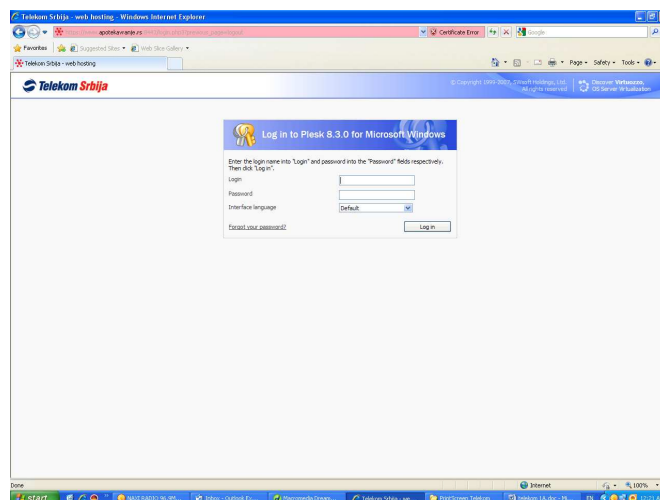
U našem slučaju uslugu Web Hostinga zakupljujemo kod proverene web hosting kompanije koja garantuje 99,9% dostupnosti našem web sajtu 24h dnevno i naš izbor je bio kompanija „Telekom Srbija“.

Usluga Web Hostinga omogućava iznajmljivanje prostora na disku i odgovarajućih serverskih resursa za smeštaj web stranica na web serveru. Uz Web Hosting uslugu Telekom Srbija omogućava svojim korisnicima stalno prisustvo na Internetu postavljanjem Web prezentacija na servere Telekoma Srbije.

Usluga Web Hosting namenjena je svim korisnicima koji žele da budu stalno prisutni na Internetu. Ovaj servis omogućava korisnicima da odgovore na zahteve savremenog poslovanja čiji je imperativ stalno prisustvo na Internetu. Postavljanjem odgovarajućeg Web sadržaja, ova usluga otvara nove mogućnosti.

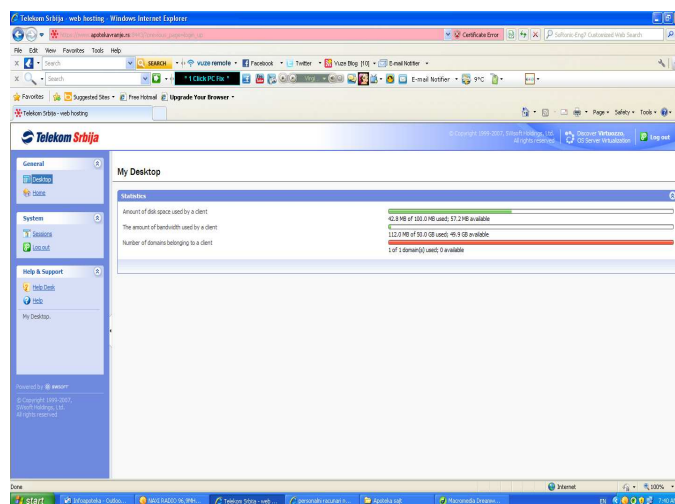
Kada se obezbedi prostor u Web okruženju, dobija se ključ za ulazak na *Cyberspace*. Ovaj ključ, u obliku korisničkog imena i lozinke, omogućava konekciju na Web Hosting server kako bi korisnik mogao da postavi svoju Web prezentaciju ili da menja njen sadržaj.

Prezentacije se mogu hostovati na Windows ili Linux platformi. Omogućen je 24x7 FTP pristup ka Web serveru radi udaljenog administriranja i ažuriranja prezentacije, uvid u statičke podatke o prezentaciji i uvid u zauzeće prostora, ostvaren saobraćaj i posećenost sajta. Izgled prozora logovanja na Web server Telekoma Srbija vidi se na slici 2.15. :



Slika 2.15. Logovanje na Web server Telekoma Srbija

Opšti statistički podaci o prezentaciji i uvid u zauzeće prostora vidi se sa slike 2.16. :



Slika 2.16. Opšti statistički podaci

Karakteristike Web Hosting paketa su:

- 24x7 FTP (*File Transfer Protokol*) pristup za administraciju sajta dostupan sa bilo koje pristupne tačke na Internetu,
- Statistika web sajta, detalja uvid u zauzeće prostora, ostvareni saobraćaj i posećenost sajta,
- Dnevni backup,
- Redundantnost sa RAID diskovima,
- Intuitivan kontrolni panel za administraciju sajta,
- *Web Site Builder* aplikacija,
- *Firewall* zaštita,
- Antivirus zaštita,
- Odgovarajući broj mail naloga (Web mail i POP3),
- Realizacija paketa na Windows ili Linux platformi.

2.3.4. Servisi

2.3.4.1. Web servisi

Razvojem Internet tehnologija dolazi se do pojave Web servisa. Web servisi omogućavaju zadovoljenje koncepta rada aplikacije u distribuiranom mrežnom okruženju. Uočena je potreba da se pojedine procedure i funkcije izvršavaju u mrežnom okruženju, pri čemu se uzimaju u obzir svi učesnici u komunikaciji. Takođe je neophodno ispuniti uslov da se rezultati istraživanja distribuiraju zainteresovanim učesnicima.

Web servisi čine integralni deo Web aplikacije i zaduženi su za specifične projektom definisane zadatke. U toku razvoja komunikacionih modula, razvijeno je više Web servisa od kojih je neophodno kao najbitnije pomenuti sledeće:

- Web servis *Formatter*: ima ulogu da prevodi format podataka koji se koristi kod klijenta ili u samom Registru u XML format putem koga se komunicira sa ostalim učesnicima u komunikaciji,

- Web servis *DataTransfer*: omogućava protok podataka, putem hardverske komunikacione opreme, do željene destinacije
- Web servis *WSPodaci*: proverava protok podataka i to kako u smislu ispravnosti formata podataka tako i u pogledu nenarušivosti integriteta podataka,
- Web servis *Autor*: proverava identitet učesnika u komunikaciji.

Web servisi moraju se instalirati na serveru.

2.3.4.2. Windows servisi

U periodu pre razvoja Web aplikacija i Web servisa, windows servisi su imali ključnu ulogu u implementaciji windows aplikacija. Pojavom Web aplikacija i Web servisa, windows servisi bivaju potisnuti u drugi plan. Iako ih mnogi smatraju recidivima prošlosti, windows servisi se i dalje koriste, najčešće sa opravdanim razlogom, jer je njihova uloga u pojedinim segmentima programiranja nezamenljiva.

Prilikom razvoja komunikacionog sistema registra razvijeno je više windows servisa, od kojih kao najbitniji treba izdvojiti *WinServiceSetup.msi*. Servis se instalira na radnu stanicu, kako bi računar mogao uspešno da komunicira sa svojim serverom u cilju obezbeđenja komunikacije Registra sa okruženjem.

Nakon instalacije opisanog servisa, pristupa se podešavanju app. config segmenta i to :

- *Konekcija* – konekcija za pristup bazi
- *PRFileStore* lokacija na kojoj se čuvaju dokumenti za razmenu,
- *TimeM.Interval* – interval u kome se startuje servis

Potom sledi podešavanje windows servisa koji se pokreće pod *account*-om koji ima pravo pristupa SQL Serveru. Na samom SQL Serveru su definisani korisnički računi sa određenim privilegijama i pravima pristupa resursima samog SQL Servera. Nakon toga se aktivira i windows servis koji ima svoju log funkciju.

Iz razloga definisanja prava pristupa SQL Server-u neophodno je podići odgovarajuće windows servise. U tu svrhu se aktivira user *prservis* (*password: prservis*) koji prihvata korisničke račune samog SQL Server-a i implementira ih u sigurnosni sistem operativnog sistema. Koordinacija sigurnosnih sistema SQL Server-a i Windows operativnog sistema je od presudne važnosti za celokupnu sigurnost pristupa podacima.

Imajući u vidu činjenicu da komunikacioni deo aplikacije prati stanje u određenim folderima neophodno je u tom smislu definisati odgovarajuće windows servise. Ovde se pre svega misli na preuzimanje fajlova iz, za to definisanih, foldera. To se vrši primenom data servisa *WSPDownload* kao i smeštanje obrađenih fajlova u propisane foldere primenom data servisa *WSPUpload*.

2.3.5. DNS server

DNS (*Domain name system*) je, u osnovi, sistem koji pretvara imena računara (*hostname*) u IP adrese. DNS takođe obezbeđuje podatke i o serverima elektronske pošte na domenu (MX), početnom DNS serveru (SOA) i druge. DNS je zasnovan na hijerarhijskom principu i jedna je od osnovnih komponenti Interneta.

Najvažniji tipovi podataka koji se čuvaju u DNS-u su sledeći:

- Tip A – adresa – povezuje ime računara i njegovu adresu,
- Tip CNAME – kanonsko ime (*Cannonical NAME*) – povezuje jedno ime računara sa drugim imenom,

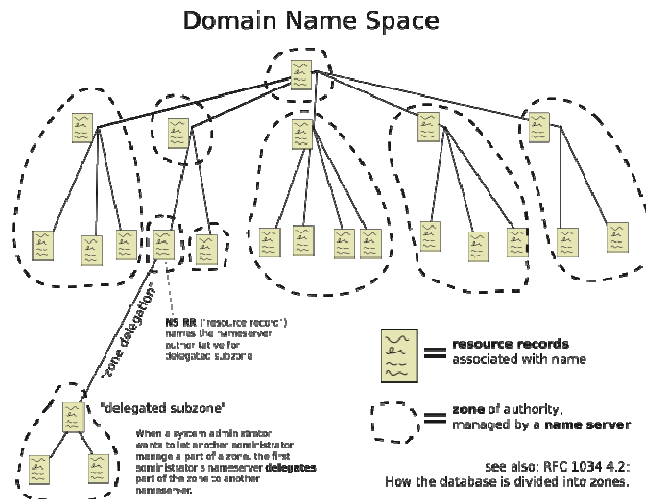
- Tip MX – razmena pošte (*Start eXchange*) – adresa servera zaduženog za elektronsku poštu,
- Tip SOA – početni autoritet (*Start Of Authority*) – adresa DNS servera koji je nadležan za domen.

DNS je u stvari jedna baza podataka u kojoj su upisana sva imena i odgovarajuće IP adrese pojedinih računara, te grupe funkcija koje omogućavaju prevođenje istih. Treba naglasiti da kompletan Internet, koji je ustvari jedna velika mreža, koristi DNS mehanizam. IP adrese DNS servera Telekoma Srbija su :

- Primarni DNS server: 212.200.190.166
- Sekundarni DNS server: 212.200.191.166

Postoje dve metode koje se, zavisno od veličine mreže, koriste za prevođenje IP adresa.

- Datoteka/etc/hosts (Linux)
U manjim mrežama je dovoljno uneti adrese i imena lokalnih računara u ovu datoteku. U nju je takođe moguće navesti i udaljene računare (npr. server provajdera). Međutim, ova metoda je statičkog karaktera jer ukoliko se neka IP adresa u međuvremenu promeni, moramo ručno uneti nove podatke.
- *Domain Name System (DNS)*
Ovaj sistem deli čitav Internet u pojedine domene. Svaki domen koristi *nameservere* koji poznaju IP adrese i imena računara koja se nalaze u području tog domena. Svi *nameserveri* su međusobno povezani u obliku stabla tako da se mogu posmatrati kao jedna velika centralna baza podataka.



Slika 2.17. Domeni složeni u stablo, podeljeni u zone, svaki opslužuje nameserver [43]

2.3.5.1. Root Domain

Pogledom na sliku br. 2.17. se može videti da se na vrhu nalazi tzv. root domen koji se označava tačkom. U praksi se ta tačka ignoriše tako da je ne moramo koristiti.

2.3.5.2. Top Level Domain

Drugo područje pripada tzv. *Top Level Domenu* (TLD) i iz njega se može otprilike pretpostaviti kojoj organizaciji ili državi taj dome pripada. Ispod ili iznad TLD ne može se nalaziti neki drugi domen.

Evo nekih čestih TLD-ova i njihovih značenja:

Tabela 2.5. Česti TLD-ovi i njihovo značenje

Domen najvišeg nivoa	Značenje
.com	Komercijalna (poslovna) lokacija
.net	Administrativna Internet lokacija
.org	Neprofitna organizacija
.gov.rs	ministarstva vlade Republike Srbije
.edu	Obrazovna ustanova

2.3.5.3. Second Level Domain

Second Level Domain je sledeće niže područje ispod TLD i označava ime pod kojim se neka firma može registrovati. Pre registracije moramo saznati da li je taj domen koji želimo slobodan. Centralno mesto za registraciju domena je InterNIC (<http://www.internic.net>). Ovde je takođe moguće prekontrolisati dostupnost slobodnih domena.

2.3.5.4. Poddomen

Ispod gore navedenih domena moguć je još jedan sloj domena koji se zove poddomen (*subdomain*). U praksi se retko susrećemo sa poddomenima jer je za njihovo korišćenje potrebno pamtiti dugačka imena. Univerziteti npr. često koriste poddomene jer su podeljeni u više stručnih područja.

2.3.5.5. Zone

Sve informacije koje se odnose na hostove snimljene su u jednoj datoteci koja se u praksi često naziva „zone-file“. Pod zonom se podrazumeva područje za koje je naš DNS server zadužen. U praksi se često za svaku zonu koristi poseban DNS server čime se znatno olakšava administracija.

2.3.5.6. Redosled ispitivanja

Ispitivanje DNS servera od strane klijenta je vrlo interesantan postupak. Razlikujemo dve vrste ispitivanja:

- Rekursivno ispitivanje
Kao prvo korisnik upisuje u svoj browser ime računara sa kojim želi da uspostavi vezu. Nakon toga se aktivira funkcija za prevođenje imena tzv. resolver koja pita lokalni DNS server za IP adresu tog imena. Server sada traži u svojoj datoteci za zonu kao i u svom cache-u. Ako nađe traženu IP adresu, vraća je clientu kao odgovor, u suprotnom vraća poruku da adresa nije uvedena.
- Forward-Lookup
Kao prvo korisnik upisuje u svoj browser ime računara sa kojim želi da uspostavi vezu. Nakon toga se aktivira funkcija za prevođenje imena tzv.

resolver koja upita lokalni DNS server za IP adresu tog imena. Server sada traži u svojoj datoteci za zonu kao i u svom cache-u. Ako nađe traženu IP adresu, vraća je clientu kao odgovor, ako ne onda taj DNS server šalje pitanje na DNS server koji je zadužen za root domen i koji mora biti unešen u lokalnom DNS serveru. Ako i ovaj ne pronade odgovarajuću adresu, onda šalje pitanje na DNS server koji je autorizovan za traženi domen. Ukoliko ovaj pronade adresu, vraća je direktno lokalnom DNS serveru, ako ne onda šalje pitanje DNS serveru zaduženom za domen koji tražimo. Postupak se ponavlja sve dok se tražena adresa ne pronade.

2.3.5.7. Cache Name Server

Zadatak jednog *Cache Name Servera* je da oslobodi odnosno rastereti druge *name* servere. U njemu ne postoji datoteka za zonu, već se sve informacije prikupljaju u sopstvenom *cache-u*. Cache je nakon podizanja sistema prvo potpuno prazan i vremenom se postepeno puni informacijama. Ako clienti često koriste iste informacije za neki udaljeni računar, intervencija će biti puno brža jer naš *Cach Name Server* nakon prvog ispitivanja udaljenih DNS servera pamti informacije u svom *Cache-u*.

2.3.5.8. Bezbedni DNS

Osnovni princip na kome se zasniva sistem DNSsec je izuzetno jednostavan. To je šifrovanje javnim ključem. Za svaku DNS zonu važe dva ključa (javni i privatni). Sve informacije koje šalje DNS server potpisuju se privatnim ključem izvorišne zone, pa primalac može da proveri njihovu autentičnost.

Sistem DNSsec nudi tri osnovne usluge:

- a) Potvrđivanje porekla podataka
- b) Distribuiranje javnog ključa
- c) Proveravanje identiteta transakcija i zahteva

Osnovna je prva usluga: podatke koji se šalju u odgovor na zahtev potvrđuje vlasnik zone. Druga usluga je korisna za bezbedno skladištenje i preuzimanje javnih ključeva. Treća služi kao zaštita od napada ponovljenim slanjem poruka i lažiranjem. Neophodno je da se obrati pažnja na to da se ne nudi usluga obezbeđivanja pošto se sve informacije u DNS sistemu smatraju javnim. Pošto se očekuje da uvođenja sistema DNSsec može potrajati godinama, neophodno je omogućiti saradnju između DNSsec i običnih DNS servera, što znači da se sam protokol ne može menjati.

DNS zapisi se grupišu u skupove zapisa resursa (*Resource Record Sets, RR-Sets*), pri čemu svaku skup sadrži zapise istog imena, klase i tipa. *RRSet* može da sadrži više *A* zapisa ako se DNS ime prevodi u primarnu i sekundarnu IP adresu. *RRSet*ovi su prošireni mnogim novim tipovima zapisa. Svaki *RRSet* se kriptografski hešira (npr. algoritmima MD5 ili SHA-1). Heš se potpisuje privatnim ključem zone. Potpisani *RRSet* je jedinična količina podataka koja se šalje klijentu. Pošto primi potpisani *RRSet*, klijent može proveriti da li je on potpisan privatnim ključem izvorišne zone. Ako je potpis valjan, podaci se prihvataju. Pošto svaki *RRSet* sadrži sopstveni potpis, *RRSet*ovi se mogu keširati bilo gde – čak i na nepouzdanim serverima – a da se ne naruši bezbednost.

DNSsec uvodi više novih tipova zapisa. Prvi je zapis *KEY*. U tom zapisu se javni ključ zone, korisnik, računar ili neki drugi principal, kriptografski algoritam koji se koristi za potpisivanje, protokol koji se koristi za prenos i još nekoliko drugih podataka. Javni ključ se u zapisu čuva nešifrovan. Sertifikati prema standardu X.509 ne koriste se jer su

preveliki. Polje za algoritam sadrži vrednost i za potpise algoritmima MD5/RSA ili druge vrednosti za druge kombinacije. Polje za protokol može da sadrži i naznaku IPsec ili neki drugi bezbednosni protokol.

Drugi zapis novog tipa je *SIG*. On sadrži heš potpisan algoritmom zadatim u zapisu *KEY*. Potpis važi za sve zapise *RRSeta*, uključujući i svaki postojeći *KEY* zapis, osim za sam zapis *SIG*. On sadrži i početak i kraj roka važnosti potpisa, ime potpisivača i još nekoliko drugih stavki.

Ustrojstvo sistema DNSsec je takvo da se privatni ključ zone ne mora čuvati na mreži. Sadržaj baze podataka za zonu može se jednom ili dvaput na dan ručno prebacivati na samostalni računar na kome se čuva privatni ključ. Tada se mogu potpisivati svi *RRSetovi* i tako dobijeni zapisi *SIG* prebaci ponovo na osnovni server zone na kompakt disku. Na taj način se privatni ključ na kompakt disku može čuvati u sefu i iz njega vaditi samo jednom ili dvaput na dan kada treba potpisati nove *RRSetove* (na računaru koji nije umrežen). Kada se završi potpisivanje, sve kopije ključa se brišu iz memorije i čvrsti disk i kompakt disk se vraćaju u sef. Takav postupak svodi elektronsku bezbednost na fizičko obezbeđivanje, nešto što funkcioniše prilično uspešno.

Prethodno potpisivanje *RRSetova* umnogome ubrzava odgovaranje na zahteve, pošto ništa ne treba šifrovati u hodu. Međutim, za čuvanje svih ključeva i potpisa iz DNS baza podataka potreban je veliki prostor na disku. Neki zapisi se posle potpisivanja desetostruko povećavaju.

Kada klijentski proces dobije potpisani *RRSet*, on na njega mora da primeni javni ključ izvorišne zone da bi dešifrovao heš, mora da izračuna heš i da uporedi dve vrednosti. Ako se vrednosti slože, podaci se smatraju ispravnim. Međutim, da bi ovaj postupak radio mora imati javni ključ zone. Jedno rešenje je da ga preuzme s pouzdanog servera putem bezbedne veze. U praksi se, međutim, očekuje da su svi klijenti unapred konfigurisani tako da znaju javne ključeve svih osnovnih domena.

DNSsec podržava i nekoliko drugih tipova zapisa. Zapis *CERT* se može koristiti za čuvanje (npr. X.509) sertifikata. Takav zapis je uveden jer neki žele da DNS sistem pretvore u PKI.

2.3.5.9. SSL – sloj bezbedne konekcije

Obezbeđivanje imena je dobar početak, ali je za bezbednost Weba potrebno mnogo više. Sledeći korak je obezbeđivanje veza. Kada je Web postao javno dobro, najčešće je korišćen za distribuiranje statičnih strana. Međutim, ubrzo su neke kompanije došle na ideju da ga koriste za finansijske transakcije: kupovinu kreditnom karticom, mrežno bankarstvo i elektronsko učešće na berzi. Za takve aplikacije su bile neophodne bezbedne veze. Godine 1995, korporacija Netscape Communications, tada glavni proizvođač Web čitača, odgovorila je na iskazanu potrebu uvodeći bezbednosni paket pod nazivom **Sloj bezbedne konekcije** (*Secure Socket Layer, SSL*). Taj softver i njegovi protokoli sada se široko koriste, takođe i u Internet Exploreru.

SSL pravi bezbednu vezu između dve utičnice, što podrazumeva :

- a) Dogovaranje parametara između klijenata i servera
- b) Međusobnu proveru identiteta klijenta i servera
- c) Tajno komuniciranje
- d) Zaštitu integriteta podataka

SSL obezbeđuje tri svojstva zaštite:

- Privatnost – podaci šifrovani simetričnim algoritmom (DES, RC4)
- Provera identiteta – identitet se proverava javnim ključem koristeći RSA
- Integritet – za proveru primljenih podataka koristi se SHA ili MD5

SSL je praktično nov sloj između sloja aplikacija i transportnog sloja, koji prihvata zahteve od čitača i šalje ih naniže protokolu TCP za slanje serveru. Pošto se uspostavi bezbedna veza, SSL uglavnom komprimuje i šifruje podatke. Kada se protokol HTTP koristi preko sistema SSL, to se zove **bezbedni HTTP** (*Secure HTTP, HTTPS*), iako se i dalje koristi standardni HTTP protokol. Međutim, on ponekad ne radi preko standardnog priključka (80), već preko novog priključka (443). SSL se ne mora koristiti samo s čitačima Weba, ali je to njegova najčešća primena.

Sloj aplikacija (HTTP)
Bezbednosni sloj (SSL)
Transportni sloj (TCP)
Mrežni sloj (IP)
Sloj veza podataka (PPP)
Fizički sloj (modem, ADSL, kablovska TV)

Slika 2.18. Slojevi (i protokoli) za čitač Weba koji koristi SSL

Protokol SSL pretrpeo je više izmena. SSL podržava niz različitih algoritama i opcija. Opcije obuhvataju prisustvo ili odsustvo kompresije, algoritme za šifrovanje koji će se koristiti i neke detalje koji se tiču izvoznih ograničenja za šifre. Ovo poslednje treba da osigura da će se ozbiljno šifrovanje koristiti samo kada su oba kraja veze u SAD. U ostalim slučajevima ključ se ograničava na 40 bitova, što kriptografi smatraju lošim vicem. Netscape je bio prisiljen da ugradi ovo ograničenje kako bi dobio izvoznu dozvolu od Vlade SAD.

SSL se sastoji od dva „podprotokola“:

- SSL Handshake – uspostavljanje sesije koja omogućava klijentu i serveru međusobnu identifikaciju i izbor algoritma i ključeva,
- SSL Record – šifrovanje i prenos poruka.

SSL podržava razne algoritme za šifrovanje. Najmoćniji od njih koristi trostruki DES s tri zasebna ključa za šifrovanje i SHA-1 za integritet poruke. Ta kombinacija je srazmerno spora, pa se najčešće koristi za elektronsko bankarstvo i aplikacije za koje je neophodan najviši stepen bezbednosti. Za obične trgovačke primere koristi se RC4 sa 128-bitnim ključem za šifrovanje i MD5 za proveravanje identiteta. RC4 koristi 128-bitni ključ kao klicu (*seed*) i proširuje ga za interno korišćenje u mnogo veći broj. Zatim taj interni broj koristi da bi generisao neprekidni ključ. Neprekidni ključ se podvrgava isključivoj disjunkciji sa osnovnim tekstom u klasičnom režimu uzastopnog šifrovanja. Izvozne verzije takođe koriste RC4 sa 128-bitnim ključevima, ali su njihovih 88 bitova javni, tako da se šifra lako može provaliti.

Za prenos podataka se koristi drugi protokol. Poruke od čitača prvo se razbijaju na jedinice veličine do 16 KB. Ako je uključena kompresija, svaka jedinica se zasebno komprimuje. Posle toga se tajni ključ koji je izveden od dva jednokratna uzorka i osnovnog ključa nadovezuje na komprimovani tekst i rezultat hešira dogovorenim algoritmom za heširanje (obično algoritmom MD5). Ovaj heš se pridružuje svakom fragmentu kao kôd za proveru identiteta poruke (MAC). Komprimovani fragment i MAC tada se šifruju dogovorenim algoritmom za simetrično šifrovanje (obično podvrgavanjem isključivoj disjunkciji sa neprekidnim RC4 ključem). Na kraju se fragmentu dodaje zaglavlje i sve se prenosi TCP vezom.

Treba ipak upozoriti na oprez. Pošto je pokazano da RC4 ima neke slabe ključeve koji se lako mogu analizirati, bezbednost SSL-a zasnovana na RC4 stoji na klimavim

nogama. Čitače koji korisnicima omogućavaju da biraju skup šifara treba konfigurisati tako da sve vreme koriste trostruki DES sa 168-bitnim ključevima i SHA-1, iako je ta kombinacija sporija od RC4 i MD5.

Drugi problem je to što principi možda nemaju sertifikate ili to što dok koriste SSL ne proveravaju uvek da li korišćeni ključevi odgovaraju sertifikatima.

Godine 1996. korporacija *Netscape Communications* ponudila je SSL organizaciji IETF za standardizovanje. Rezultat je bio **Bezbednost transportnog sloja** (*Transport Layer Security, TLS*), protokol opisan u RFC dokumentu 2246.

SSL je srazmerno malo izmenjen, ali dovoljno da njegova treća verzija ne može da sarađuje sa TLS-om. TLS je poznat i kao SSL verzije 3.1. Prve realizacije su se pojavile 1999, ali još uvek nije jasno da li će sistem TLS u praksi zameniti SSL, uprkos tome što je malo jači. Međutim, problem sa slabim RC4 ključevima i dalje ostaje.

Komunikacija između klijenta i servera se odvija uz pomoć poruka. Poruke odnosno njeni formati su unapred definisani:

- **Alert** – obaveštava entitete u komunikaciji o mogućem sigurnosnom propustu ili grešci u komunikaciji
- **ApplicationData** – podaci koje dve strane razmenjuju, šifrovani su, autentifikovani i verifikovani su od strane SSL-a
- **Certificate** – poruka koja prenosi sertifikat sa javnim ključem
- **CertificateRequest** – zahtev servera klijentu za klijentovim sertifikatom
- **CertificateVerify** – poruka kojom klijent potvrđuje da ima tajni ključ koji odgovara javnom ključu u sertifikatu
- **ClientHello** – poruka od strane klijenta kojom obaveštava server o sigurnosnim servisima koje želi i koje podržava
- **ClientKeyExchange** – klijentova poruka koja sadrži kriptografske ključeve za komunikaciju
- **Finished** – obaveštenje da su svi koraci pregovora gotovi i da je uspostavljena sigurna komunikacija
- **HelloRequest** – zahtev servera klijentu za početak pregovora oko sigurnosnih parametara u komunikaciji
- **ServerHello** – poruka kojom server javlja koji će sigurnosni servisi biti korišćeni
- **ServerHelloDone** – obaveštenje servera da je poslao sve zahteve klijentu za uspostavljanje komunikacije
- **ServerKeyExchange** – poruka servera koja sadrži kriptografske ključeve za komunikaciju

Opis postupka:

- Klijent šalje *ClientHello* poruku predlažući parametre za SSL komunikaciju
- Server odgovara sa *ServerHello* porukom i bira parametre
- Server šalje svoj javni ključ u *ServerKeyExchange* poruci
- Server zaključuje svoj deo pregovora sa *ServerHelloDone* porukom
- Klijent šalje ključ šifrovan javnim ključem servera u *ClientKeyExchange* poruci
- Klijent šalje *ChangeCipherSpec* poruku da bi aktivirao sigurnosne opcije za sve buduće poruke
- Klijent šalje poruku *Finished* i javlja serveru da proveri nove opcije
- Server šalje *ChangeCipherSpec* poruku kako bi aktivirao sigurnosne opcije za svoje buduće poruke
- Server šalje poruku *Finished* i javlja klijentu da proveri nove opcije

Moguće greške u SSL protokolu:

- Neispravna MAC vrednost – prekid veze, sumnja na napad
- Greška prilikom dekomprimovanja delova poruke
- Greška pri uspostavljanju sesije – neusklađeni predloženi atributi zaštite
- Neočekivana poruka – prekid veze
- Neodgovarajući parametri koji se odnose na sertifikate – nevažeći sertifikat, nepodržavanje sertifikata od strane protokola ili nepostojanje istog

2.3.6. Sistem zaštite web transakcija

Jedna od najrasprostranjenijih standardnih klijent-server Internet opštenamenskih aplikacija je *http* komunikacija ili Web servis u okviru koga je potrebno realizovati pouzdan sistem zaštite. Za tu namenu je razvijeno, verifikovano i u praksi dokazano rešenje sistema zaštite Web servisa pod imenom zaštićene Web transakcije – *SWT*.

U okviru pomenutog rešenja, u skladu sa odgovarajućom usvojenom politikom zaštite predviđa se višeslojna struktura i slojevitost sistema zaštite. U odnosu na kriptografski kvalitet i kompletnost rešenja, sistemi za zaštitu Web transakcija se mogu podeliti na sledeće 4 kategorije rešenja:

- Sistem sa uključenom zaštitom samo na aplikativnom nivou i nezaštićenom – otvorenom *http* komunikacijom na transportnom nivou,
- Sistem zaštite na aplikativnom nivou i korišćenje standardnog *SSL* protokola za zaštitu *http* komunikacije klijenta i servera na transportnom nivou, pri čemu se u fazi autentifikacije razmenjuju sopstveno realizovani digitalni sertifikat Web servera,
- Sistem zaštite na aplikativnom nivou i korišćenje standardnog *SSL* protokola za zaštitu *http* komunikacije klijenta i servera na transportnom nivou, pri čemu se u fazi autentifikacije razmenjuju sopstveno realizovani digitalni sertifikati koji su ugrađeni u Web server i klijentski Internet browser program,
- Korišćenje prethodno opisanog sistema *SWT* sa realizacijom kriptografske zaštite koja je u potpunosti samostalno realizovana, kako na aplikativnom tako i na transportnom nivou.

U ZU *Apoteka Vranje* zastupljena je opcija realizacije Web transakcija zasnovana na drugoj navedenoj opciji, koja je izabrana iz razloga kvaliteta zaštite, kao i optimalnog vremena potrebnog za projektovanje i implementaciju. Ova opcija uključuje *SWT* mehanizme zaštite na aplikativnom nivou i *SSL* protokol na transportnom nivou.

SWT je namenjen za integraciju u savremene client-server arhitekture koje se realizuju na *TCP/IP* mrežnim protokolima, uz primenu Web aplikativnih tehnologija. *SWT* sistem je razvijen sa ciljem kriptografske podrške komunikaciji između Web klijenta pri čemu se koriste standardni Internet browser program i Web server implementacija kvalitetnih kriptografskih funkcija. *SWT* sistem je prvenstveno namenjen za zaštitu u sistemima elektronske trgovine i poslovanja ali se može koristiti i za kompletnu zaštitu bilo koje *http* komunikacije. Sistem *SWT* je sličan standardizovanom i široko rasprostranjenom *SSL* protokolu. Međutim, *SWT* sistem ima četiri osnovne prednosti u odnosu na *SSL* protokol:

- a) Sistem *SWT* realizuje funkcije zaštite podataka na aplikativnom nivou korišćenjem asimetričnih i simetričnih kriptografskih sistema,
- b) Sistem *SWT* uključuje originalnu proceduru autentifikacije klijenta i servera za uspostavljanje kriptografskog tunela na transportnom nivou, kriptografski jaču od procedure autentifikacije primenjene u *SSL* protokolu,

- c) Obzirom da predstavlja proizvod domaćeg razvoja i da je pod punom kontrolom proizvođača, sistem *SWT* uključuje mogućnost, pored ugradnje standardnih odnosno javnih algoritama i ugradnju privatnih simetričnih algoritama, definisan od strane samih korisnika, kako za zaštitu tajnosti podataka na aplikativnom nivou, tako i za realizaciju kriptografskih tunela na transportnom nivou,
- d) Obzirom da je plod domaćeg razvoja, sistem *SWT* je moguće u potpunosti verifikovati na nivou izvornog koda.

U sistemu *SWT* se primenjuje kombinacija tehnika za realizaciju kriptografskog tunela na transportnom nivou i zaštite na aplikativnom nivou korišćenjem simetričnih i asimetričnih šifarskih sistema.

2.3.6.1. Kriptografski mehanizmi zaštite u troslojnoj arhitekturi

U kontekstu savremenih kretanja, kao opšteprihvaćeni trend u razvoju Internet aplikacija, primenjuju se troslojne ili višeslojne arhitekture aplikacija na bazi Web komunikacije. U tom smislu, tipična troslojna aplikacija se sastoji od:

- a) Klijenta
- b) Web servera i
- c) Baze podataka.

Pri tome, klijent najčešće predstavlja standardni Internet browser program, dok Web server može biti kombinacija Web servera i aplikativnog servera.

Sistem zaštite ovakve arhitekture se generalno sastoji iz dva segmenta :

- a) Zaštita između klijenta i Web servera i
- b) Zaštite između Web servera i servera baze podataka.

Zaštita između klijenta i Web servera je ostvarena primenom mehanizama zaštite na aplikativnom i transportnom nivou. Zaštita između Web servera i servera baze podataka je realizovana primenom mrežne barijere – *firewall*. Ova mrežna barijera ima veoma bitnu i osetljivu ulogu krajnje instance zaštite servera baze podataka, tako da je neophodno da to bude kriptografski što kvalitetnija mrežna barijera. U tu svrhu se koristi *KPS* server zaštite, kao sopstvena mrežna barijera na aplikativnom i transportnom nivou, koji poseduje dve mrežne kartice za bezbednu separaciju mrežnih segmenata. Prilikom korišćenja kombinacije Web servera i aplikativnog servera, *KPS* server zaštite je postavljen između aplikativnog servera i baze podataka. U tom slučaju, ukoliko je neophodno, i shodno konfiguraciji mreže, dodatna bezbednost se postiže primenom dodatnog *firewall*-a između Web servera i Web aplikativnog servera.

U ovakvoj konfiguraciji je neophodno da se na Web serveru ili na Web aplikativnom serveru, ugradi kriptografska komponenta, pod nazivom *KPS gateway*, koji služi za uspostavljanje kriptografske komunikacije – jaka autentifikacija i kriptografski tunel između Web aplikativnog servera i servera baze podataka.

2.3.6.2. Zaštita na aplikativnom nivou

Zaštita na aplikativnom nivou Web komunikacije u okviru ZU Apoteka Vranje realizovana je primenom *SWT* aplikativnog modula zaštite koji se bazira na originalnoj proceduri autentifikacije, klijentskom softveru koji realizuje simetrične i asimetrične kriptografske algoritme i odgovarajućem tokenu za smeštanje kriptografskih parametara

kao i odgovarajućem serverskom softveru zaštite koji je instaliran na aplikativnom serveru ZU Apoteka Vranje i koji služi kao drugi kraj u zaštiti od klijenta do servera.

Moguće su tri varijante rešenja zaštite na aplikativnom nivou:

- a) Rešenje koje se bazira na korišćenju korisničkog imena i lozinke, kao i na čisto softverskoj klijentskoj kriptografskoj aplikaciji,
- b) Rešenje koje se bazira na korišćenju korisničkog imena i lozinke, kao i na klijentskoj kriptografskoj aplikaciji koja se zasniva na korišćenju mini CD-a, kao dodatne hardverske komponente,
- c) Rešenje koje se bazira na korišćenju korisničkog imena i lozinke, kao i na klijentskoj kriptografskoj aplikaciji koja se zasniva na korišćenju smart kartice, kao dodatne hardverske i kriptografske komponente.

U ZU Apoteka Vranje koristi se prva pomenuta varijanta. U ovoj varijanti kriptografski ključevi, simetrični i asimetrični, čuvaju se šifrovani na hard disku klijentskog računara. Ovo rešenje je najjednostavnije i najjeftinije. Međutim, ovo rešenje se bazira na jednokomponentnoj proceduri autentifikacije, samo korišćenjem onoga što se zna – korisničko ime i lozinka, što je nedovoljno bezbedno sa kriptografskog stanovišta, jer su ključevi smešteni u okviru nebezbednog okruženja operativnog sistema klijentske radne stanice. Takođe, nije obezbeđena funkcija neporecivosti transakcija u slučaju primene tehnologije digitalnog potpisa.

U sva tri slučaja bilo bi moguće klijentski softver instalirati na klijentu ili ga pokretati sa Web aplikativnog servera.

2.3.7. Primer realizacije funkcionalnog modela TTPS provajdera

Funkcionalni model TTPS treba da obuhvata različite tipove i nivoe usluga, identifikovanih kroz različite korisničke zahteve, kao i sve pravilnike i uputstva za menadžment i rad TTPS provajdera. Sva relevantna pitanja koja treba sagledati u izgradnji funkcionalnog modela TTPS provajdera, razmatrana su na primeru uloga TTPS u PKI u zdravstvenom informacionom sistemu (ZIS).

2.3.7.1. Opšti model TTPS za PKI u ZIS

Relevantne uloge TTP u ovom modelu su:

- PKI telo za registraciju (*PKI Registracion Authority* – PKIRA): entite (individua ili organizacija) koji jedinstveno identifikuje i registruje korisnike koji zahtevaju obezbeđenje servisa digitalnog potpisa – DS;
- (*Professional Registration Authority* – PrRA) – Telo za registraciju profesionalno zaposlenih. Ovo je entitet (autoritet) koji registruje profesionalno zaposlene pojedince u oblasti zdravstva.
- (*Professional Certificate Authority* – PrCA) – Telo za sertifikaciju profesionalno zaposlenih
- User (*Health care professional*) – Korisnici (profesionalni zdravstveni radnici)
- (*Naming Authority* – NA) – Telo za imenovanje je entitet koji daje jedinstven sertifikat korisnicima i upravlja sa imenikom klasa: profesija (npr. lekar opšte prakse), specijalizacija (npr. interna medicina) i mogućih sub-specijalizacija (npr. nefrolog).
- (*PKI Certificate Authority* – PKCA) – Telo za sertifikaciju javnih ključeva je entitet koji izdaje sertifikate (opotiva i ponovo ih izdaje) određujući jedinstvenu

vezu između sertifikata i javnog ključa za DS ili ključeva za PKI izdavanjem sertifikata javnog ključa potpisanog od strane PKCA.

- (*Card issuing system – CIS*) – Sistem za izdavanje identifikacione kartice je entitet koji izdaje čip-karticu sa DS i/ili sa ključem za dešifrovanje, a koja sadrži najmanje privatne ključeve korisnika (vlasnika).
- (*Local/central key generator – LKG/CKG*) – Lokalni/centralni generator ključeva je entitet lociran u lokalu (kod korisnika ili PKRA) ili u centru (kod PKCA ili CIS) koji generiše zahtevane parove javnih ključeva.
- (*Certificate directory – DIR*) – Imenik sertifikata je entitet koji obezbeđuje sertifikate javnih ključeva, sertifikate profesionalno zaposlenih, liste opozvanih sertifikata i moguće druge informacije o korisnicima po zahtevu drugih korisnika.
- (*Public key registration – PKR*) – Registracija javnih ključeva

2.3.7.2. Modelovanje poverenja i sigurnosti TTP servis provajdera

Poverenje se definiše kao zbir očekivanja i pretpostavki koje korisnici servisa i drugi učesnici imaju i potencijalne mogućnosti konkretne organizacije i njenog tehničkog sistema da obezbedi zahtevane servise na takav način da se potvrđuju relevantna politika zaštite i druga navedena svojstva TTPS provajdera, kao što su funkcionalnost, cena itd. Treba razlikovati funkcionalno i безусловno poverenje u TTP.

Funkcionalno poverenje se zasniva na verovanju korisnika u sposobnost TTP da izvrši svoje servise i funkcije u skladu sa planiranim obavezama, bez otkrivanja poverljivih podataka i informacija bilo kojeg korisnika servisa.

Bezuslovno poverenje je ono što korisnik mora imati u TTPS provajderu, koji rukuje (generiše, skladišti, i/ili komunicira) njegovim poverljivim podacima i informacijama. Korisnik mora verovati da TTP neće zloupotребiti privatne informacije ili njima manipulirati na taj način da mogu biti kompromitovane od drugih lica. Primer безусловnog poverenja u TTPS provajdera je generisanje privatnih (tajnih) ključeva.

Stepen sigurnosti (uverenje) definiše se kao svojstvo tehničkog ili/i organizacionog sistema koji obuhvata sve najvažnije sastavne elemente TTP. Ovo svojstvo indicira stepen do kojeg su funkcionalnost i drugi tehnički i organizacioni aspekti TTP prihvatljivi za date servise i ciljeve ovih servisa. Ovo svojstvo, takođe, indicira do kojeg je stepena TTP stvarno sposoban da izvrši nameravane ili navedene funkcije. Može se reći da visok stepen sigurnosti obezbeđuje visoko poverenje, ali ne važi i obrnuto.

Osim bezbednosnih zahteva, zavisno od konkretne politike zaštite, postoje za svaki specifični sektor delatnosti i drugi zahtevi za TTPS provajdera, kao što su pogodnost i iskoristivost servisa (npr. organizacija i funkcionisanje PKI i tela za registraciju profesionalno zaposlenih i interakcija sa imenikom servisa). Posebno značajno može postati bezbednosno pitanje stepena kontrole korisnika nad ulogom TTPS provajdera koji zahteva безусловno poverenje (npr. generisanje ključa, zbog zahteva vlade da ga može pratiti).

2.3.7.3. Zakonodavna pitanja

Izgradnja funkcionalnog modela TTPS provajdera zaštite podrazumeva istovremeno rešavanje svih relevantnih zakonskih i administrativnih pitanja koja se odnose na formiranje pojedinih nadležnih tela i institucija namenjenih za obezbeđenje svih potrebnih funkcionalnih i zakonskih aspekata rada TTPS provajdera.

Zakonodavna pitanja koja je potrebno rešavati u vezi sa uspostavljanjem pojedinih entiteta i organizacija u funkciji TTPS provajdera zaštite mogu se svrstati u sledeće kategorije:

- regulativa zaštite privatnosti (ličnih podataka)
- zaštita profesionalne tajne
- pouzdanost, pitanja evidencije i ugovornih obaveza
- regulativa za kriptozastitu i kompjuterski kriminal
- zaštita prava vlasništva i intelektualne svojine
- definisanje oblasti praktičnog delovanja profesionalnih (strukovnih) udruženja

2.3.7.4. Predlozi za realizaciju univerzalnog TTPS provajdera

Kao praktične posledice uvođenja elektronskog poslovanja i ubrzane informatizacije svih sektora društva (zdravstva, bankarstva, pravosuđa, itd.), treba očekivati značajan porast svih vrsta kompjuterskog kriminala. U tom smislu, u daljem radu u oblasti uspostavljanja zakonske regulative funkcija i mreže TTPS provajdera zaštite u IS, pažnju treba usmeriti na rešavanje sledećih pitanja:

- a) Politika kriptozastite (poverljivosti, integriteta i autentičnosti) korisnika i podataka u svakom IS, mora uključiti nužna zakonska ograničenja u pogledu korišćenja mehanizama kriptozastite (sertifikacija, i dr.).
- b) U zaštiti prava na intelektualnu svojinu razmatrati posledice neovlašćenog korišćenja baza podataka autora od strane legitimnih korisnika, kao i mogućnost zaštite tih prava, upotrebom tehnologija digitalnog vodenog pečata (*Digital Watermarking*)
- c) U skladu sa zakonom o zaštiti ličnih podataka, razmatrati ko treba u IS supervizirati poverljive podatke i kako definisati i harmonizovati koncept vlasništva.
- d) U slučaju spora i sudske procedure oko elektronskih podataka u IS, podrazumeva se, da se dokazni postupak odvija u oblasti elektronskih medija. Potrebno je zakonski jasno definisati prihvatljive forme elektronskih dokaza, profil eksperata za sudsko veštačenje, uslove obaveznog prihvatanja istih kao sudskih veštaka u oblasti IT, i uslove prihvatanja digitalnih dokaza kao sudski validnih.
- e) Analizirati opravdanost i eventualno regulisati potrebu administrativne prakse da se odgovarajući ugovori, osim u klasičnoj pisanoj formi, prave i potpisuju i u digitalnoj formi, gde god se podaci razmenjuju i manipulišu u elektronskoj, digitalnoj formi.
- f) Zakon na nacionalnom nivou treba da precizno definiše i stalno ažurira uslove za izbor kompetentnih tela (institucija) za akreditacije i sertifikacije i obavezu da sertifikate izdaju osim u papirnoj i digitalno potpisane u elektronskoj formi.
- g) Racionalno je istraživati prikladne kodove za kodifikaciju raznih ugovornih obaveza koje regulišu razne zakonske obaveze (odgovornost, dokazi, privatnost, intelektualno vlasništvo, itd.) između različitih učesnika u konkretnom IS
- h) U procesu definisanja politike i izrade funkcionalne infrastrukture TTPS provajdera, potrebno je da TTPS provajder izradi svoj operativan (iskoristiv) digitalni potpis i sa njim istovremeno zahteva bezuslovno poverenje korisnika i sudskih organa kod kojih se mora registrovati.
- i) Razvoj TTP servisa i mreže TTPS provajdera treba da određuju tržišni uslovi na otvorenom i konkurentnom tržištu, da bi se izbeglo zakonsko nametanje entiteta kao TTPS provajdera za neke servise, kao i monopol pojedinih institucija na neke

servise (akreditacije i sertifikacije) i omogućilo pravo korisnika na izbor TTPS provajdera.

2.4. CLOUD COMPUTING

2.4.1. Šta je *Cloud Computing* ?

U roku od samo nekoliko meseci, CC (*Cloud Computing*), nekada relativno malo poznat koncept, postao je najprimamljivija tehnologija godine. Čitav niz kompanija pridružio se novom trendu, lansirajući nove usluge vezane za CC. IBM, Yahoo i Google su udružili moć CC-a za posao.

Danas svi govore o CC-u, ali čini se da svako koristi drugačiju definiciju, u zavisnosti od svoje pozicije. Oni koji rade u oblasti usluga imaju drugačiju definiciju CC-a od onih koji rade na sistemskoj arhitekturi.

Gartner i Forest imaju sledeću definiciju:

„Oblast računarstva u kojoj se veoma skalabilni informatički kapaciteti obezbeđuju u vidu usluge isporučene putem interneta brojnim eksternim potrošačima.“

Daryl Plummer ima sledeću definiciju:

„Apstrahovana, visoko skalabilna i kontrolisana kompjuterska infrastruktura koja hostuje aplikacije namenjene krajnjim korisnicima i čije se usluge naplaćuju na bazi ostvarene potrošnje.“

I Intel ima sopstvenu definiciju CC-a, koja uzima u obzir njegovu arhitekturu i usluge, pri čemu postoji razlika između javnih i privatnih CC mreža:

- Arhitektura CC: usluge i podaci egzistiraju u deljenom, dinamički skalabilnom skupu resursa zasnovanom na tehnologijama virtuelizacije i/ili skaliranim aplikativnim okruženjima.
- Usluge CC-a: servisi za potrošače ili kompanije realizuju se putem javnog interneta. Oslanjajući se na arhitekturu CC, skaliranje usluga vrši se bez intervencije korisnika i obično se naplaćuje na osnovu ostvarene potrošnje.
- Privatni CC: arhitektura oblaka je smeštena iza *firewall*-a organizacije i pruža informatičke usluge za internu upotrebu.

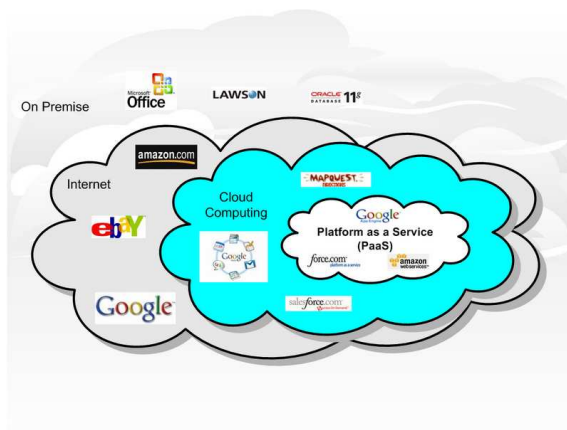
U CC sistemu postoji značajan napredak u radu. Lokalni računari ne moraju više da izvršavaju teške poslove prilikom izvršavanja aplikacija. Mreža računara koja kreira oblak obavlja te poslove umesto lokalnih računara. Hardverski i softverski zahtevi na strani korisnika se smanjuju. Jedina stvar koju korisnik mora da ima da bi mogao da radi u CC sistemu je softverski interfejs, koji može biti običan Web Browser, a CC mreža obavlja sve ostalo. CC od tradicionalnog internet servisa razdvaja inherentna dinamička i fleksibilna arhitektura koja omogućava korisnicima informatičkih tehnologija da plaćaju samo one usluge koje su im zaista potrebne, kao i da u kratkom vremenskom roku višestruko povećaju njihov obim.



Slika 2.19. Računari u oblaku [42]

Postoje veoma velike šanse da mi već koristimo neku formu CC-a. Ako imamo e-mail nalog sa web baziranim e-mail servisima kao što su Hotmail, Yahoo!Mail ili Gmail, onda imamo neko iskustvo sa CC-om. Umesto izvršenja e-mail programa na našem računaru, mi prilazimo Web e-mail nalogu udaljenom od nas. Softver i skladišni prostor za naš nalog ne postoji na našem računaru, on je na servisima kompjuterskog oblaka.

Dok je procenu teško naći, potencijalna upotreba je rasprostranjena. Umesto korišćenja relativno male grupe visoko obučених korisnika, cilj CC je da se omogući svim korisnicima. Javne usluge CC-a uglavnom su usmerene ka potrošačkim uslugama kao što je pretraživanje na internetu, lični e-mail servisi, društveno povezivanje (*social networking*), reklamiranje i predstavljanje preduzeća na internetu i druge primene interneta.



Slika 2.20. Šta je Cloud Computing? [42]

2.4.2. Ko pruža usluge *Cloud Computing*-a?

Postoje tri kategorije visokog nivoa usluga CC-a:

- Softver u vidu servisa (*software-as-a-service*, SaaS) – softver koji je implementiran u obliku hostovanog servisa kome sa pristupa putem interneta. Kod SaaS modela većinu odgovornosti za bezbednost upravljanja preuzima cloud provajder. SaaS obezbeđuje više načina za kontrolu pristupa web portala, kao što je upravljanje identitetima korisnika, aplikacija na nivou konfiguracije i

mogućnost da ograničite pristup određenim IP adresama opsega ili geografskog područja.

- Platforma u vidu servisa (*platform-as-a-service*, PaaS) – platforme koje mogu biti korišćene za realizaciju aplikacija obezbeđenih od strane klijenata ili partnera provajdera platforme. PaaS omogućava klijentima da preuzmu više odgovornosti za upravljanje konfiguracijom i bezbednošću baze podataka i softverskih aplikacija.
- Infrastruktura u vidu servisa (*infrastructure-as-a-service*, IaaS) – računarska infrastruktura, kao što su serveri, skladištenje podataka i umrežavanje, ostvarena u vidu CC-a, obično korišćenjem virtuelizacije. IaaS prebacuje još više kontrole i odgovornosti za bezbednost od cloud provajdera ka klijentu. U ovom modelu dozvoljen je pristup operativnom sistemu koji podržava virtuelne slike, umrežavanje i skladištenje.



Slika 2.21. Taksonometrija Cloud Computing-a [43]

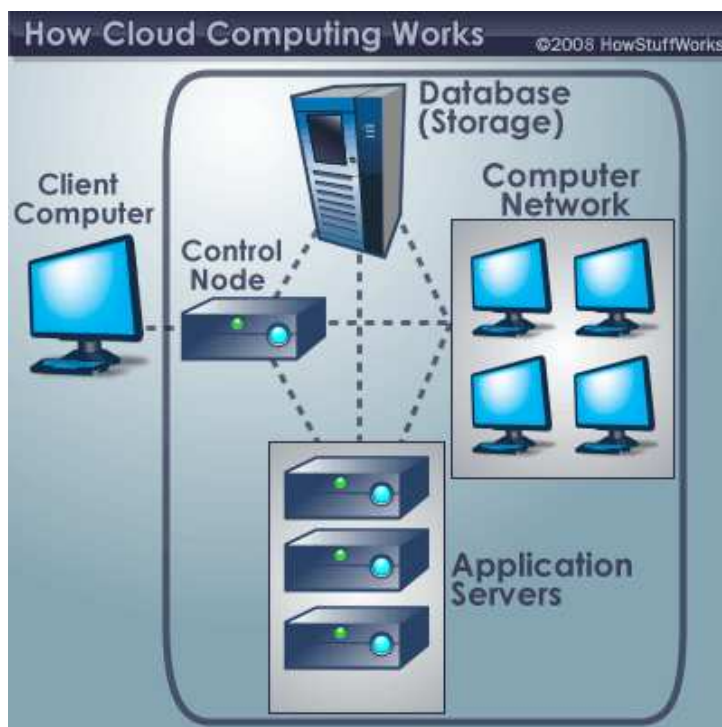
Kroz SaaS, kompanije mogu da priđu aplikacijama i velikoj količini virtualne računarske moći bez kupovine istih. Umesto toga, aplikacije su hostovane od strane drugih kompanija, što ih oslobađa glavobolja održavanja i većine troškova podešavanja za korisnike. Neke SaaS aplikacije mogu da funkcionišu putem konekcije između samo dva ili tri računara.

Zašto se ovaj model naziva CC? Neki kažu da je to zato što se kompjuterska funkcionalnost izvršava negde „u oblacima“. Eksperti Wikipedie tvrde da termin dolazi iz činjenice da mnogi tehnološki dijagrami opisuju Internet ili IP strukturu koristeći crtanje oblaka.

Po analitičarima u Gartner-u, vodećoj IT istraživačkoj kompaniji do 2011. godine, rana tehnološka usvajanja će se odreći kapitalnih troškova i umesto toga naručiti 40% njihove IT infrastrukture u vidu servisa. Povećanje brzih konekcija omogućava praktično korišćenje infrastrukture na drugim mestima i dobijanje rezultata u željenom vremenskom periodu. Preduzeća veruju da kako servisno-orjentisana arhitektura (SOA) postaje sve češća, CC će se baviti odvajanjem aplikacija sa specifične infrastrukture.

Neke od vodećih IT kompanija investiraju u razvoj CC-a od kojih ćemo spomenuti: IBM, Google, HP, Yahoo, Intel, Microsoft, Apple, Amazon, Salesforce. HP, Intel i Yahoo su objavili da su se udružili da bi kreirali „Test Postolje“, projekat za istraživanje u CC-u, opšti tim za vanjske hardverske i softverske kapacitete umesto manipulisanja njime u lokalnu, dok je Microsoft objavio *Live Mesh Cloud Computing* platformu čime se omogućava korisnicima povezivanje svih njihovih uređaja u CC mrežu. Google je otišao korak dalje i ostvario je veliki uticaj integracijom CC-a u mobilne uređaje. Kompanija je u

skorije vreme objavila Android, platformu koja omogućava ljudima izgradnju softvera za razne mobilne uređaje.



Slika 2.22. Kako radi Cloud Computing [42]

2.4.3. Bezbednost u Cloud Computing-u

CC je fleksibilna, ekonomična i proverena platforma za isporuku i pružanje poslovnih ili potrošačkih IT usluga putem interneta. Kao dodatna prednost, CC poboljšava korisničko iskustvo bez povećanja složenosti. Korisnici ne moraju da znaju ništa o korišćenim osnovnim tehnologijama ili implementacijama.

I javni i privatni cloud modeli su sada u upotrebi. Dostupni su svakome na internetu. Javni modeli uključuju Softver kao servis (SaaS) cloud kao što je IBM LotusLive, Platforma kao servis (PaaS) cloud kao što je IBM Računarstvo na zahtev i bezbednost i zaštita podataka kao servis (SDPaaS) cloud kao što je IBM Menadžment servis ranjivosti.

Pored standardnih izazova razvoja bezbednih informacionih sistema, CC predstavlja dodatni nivo rizika, jer su osnovne usluge dostupne trećoj strani. „Spoljašnji“ aspekt dostupnosti čini težim za održavanje integriteta i privatnosti podataka, podrške podataka i dostupnosti servisa i pokazivanja elastičnosti.

Masivno deljenje infrastrukture na CC-u stvara značajnu razliku između cloud bezbednosti i bezbednosti u više tradicionalnom IT okruženju. Korisnici povezuju različite korporacije i nivoe poverenja često komunicirajući sa istim setom kompjuterskih resursa. U isto vreme, ravnoteža posla, promena servisnog nivoa sporazuma (SLAs) i drugih aspekata današnjeg dinamičkog IT okruženja stvaraju još više mogućnosti za dekonfiguraciju, otkrivanje podataka i zlonamerno ponašanje.

Infrastruktura deljenja poziva na visok stepen standardizacije i automatizacije procesa, a to može poboljšati sigurnost eliminišući rizik od greške operatera i previda. Međutim,

rizici nerazdvojni od masovne deljene infrastrukture znače da CC modeli moraju i dalje naglasiti značaj izolacije, identiteta i istinitosti.

Organizacija zahteva uvid u bezbednosno stanje svojih CC-ova. Ovo uključuje širok uvid u promene, imidž i upravljanje incidentima, kao i izveštavanje incidenata za članove i specifične logove članova i reviziju podataka.

Vidljivost može biti posebno kritična po istinitost. Sarbane-Oksley-akta, Zakon zdravstvenog osiguranja o prenosivosti i odgovornosti (HIPAA), Evropski zakoni o privatnosti i mnogi drugi propisi zahtevaju sveobuhvatne revizije mogućnosti. Pošto su javni CC-i po definiciji „crna kutija“ za pretplatnika, potencijalnom cloud pretplatniku neće biti u stanju da pokaže istinitost (privatni ili hibridni cloud, sa druge strane, može biti konfigurisan da ispuni te zahteve).

Većina organizacija navodi zaštitu podataka, kao njihov najvažniji sigurnosni problem. Tipični koncepti obuhvataju način na koji se podaci skladište i na koji im se pristupa, pridržavanje i reviziju zahteva, i poslovnih problema koji uključuju troškove povrede podataka, obaveštenje o zahtevima i oštećenja vrednosti brenda. Svi osetljivi ili regulisani podaci treba da budu pravilno odvojeni na cloud strukturi skladištenja, uključujući i arhivirane podatke.

Kriptovanje i upravljanje ključevima za šifrovanje podataka u prenosu do CC-a ili ostatka servisa u provajderskom centru za podatke su od ključne važnosti za zaštitu podataka i saglasnosti u skladu sa mandatima. Enkripcija mobilnih medija i mogućnost da bezbedno dele ključeve za enkripciju između cloud provajdera servisa i potrošača je veoma važna i često predviđena potreba. Budući da kretanje velike količine podataka brzo i jeftino preko interneta još uvek nije praktično moguće u mnogim situacijama, u mnogim organizacijama moraju da pošalju mobilne medije do cloud provajdera. Veoma je važno da podaci budu šifrovani i da samo cloud provajder i klijent imaju pristup šifrovanim ključevima.

2.4.4. Uticaj virtualizacije na bezbednost *Cloud Computinga*

Pojava virtualizacije serverske i klijentske strane na globalnom tržištu unela je velike promene u arhitekturi sistema i dovela do značajne uštede materijalnih sredstava za nabavku hardvera, softvera i infrastrukture. Virtualizacija je klijentske i serverske hardverske resurse zamenila fajlovima i folderima koji opisuju virtuelne mašine (VM) sa virtuelnim hardverom i funkcionalnostima. Virtualizovani sistemi distribuiranog Internet računarstva – CC prodaju firmama softver, hardver i mrežnu infrastrukturu kao servise. Za kompanije je atraktivna adaptivnost (fleksibilnost) virtuelnog okruženja CC sistema, jer omogućava jednostavno i brzo prilagođavanje dizajna i arhitekture sistema specifičnim potrebama određene kompanije.

Bezbednost informacija u virtualnom okruženju postaje kritičan faktor za praktičnu primenu brojnih funkcionalnih prednosti CC sistema. Dopuna istraživanja sugerise novu paradigmu zaštite u CC sa: primenom tradicionalnih servisa zaštite; ugradnjom umesto naknadnom instalacijom mehanizama zaštite u sistemski hardver i softver; praćenjem toka osetljivih informacija u virtuelnom okruženju kroz intranet, ektranet i privatne virtualne mreže; primenom distribuiranih i inovativnih mehanizama zaštite i deljenjem odgovornosti za zaštitu između vendora i klijenta CC servisa, potpisivanjem detaljnog sporazuma o nivou usluga – SLA. Izbor politike zaštite CC sistema, najviše zavisi od SLA. Dokazana je i korisna primena virtualne mašine za ispitivanje prisustva malicioznih programa u ispitivanoj mašini [4].

Cloud provajderi mogu podržati i SaaS i IAAS unutar i između cloud-a. Provajder treba da se pridržava najbolje praktične implementacije i klijentima obezbedi maksimalnu

vidljivost u sigurnost i poštovanje položaja cloud servisa. Sposobnost da prati i odgovori na pretnje od strane privilegovanih IT administratora zauzima veliki značaj u javnom cloud modelu, gde nezavisni administratori imaju pristup podacima iz različitih organizacija.

Sigurni virtuelni trajni sloj (*Secure Virtualized Runtime layer*) na dnu je virtuelnih sistema koji pokreću procese koji pružaju uvid u podatke o skladištima podataka. Ovaj *run-time* sistem se razlikuje od klasičnog *run-time* sistema koji radi na virtuelnoj mašini slike pre nego na pojedinačnim aplikacijama. On pruža bezbednosne usluge kao što su antivirusni programi, introspekcija i spoljni sigurnosni servisi oko virtualne slike.

2.4.5. iStor Secure Data Vault

Zašto je potreban *back-up*? Najbolji način zaštite od gubitka podataka je redovno pravljenje *back-upa*. *Back-up* podataka predstavlja pravljenje kopije fajlova, sadržaja hard diska ili dela sadržaja hard diska, na nekim medijima sa kojih se podaci mogu ponovo restaurirati odnosno povratiti. Pre samog *back-upa* potrebno je izvršiti određene radnje, kao pripremu za *back-up*. Treba prvo izvršiti izbor medija na kome će se vršiti *back-up* (npr. DVD, hard disk i sl.). Treba izabrati softver iz kojeg će se vršiti *back-up* i odrediti dinamiku pravljenja *back-upa*. Takođe, pre pravljenja samog *back-upa* treba podatke proveriti odnosno skenirati na viruse. Nakon izvršenog *back-upa* poželjno je proveriti ispravnosti *back-up* podataka.

U današnjem informacijama pokretanom društvu, troškovi održavanja, dostupnosti i povraćaja podataka mogu biti poražavajući. Istražena šteta usled gubitaka podataka administracije Evropske unije u 2011 godini je više od 23 milijarde eura. Statistika vezana za gubitak podataka daje nem sledeće poražavajuće vrednosti:

- 7 od 10 malih preduzeća koje dožive veliki gubitak podataka propadnu u roku od jedne godine (DTI/PriceWaterhouse Coopers)
- 15% svih notebook računara biva ukraden ili im otkáže hard disk (Gartner Group)
- 96% poslovnih radnih stanica se ne bekapuju (*Contingency Planning & Strategic Research Corp.*)
- U 2009 godini je prijavljeno više od 90.000 računarskih krađa u EU. To daje broj od preko 245 računara svakog dana – 10 na sat.
- Svakih 8 sekundi nekom otkáže hard disk
- 50% velikih kompanija koje izgube više od polovine podataka o poslovanju bankrotira u roku jedne godine, dok 90% preostalih bankrotira u roku od dve godine.

Ove glavne pretnje našim podacima su nepredvidljive, i u većini slučajeva nekontrolisane. Stoga uobičajene lokalne mere zaštite koje se mogu primeniti ne mogu u potpunosti da spreče gubitak podataka. Ne postoji način da se obezbedi adekvatna zaštita naših podataka ako se oni čuvaju samo na jednom mestu.

iStor DataVault je sistem za sigurno čuvanje kritičnih podataka na udaljenoj lokaciji. Podaci sa servera su enkriptovani i kopirani na iStor sigurne data centre koji su raspoloživi 24 časa dnevno. iStor DataVault je dizajniran za najviši nivo sigurnosti i dostupnosti. Omogućava izuzetno napredne funkcije optimizovane za sigurno bekapovanje i povraćaj podataka, u skladu sa svim zakonskim regulativama. iStor DataVault obezbeđuje sve vidove zaštite podataka, od automatskog izvršavanja i šifriranja, prenosa podataka na udaljene loakcije i brzog oporavka podataka [26].

iStor Secure DataVault (iStor SDV) omogućava jednostavno sigurnosno skladištenje podataka u realnom vremenu, lokalno i na udaljenoj lokaciji. iStor pruža pouzdano rešenje za sigurno skladištenje sa centralnim upravljanjem koje skladištenje

podataka čini jednostavnim i olakšava menadžerima i vlasnicima zaštitu najvažnije imovine njihovih preduzeća, a to su podaci.

Ključne prednosti su [45]:

- jaka enkripcija – AES, Serpent, Twofish, MARS ili kombinovanje istih obezbeđuje da niko drugi ne može čitati podatke. Podaci se šifriraju na izvoru i ostaju šifrirani u toku prenosa i na samom skladištu.
- deduplikacija podataka
- čuvanje podataka iz izdvojenih kancelarija
- centralno upravljanje
- trag rukovanja podacima
- sveobuhvatna podrška za aplikacije i baze podataka
- geografski međusobno udaljeni centri za skladištenje osiguravaju neprikosnovenu pouzdanost
- nema početnih ulaganja
- licenciranje temeljeno na iskorišćenom kapacitetu; mogućnost zaštite neograničenog broja servera, radnih stanica ili prenosivih računara
- podrška 24/7

2.4.5.1. Izuzetna efikasnost i pouzdanost

iStor SDV osmišljen je da pruži najviši nivo preciznosti i pouzdanosti. iStor SDV ima izuzetnu efikasnost sa posebno prilagođenim sigurnosnim opcijama za skladištenje i oporavak podataka, i na taj način pomaže poslovnim subjektima da usklade svoje poslovanje sa zakonskom regulativom. iStor SDV pojednostavljuje svaki vid zaštite podataka od jednostavnog uvođenja i automatizovanog skladištenja do neposrednog čuvanja na izdvojenoj lokaciji kao i izuzetno brzog vraćanja izgubljenih podataka.



Slika 2.23. Izgled software-a iStor [45]

2.4.5.2. Napredna obrada

iStor SDV nudi široki opseg naprednih mogućnosti. Izuzetno efikasno sažimanje i globalna deduplikacija podataka značajno smanjuje vreme skladištenja, potrošnju kapaciteta skladišta, kao i opterećenje mrežne infrastrukture. Deduplikacija podataka uklanja duple podatke na nivou čitave organizacije, uključujući i izdvojene kancelarije i mobilne korisnike. *Data Integrity Verification* (provera integriteta podataka) sa automatskim oporavkom neprestano osigurava ispravnost podataka. Mogućnost

AdvancedRecovery (napredni oporavak) pruža direktan pristup bez potrebe za manuelnim spašavanjem podataka.

2.4.5.3. Pojačana sigurnost

Pre nego što se bilo koji podatak prenese, šifruje se najsigurnijim metodama enkripcije. Podaci ostaju šifrovani za vreme skladištenja i tokom svih prenosa. Klijent jedini poseduje ključ za dešifrovanje, a svi procesi čuvanja i oporavka podataka se beleže, omogućava jasan prikaz rada sa podacima. Višeslojna provera autentičnosti ugrađena u sistem *RestoreLock* zadovoljiće ključne zahteve za proverom identiteta čak i najzahtevnijih klijenata. Sa iStor SDV-om jednostavno je poštovati propise kojima se uređuje digitalno skladištenje i pristup poverljivim podacima.

2.4.5.4. Brza offsite zaštita

Podaci se sažimaju, šifruju i odmah prenose na međusobno geografski udaljene sigurnosne data centre ili na korisnikovu izdvojenu lokaciju, odnosno lokaciju za oporavak od katastrofe (DR = *Disaster Recovery*). Za prenos na sigurnu lokaciju nije potrebna manuelna intervencija, čime se obezbeđuje zaštita svih podataka klijenta i omogućava vraćanje izgubljenih podataka na postojeću lokaciju ili na lokaciju za oporavak katastrofe.

Centralna *back-up* lokacija za Evropu nalazi se u Švajcarskoj, dok se replikacija vrši na data centre u Australiji i Indoneziji u svim pravcima i u realnom vremenu.

2.4.5.5. Centralno upravljanje

Nema potrebe za lokalnim osobljem za održavanje koje će raditi sigurnosno skladištenje na izdvojene lokacije. iStor SDV omogućava da se čitavim postupkom sigurnosnog skladištenja, oporavka, odnosno arhiviranja upravlja sa jednog mesta. Uz pojedinačna pravila mogu se zadati i globalna na nivou preduzeća koje organizuje upravljanje sigurnosnim skladištenjem. Svi podaci se mogu vratiti sa bilo kog arhiviranja na lokaciju gde su potrebni, bilo gde unutar kompanije.

2.4.5.6. Trag rukovanja podacima

Trag rukovanja podacima omogućava sveobuhvatno praćenje svih aktivnosti i operacija za interno ili zakonski propisano praćenje. Prikupljene informacije se arhiviraju u nepromenjenom obliku, a pristup imaju samo ovlašćena lica.

Event list		
Time	Type	Description
☐ 5/30/2010 5:26:00 PM	LOGON	Account administrator has logged on to system.
☐ 5/30/2010 5:23:23 PM	JOB UPDATE	Enhanced delta processing settings for job [ubuntu\UBUNTU TEST] were modified by Account administrator.
☐ 5/30/2010 5:23:14 PM	JOB UPDATE	Folder selection filter for job [ubuntu\UBUNTU TEST] was modified by Account administrator.
☐ 5/30/2010 5:22:29 PM	JOB UPDATE	File selection filter for job [ubuntu\UBUNTU TEST] was modified by Account administrator.
☐ 5/30/2010 5:22:00 PM	JOB UPDATE	General settings for job [ubuntu\UBUNTU TEST] were modified by Account administrator.
☐ 5/30/2010 5:22:00 PM	JOB UPDATE	New job for computer ubuntu was added by Account administrator.
☐ 5/30/2010 5:21:23 PM	LOGON	Account administrator has logged out from system.
☐ 5/30/2010 5:21:06 PM	LOGON	Account administrator has logged on to system.
☐ 5/30/2010 5:20:39 PM	COMPUTER UPDATE	Computer ubuntu was added by Account administrator.
☐ 5/30/2010 5:20:17 PM	LOGON	Account administrator has logged on to system.
☐ 5/30/2010 5:10:13 PM	LOGON	Account administrator has logged out from system.
☐ 5/30/2010 5:07:21 PM	LOGON	Account administrator has logged on to system.
☐ 5/30/2010 5:06:26 PM	LOGON	Account administrator has logged out from system.
☐ 5/30/2010 5:06:05 PM	LOGON	Account administrator has logged on to system.

Slika 2.24. Trag rukovanja podacima [45]

2.4.5.7. Sigurno uklanjanje podataka

Kada podaci dođu do kraja svog upotrebnog ciklusa, uklanjaju se na bezbedan način koji osigurava da neovlašćene osobe neće imati prava pristupa. Metoda brisanja koja je 100% sigurna je veoma bitan aspekt za svakog menadžera, a takođe je i moralna obaveza prema svim klijentima i partnerima.

Radi zadovoljenja internih i zakonskih regulativa, podaci mogu biti uništavani na kraju svog životnog ciklusa korišćenjem jednog ili više sigurnosnih standarda kao što su:

- Air Force System Security Instructions 5020
- Bruce Schneier`s algorithmBSI (German overwrite standard by Federal Office for Information Security/ Bundesamt für Sicherheit in der Informationstechnik)
- German Standard VSITRHMG Infosec Standard No:5 (baseline) [Note! Certified version: 4.8 HMG and 3.7r1]
- HMG Infosec Standard No:5 (enhanced) [Note! Certified version: 4.8 HMG and 3.7r1]
- Navy Staff Office Publication (NAVSO P-5239-26) for RLLNSA (Overwrite standard by National Security Agency)
- OPNAVINST 5239.1A Peter Gutmann`s algorithm
- The National Computer Security Centre (NCSC-TG-025)
- U.S. Department of Defense Sanitizing (DOD 5220.22-M, DOD 5220.22-M ECE)
- US Army AR380-19NIST 800-88/ATA secure eraseExtended NIST 800-88

2.4.5.8. Isplativa zaštita podataka

Troškovi održavanja, hardvera i softvera, medija i potrošnja električne energije nisu zanemarljivi u procesu skladištenja i čuvanja podataka. iStor SDV je sveobuhvatan sistem koji radi unutar postojeće infrastrukture – nema dodatnih troškova za nabavku i održavanje hardvera i softvera. Plaća se samo korišćenje usluge čime se eliminišu svi ostali troškovi.

2.4.5.9. Ekološki odobren proizvod

U iStor-u se konstantno rađaju nove ideje i programi sa ciljem snižavanja potrošnje električne energije, a takođe i za smanjenje količine elektronskog otpada. Svest o uticaju IT industrije na okolinu bi trebao biti strateški imperativ za svaku organizaciju. Korišćenjem iStor proizvoda i usluga, ne samo da se koristi najnaprednija tehnologija i usluga, već se radi i na očuvanju naše planete.

2.4.5.10. Podrška 24 sata dnevno, 7 dana u nedelji

Ovi sistemi se pažljivo nadgledaju, a tim za podršku je dostupan klijentima 24 sata dnevno, 365 dana u godini, bilo gde i bilo kada.

2.4.5.11. Dostupan na više načina

iStor SDV je dostupan kao usluga i održavanje (*Managed Service*), softver kao usluga (*SaaS = Software as a Service*) ili kao softver.

Navešćemo samo neke od korisnika koji koriste iStor DataVault:

- pojedinci,
- mala preduzeća,

- velike međunarodne korporacije,
- finansijske organizacije,
- avio prevoznici,
- zdravstvene organizacije,
- obrazovne i istraživačke insitucije,
- kontrole leta,
- sigurnosne službe,
- automobilska industrija,
- aukcijske kuće,
- turizam,
- sport,
- telekomunikacije i drugi.

2.5. POSLOVNO – INFORMACIONI SISTEM *Hubi-e*

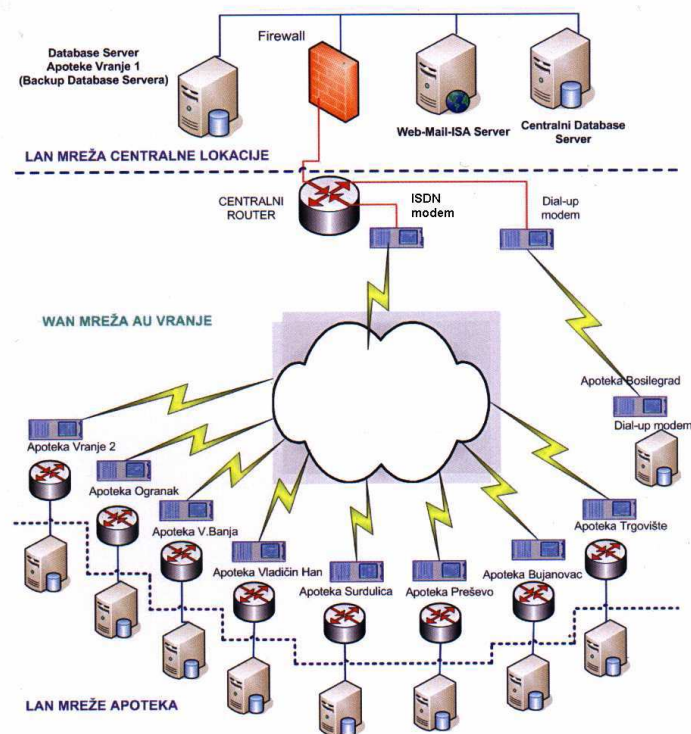
ZU Apoteka Vranje ima savremen poslovno-informacioni sistem *Hubi-e ERP*. *Hubi-e ERP* je visoko integrisan poslovno-informacioni sistem (PIS) koji povezuje praktično sve poslovne oblasti, aktivnosti i procese u savremenoj kompaniji. Namenjen je velikim i srednjim kompanijama, i primenjuje se u oblastima farmacije, trgovine, usluga, proizvodnje itd.

Hubi-e ERP odgovara svim zahtevima i očekivanjima jer je prilagodljiv, modularan, integralan, sveobuhvatan, jednostavan za korišćenje, baziran na domaćim i ino-iskustvima, što je razlog zbog čega *Hubi-e ERP* sve češće postaje stub na koji se oslanja sve više kompanija u Srbiji (Apoteka Beograd, ZU Apoteka Vranje, Veropulos, Lasta, Idea, Pepsi, itd).

2.5.1. Tehničko – poslovne karakteristike *Hubi-e ERP*

Poslovno-informacioni sistem *Hubi-e ERP* je softver koji služi za praćenje i upravljanjem poslovanjem – resursima kompanije. Namenjen je velikim i srednjim kompanija što je upravo slučaj kod ZU Apoteka Vranje. *Hubi-e ERP* ima mogućnost praćenja i upravljanja svim poslovnim procesima i evidentira sve robno novčane transakcije. Koristi najnovije tehnologije, modularan je i ima stalno obezbeđenu podršku i održavanje.

Na slici br. 2.25. dat je prikaz povezivanja servera u mreži ZU Apoteka Vranje.



Slika 2.25. Povezivanje računarskih resursa između apoteka i centralne lokacije u Upravi Apoteke Vranje [28]

S obzirom da se na slici vidi razuđenost apoteka koje se nalaze u sastavu ZU Apoteka Vranje jasno je sa kolikom pažnjom moramo da uradimo celokupan projekat zaštite IKT sistema. Ovde imamo kombinaciju sistema zaštite pod operativnim sistemom Windows XP i sistema zaštite u samom *Hubi-u*.

2.6. NIST WINDOWS XP SIGURNOSNA PODEŠAVANJA NA RAČUNARIMA ZU APOTEKA VRANJE

2.6.1. Account Policies

Ovde je važno podesiti parametre lozinke tako da su lozinke dovoljno jake. To smanjuje verovatnoću napadača da pogodi ili provali lozinku za neovlašćen pristup sistemu.

2.6.2. Local Policies

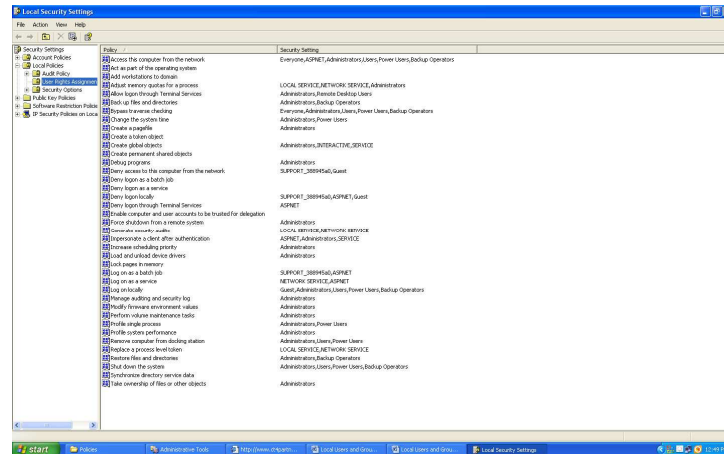
Ova kategorija obuhvata tri podkategorije :

- *System auditing policy* (politika kontrole sistema) koja sadrži evidenciju određenih vrsta logovanja, tako da ih sistem administrator može pregledati i otkriti neovlašćene aktivnosti,
- *User rights assignment* (pripisivanje korisničkih prava) gde NIST bezbednosni šabloni opisuju koje grupe imaju određena korisnička prava. Cilj je da svaka

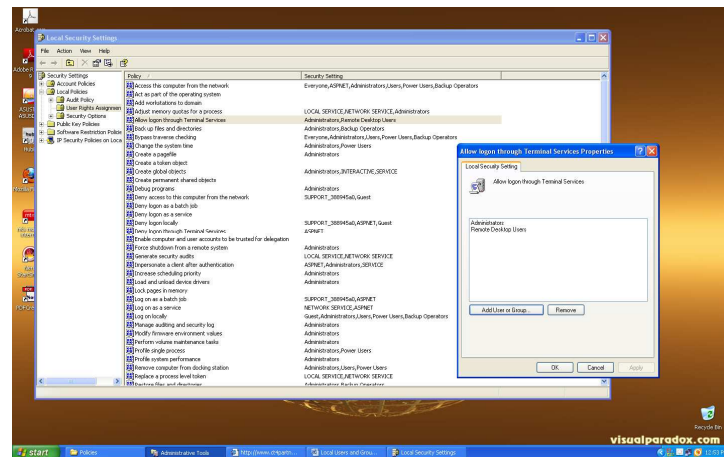
grupa ima samo neophodna prava, koja su im potrebna za obavljanje funkcionalnih zadataka i samo za korisnike koji pripadaju neophodnim grupama.

- *Security options* (bezbednosne opcije) mogu se menjati da bi se postigla veća sigurnost nego što nude unapred definisana podešavanja.

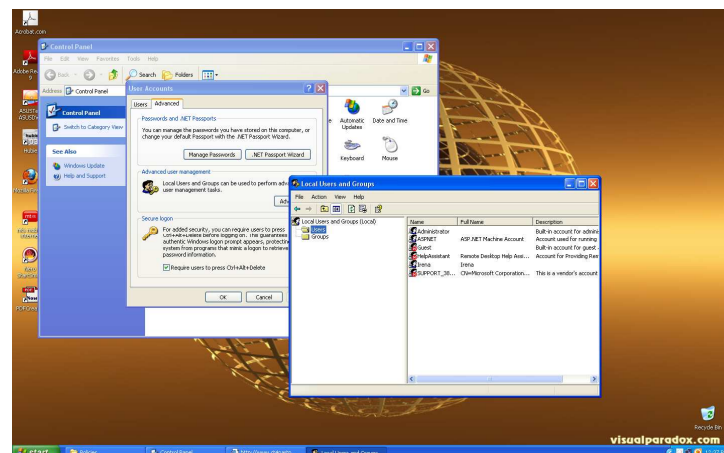
Na sledećim slikama imamo prikaz podešavanja korisničkih naloga u ZU Apoteka Vranje:



Slika 2.26. Local Security Settings



Slika 2.27. Local Security Settings



Slika 2.28. Prikaz korisnika na sistemu

2.6.3. Event Log Policies

Windows XP evidentira informacije o značajnim događajima za tri logovanja: *Application Log*, *Security Log* i *System Log*. Logovanja sadrže poruke grešaka, pregled bezbednosno relativnih informacija i ostale evidencije aktivnosti na sistemu. Logovanja se mogu koristiti ne samo za prepoznavanje sumnjivih i malicioznih dešavanja i istragu bezbednosnih incidenata već i za probleme sa aplikacijama. Prema tome važno je omogućiti sva tri logovanja.

2.6.4. Restricted Groups

NIST preporučuje da se svi korisnici uklone sa *Remote Desktop* grupe korisnika, na svim sistemima i u svim okruženjima, osim korisnika koji posebno imaju potrebu da pripadaju toj grupi. Ovo će smanjiti mogućnost da neko neovlašćeno pristupi sistemu kroz *Remote Desktop*. NIST takođe preporučuje ograničeni broj članova u *Power* grupi, jer je po privilegijama blizu grupi administratora. Unapred definisani NIST sigurnosni šablon uklanja sve korisnike sa *Remote Desktop Users* i *Power Users groups*.

2.6.5. System Services

Windows XP radi sa mnogo servisa koji se pokreću automatski prilikom startovanja sistema. Ovi servisi upotrebljavaju resurse i mogu predstavljati ranjivost hosta. Sve nepotrebne servise trebalo bi onemogućiti da bi se smanjio broj napada na sistem. U upravljačkim okruženjima treba koristiti *Group Policy Object*, da bi se podesili servisi na sistemu; u drugim okruženjima servisi se mogu ugasiti pojedinačno. Za obe metode podešavanja svaki servis na sistemu se može podesiti sa jednim od tri načina:

- Automatski – servis se pokreće automatski,
- Ručno – servis se pokreće samo onda kada je potreban sistemu i
- Onemogućen – servis se ne može pokrenuti od strane sistema.

2.6.6. Dozvole za pristup podacima

Dozvole za pristup podacima obezbeđuje opšte instrukcije u pogledu podešavanja dozvola kontrole pristupa kroz ACE (*Access Control Entries*) i ACL (*Access Control List*). NIST bezbednosni šablon ograničava pristup preko 25 izvršnih datoteka, štiteći ih od neautorizovane upotrebe i izmena. Dopunska podešavanja mogu se izvršiti na tri načina:

1. Otvoriti prozor **Properties** i kliknuti na zalistak **Security**. Imamo prikaz privilegija svih korisnika i grupa za taj resurs. Dugme **Advanced** se može koristiti za podešavanje prava pristupa i dodatna podešavanja kao što su *pregled datoteka i vlasnik resursa*.
2. Koristiti **cacls.exe** koji se nalazi **%SystemRoot%\system32**. Ovo je komandna linija interfejsa koja se koristi za podešavanje ACLs, ali ovo ne podešava Windows XP sigurnosni deskriptor.
3. Ubaciti **MMC Security Template** u namenska podešavanja iz šablona.

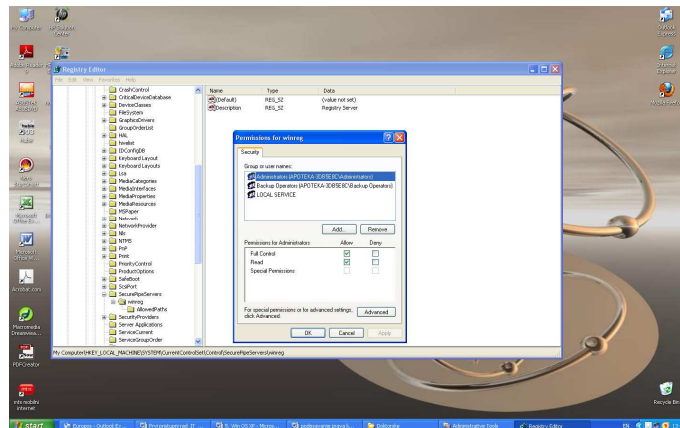
2.6.7. Dozvole za pristup registrima

Windows XP takođe ima dozvolu nad registrima. NIST podešavanja podešavaju ograničene dozvole za nekoliko ključeva registara i vrednosti za njihovu zaštitu od neovlašćenog pristupa i izmene. Dozvola za manipulaciju registrima je ograničena, prema

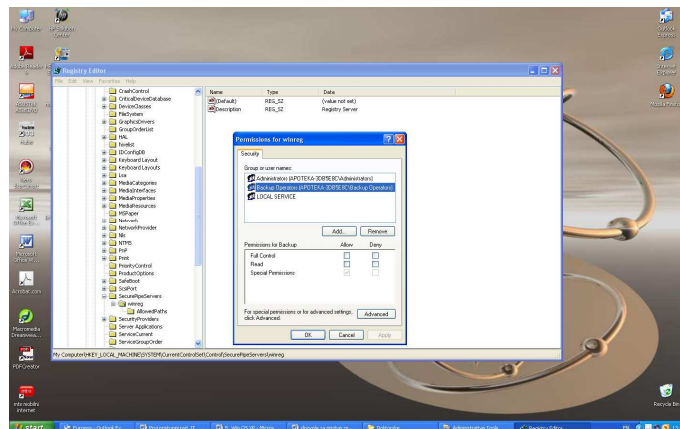
unapred definisanom podešavanju, ali zbog vrednosti registra važno je proveriti da li je registar zaštićen. Da bi to uradili trebali bi da pratimo sledeće korake:

1. Kliknuti **Start** i odabrati **Run**. Ukucati **regedit** i kliknuti **OK**.
2. Naći ključ **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg**.
3. Desnim dugmetom kliknuti na **winreg** i odabrati **Permissions**.
4. Obezbediti da samo **Administrator** ima **FullControl**, da **Backup Operators** grupa nema ovlašćenja i **LOCAL SERVICE** ima samo **Read** ovlašćenja.

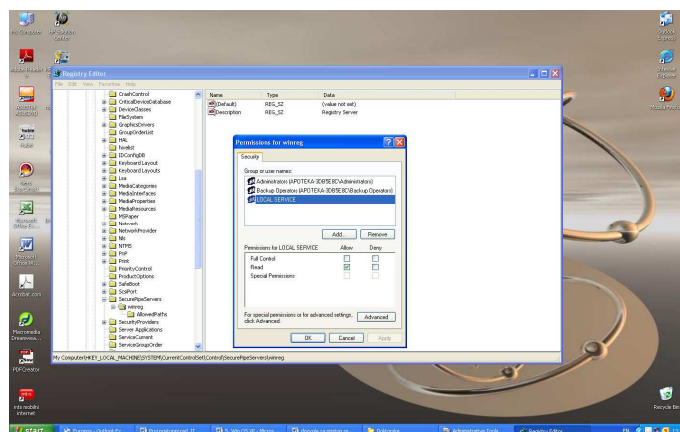
Primena se može videti na sledećim slikama:



Slika 2.29. Administratorski nalog



Slika 2.30. Backup Operators nalog



Slika 2.31. Local Service nalog

2.7. DOPUNSKA WINDOWS XP BEZBEDNOSNA KONFIGURACIJA

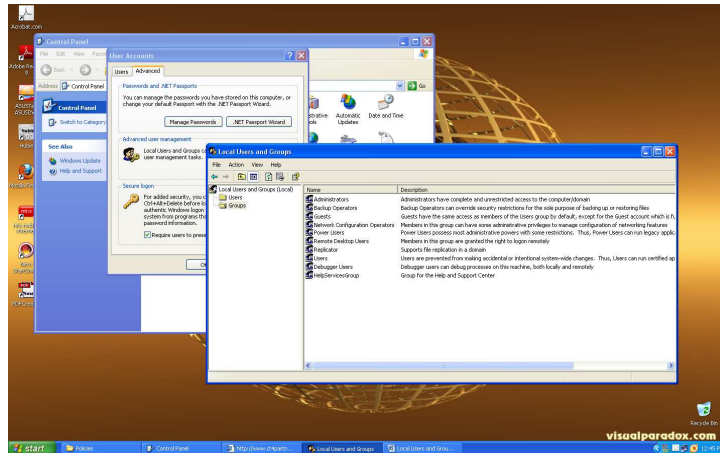
2.7.1. EFS Data Recovery

EFS proces je transparentan za krajnjeg korisnika, jer je integrisan u NTFS. Ostali korisnici sa sličnim ili manjim privilegijama ne mogu otvoriti EFS šifrovanu datoteku drugog korisnika, jer nemaju FEK. Windows XP EFS obezbeđuje integrisanu podršku za oporavak podataka.

Windows XP primorava konfiguraciju za oporavak ključeva. Ključevi za oporavak koji se nalaze u direktorijumu *Encrypted data Recovery Agents* se mogu povratiti logovanjem na sistem sa nalogom **Administrator**.

2.7.2. User Accounts and Groups

Windows XP unapred definiše instalaciju nekoliko korisničkih naloga i oni se trebaju onemogućiti ili preimenovati. Unapred definisani korisnički nalozi se često iskorišćavaju i njihovim onemogućavanjem napadačima je teže da pristupe računaru. Na sledećoj slici imamo prikaze korisničkih grupa koje su prisutne u ZU Apoteka Vranje:



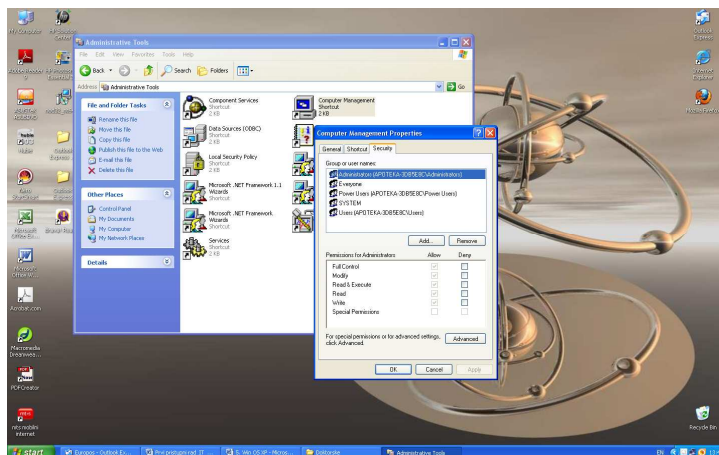
Slika 2.32. local Users and Groups

2.7.3. Reviewing Audit Logs

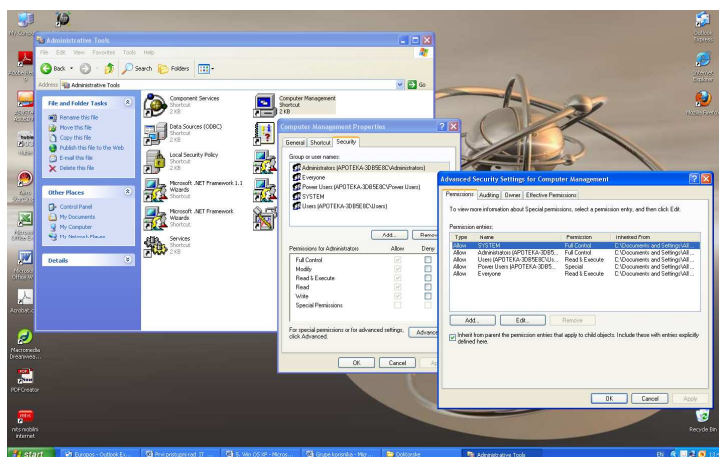
Windows XP sadrži ugrađen alat MMC zvani *Event Viewer* za pregled bezbednosti aplikacija i sistemskih logovanja. Za ručni pregled moramo izvesti sledeće korake:

1. Iz menija **Start** izaberemo **Control Panel**
2. odabrali **Administrative Tools**, a zatim **Computer management**
3. Proširujemo listu **System Tools**, a zatim proširujemo **Event Viewer**. Ovo će prikazati tri vrste logovanja: **Application**, **Security** i **System**.

Na sledećim slikama imamo prikaze korisničkih grupa sa ovlašćenjima koja su prisutna u ZU Apoteka Vranje:



Slika 2.33. Grupe korisnika



Slika 2.34. Podešavanje prava korisnika

2.7.4. Software Restriction Policy (politika restriktivnog pristupa softveru)

Sastoji se iz pet komponenti:

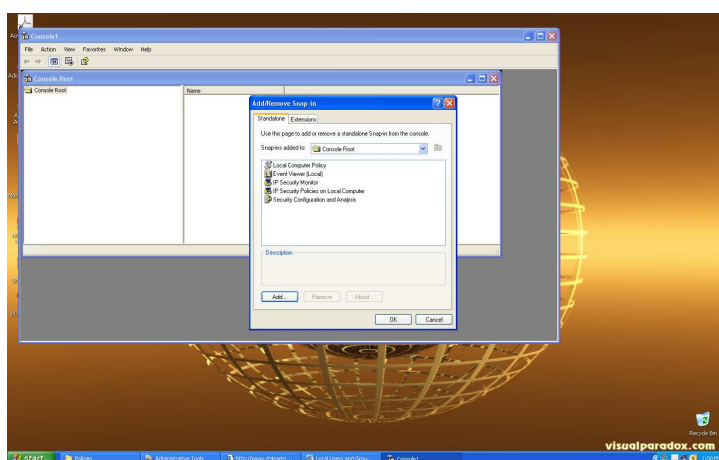
1. *Security Levels;*
2. *Additional Rules;*
3. *Enforcement;*
4. *Designated File Types;*
5. *Trusted Publishers.*

Da bi se napravile i konfigurisale politike ograničenja pristupa softverima sistema treba izvesti sledeće korake:

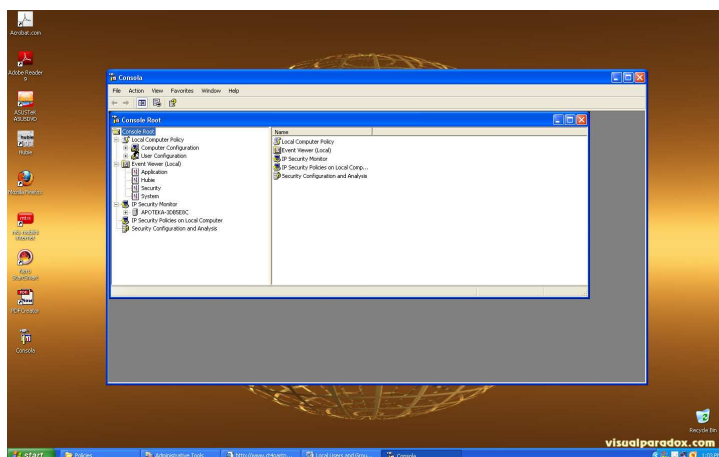
1. Logovati se kao administrator ili kao korisnik koji ima pravo da kreira politike ograničenja pristupima softvera
2. Kliknite na **Start**, a zatim odaberite **Run**. U polju **Open** ukucajte **mmc** i kliknite na **OK**
3. Pojaviće se prozor **Console**. Kliknite na **File**, zatim na **Add/Remove Snap-in**, zatim na **Add**. Odaberite **Group Policy** i kliknite na **Add**.
4. Kliknite na **Finish**.

5. Na prozoru console proširite **Local Computer Policy**, **Computer Configuration**, **Windows Setting** i **Security Setting**.
6. Iz direktorijuma **Security Settings** kliknite na **Software Restriction Policies**, a zatim na direktorijum **Security Levels**.
7. Postoje dve opcije: **Disallowed** i **Unrestricted**. Duplim klikom otvorite **Disallowed**, zatim kliknite na **Set as default**, a zatim na **OK** za nastavak.
8. Otvorite **Local Security Policy**, kliknite na **Start**, a zatim na **Control Panel**. Kliknite na **Administrative Tools**, a zatim na **Local Security Policy**. Ovo bi trebalo da otvori prozor Local Security Settings.
9. Proširite **Software restrictions Policies** i kliknite na direktorijum **Additional Rules**. Na desnoj strani treba da se prikažu unapred definisana pravila.

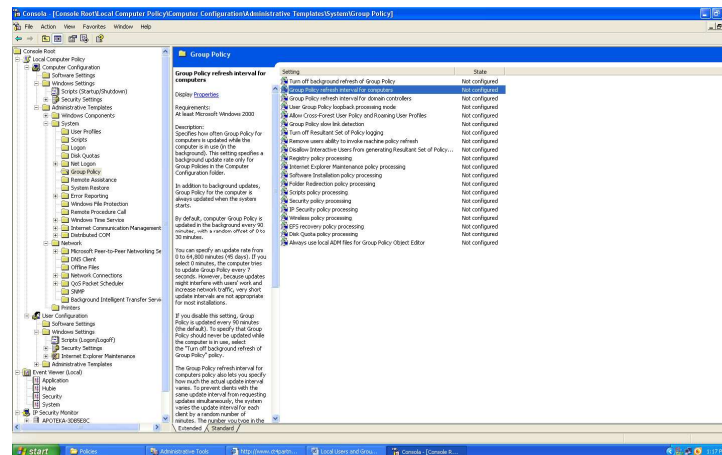
Ove konzole mogu se videti na sledećim slikama:



Slika 2.35. Console Root



Slika 2.36. Console Root 2



Slika 2.37. Console Root – Group Policy

2.8. BEZBEDNOSNA KONFIGURACIJA U Hubi-e

Što se tiče bezbednosti aplikacije i logovanja na sistem, osnovni parametri sistema *Hubi-e* sadržani su u samom *source* kodu. Od servisa za logičku kontrolu pristupa (AC) koji su:

- Obaveznu (**MAC – Mandatory Access Control**) – koja u *Hubi-u* postoji ali se ne primenjuje
- Diskrecionu (**DAC – Descretionary Access Control**)
- Na osnovu uloga (**RBAC – Role based AC**)
 - **MAC i RBAC** – kontrola na osnovu utvrđenih pravila
 - **DAC** – vlasnik sistema upravlja AC svojom odlukom

Od svih ovih servisa u *Hubi-u* se koristi isključivo kontrola na osnovu uloga – RBAC. Ovo je noviji model za kontrolu pristupa od ACL-a. Za razliku od ACL-a, pristup resursima određuje se na osnovu odnosa između podnosioca zahteva i organizacije odnosno vlasnika kontrole nad resursima. RBAC otklanja neke od nedostataka ACL-a, ali predstavlja i neke nove i zanimljive mogućnosti. To je noviji alternativniji pristup obavezne kontrole pristupa (MAC) i diskrecione kontrole pristupa (DAC). RBAC se ponekad naziva i uloga zasnovana na bezbednosti.

2.8.1. RBAC model

U okviru ZU *Apoteka Vranje*, uloge su stvorene za različite funkcije posla. Dozvole za obavljanje pojedinih poslova su dodeljene na osnovu specifičnih uloga. Radnicima uprave i drugim korisnicima sistema dodeljene su određene uloge, i kroz te uloge dobijaju se dozvole za obavljanje određenih funkcija sistema. Budući da korisnicima nisu direktno dodeljene dozvole, već ih dobijaju kroz svoje uloge, upravljanje pojedinačnim korisničkim pravima postaje stvar odgovarajuće uloge korisnika, što olakšava zajedničke operacije, kao što je dodavanje korisnika, ili promena odeljenja korisnika.

Za RBAC su definisana tri osnovna pravila:

1. Uloga (zadatak): Predmet može izvršiti transakciju samo ako je predmet izabran ili mu je dodeljena uloga

2. Uloga ovlašćenja: Subjekt aktivnim učestvovanjem mora biti nadležan za predmet. Uz pravilo 1, ovo pravilo osigurava da korisnici mogu preuzeti samo uloge za koje su ovlašćeni.
3. Autorizacija transakcija: predmet može izvršiti transakciju samo ako je nadležan za transakciju i ima aktivnu ulogu. Sa pravilima 1 i 2, ovo pravilo osigurava da korisnici mogu da izvršavaju samo transakcije za koje su ovlašćeni.

Dodatna ograničenja mogu se primeniti kao i uloge koje se kombinuju u hijerarhiji, gde uloge višeg nivoa imaju vlasništvo nad podzakonskim ulogama. Sa hijerarhijskim konceptima uloga i ograničenjima, RBAC može kontrolisati kreiranje i simulaciju pristupa rešetke zasnovanog na kontroli (LBAC). Tako se RBAC može smatrati nadskupom LBAC. Prilikom definisanja RBAC modela, koristimo sledeće korisne konvencije :

- S = subjekt = lice ili automatizovani agent
- R = uloga = poslovna funkcija ili naslov koji definiše nadležnost na nivou
- P = dozvole = odobren način pristupa resursima
- SE = sesija = mapiranje uključuje S, R i/ili P
- SA = zadatak teme
- PA = zadatak dozvole
- RH = delimično naređuje ulogu hijerarhije. RH takođe može da se napiše: $\geq$ (notacija: $x \geq y$ znači da x nasleđuje dozvole od y)
- Predmet može imati više uloga
- Uloge mogu da imaju više predmeta
- Uloga može da ima mnogo dozvola
- Jedna dozvola može biti dodeljena za više uloga

Ograničenje restriktivnih pravila o nasleđivanju potencijalnih dozvola može se koristiti za postizanje odgovarajućeg razdvajanja dužnosti. Na primer, istoj osobi ne bi trebalo biti dozvoljeno i da kreira korisnički nalog i da odobri stvaranje računa. Tako je, koristeći teoriju skupa notacija:

- $PA \subseteq P \times R$ i mnogo dozvola u vezi za zadatu ulogu
- $SA \subseteq S \times R$ i mnogi podležu vezi za zadatu ulogu
- $RH \subseteq R \times R$

Predmet može imati više istovremenih sesija sa različitim dozvolama.

2.8.2. Odnosi sa drugim modelima

RBAC je politika neutralne i fleksibilne kontrole pristupa koja je dovoljno moćna da simulira DAC i MAC. S druge strane, MAC može da simulira RBAC ako je uloga ograničena na drvo, a ne delimično na skup. Pre razvoja RBAC-a, MAC i DAC su smatrani da su jedini poznati modeli za kontrolu pristupa: ako model nije MAC, smatralo se da je DAC-model, i obrnuto. Istraživanja sprovedena u kasnim 1990-im su pokazala da RBAC ne spada ni u jednu kategoriju. Za razliku od konteksta na osnovu kontrole pristupa (CBAC), RBAC ne gleda na poruku u kontekstu (kao što je izvor veza).

RBAC se razlikuje od liste za kontrolu pristupa (ACL), koji se koristi u tradicionalnoj diskreciji sistema za kontrolu pristupa, u tome što se dodeljuju dozvole za određene

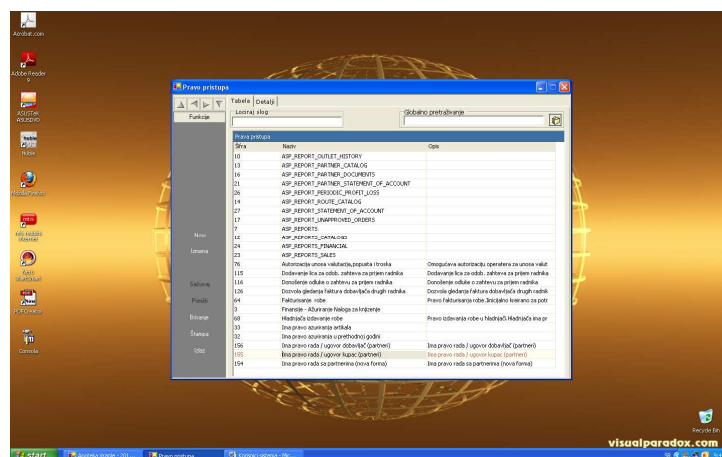
operacije sa značenjem u organizaciji, a ne nizak nivo podataka objekata. Na primer, lista kontrole pristupa bi se mogla koristiti da dozvoli ili odbije pristup pisanja na određenim fajlovima sistema, ali to neće diktirati kako će taj fajl biti primenjen. Dodeljivanje dozvola za obavljanje određenih operacija je značajno, jer su operacije značajne u okviru aplikacije. RBAC se pokazala kao posebno pogodna za razdvajanje dužnosti (SoD) i zahteva, ali je neophodno dvoje ili više ljudi koji će biti uključeni u odobravanje kritičnih operacija. Analizirani su neophodni i dovoljni uslovi za bezbednost SoD u RBAC-u. Osnovni princip SoD je da nijedan pojedinac ne može da utiče na bezbednost kroz dvostruke privilegije. Kao dodatak, niko ne može da preuzme ulogu koju vrši revizija, kao što su kontrola, koja istovremeno ima ulogu kontrole i pregleda vlasti nad drugima.

2.8.3. Korišćenje i raspolaganje

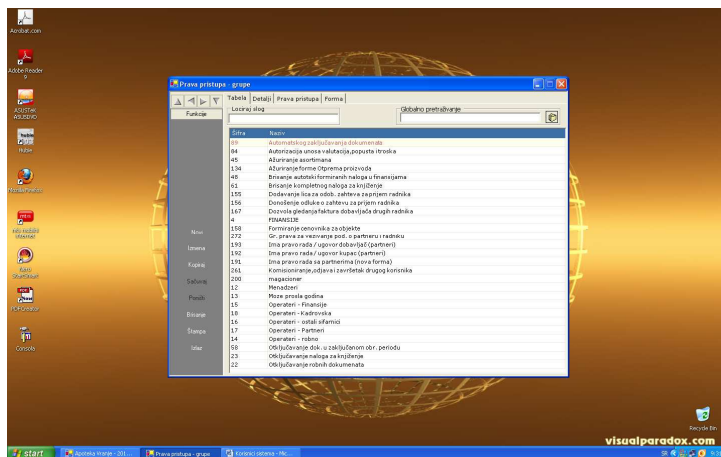
Upotreba RBAC-a za upravljanje privilegijama korisnika u okviru jedinstvenog sistema ili aplikacije je široko prihvaćena kao najbolja praksa. Sistemi tipa : Microsoft Active, Microsoft SQL Server, SELinux, grsecurity, FreeBSD, Solaris, Oracle DBMS, PostgreSQL 8.1, SAP R/3, FusionForge i mnogi drugi efikasno sprovode neki oblik RBAC-a.

U organizaciji sa heterogenom IT infrastrukturom i uslovima koji se protežu desetinama ili stotinama sistema i aplikacija, kao što je ZU Apoteka Vranje, korišćenje RBAC-a za upravljanje i dodeljivanje uloga bilo bi izuzetno kompleksno da nema hijerarhijskog stvaranja uloga i određivanja privilegija. Alternativna strategija za velike je dodeljivanje privilegija korisnicima kako se pominje u beloj knjizi : Uloga: rezervisan je praktičan pristup poslovnim korisnicima ([thhp://www.idsynch.com/docs/beyond-roles.html](http://www.idsynch.com/docs/beyond-roles.html)). Noviji sistemi produžuju stariji NIST RBAC model sa adresom ograničenja RBAC-a za preduzeća širom sistema. O tome postoji nekoliko akademskih radova. NIST model je usvojen kao standard od strane INCITS kao ANSI/INCITS 359-2004. Objavljena je i diskusija o nekim izborima dizajna za NIST-model.

Na sledećim slikama može se videti korišćenje RBAC-a prilikom formiranja grupa korisnika kao i prava pristupa.

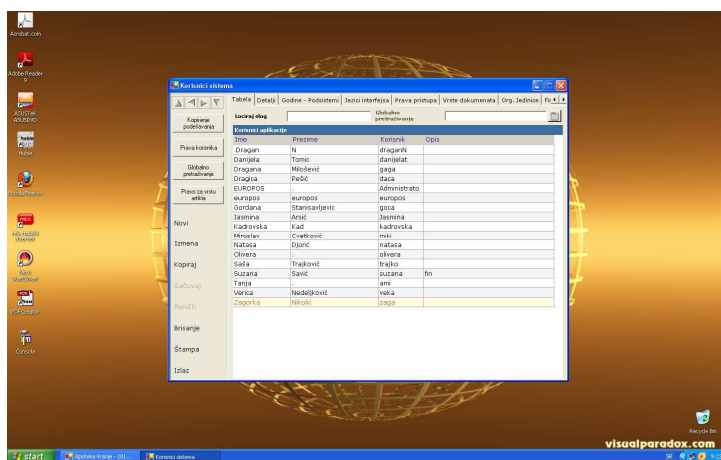


Slika 2.38. Prava pristupa u Hubie-u



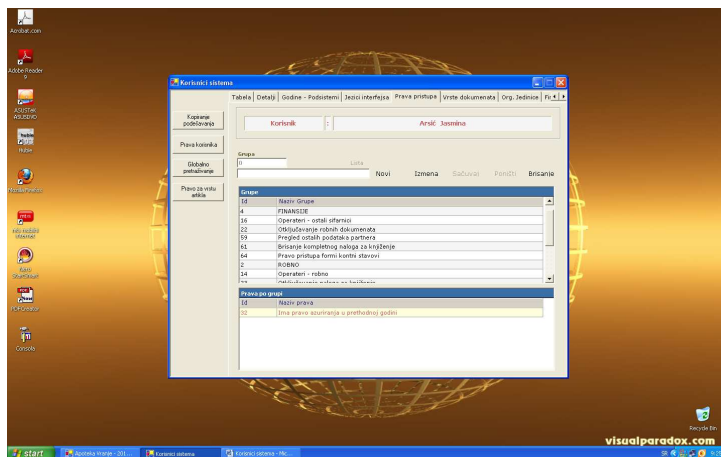
Slika 2.39. *Pravo pristupa – grupe u Hubie-u*

Na slici 2.39. vide se svi korisnici prijavljeni na sistem *Hubie* u upravi ZU Apoteka Vranje.



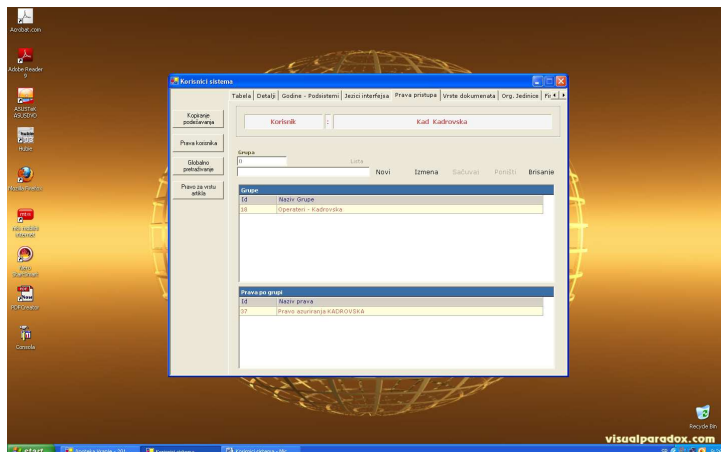
Slika 2.40. *Korisnici prijavljeni u Hubie-u*

Na slici 2.41. mogu se videti ovlašćenja koja su kompletna a odnose se na direktora ZU Apoteka Vranje.



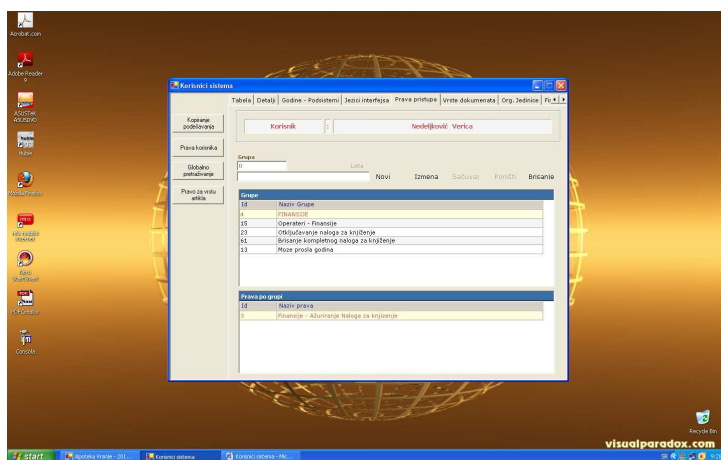
Slika 2.41. *Potpuna ovlašćenja*

Na slici 2.42. se vide ovlašćenja koja imaju pravnici u pravnoj službi:



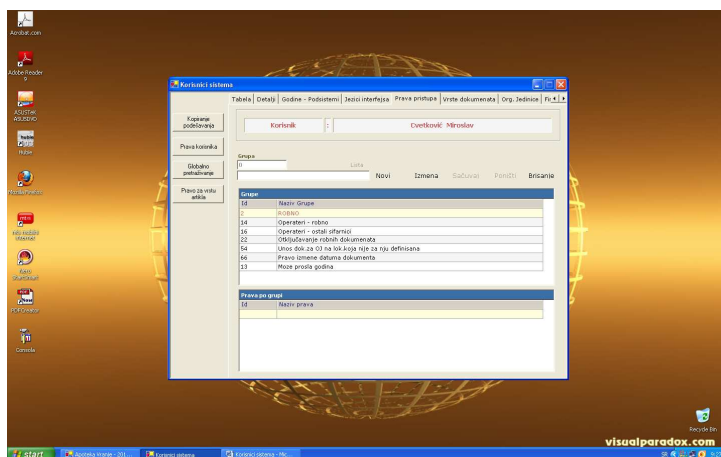
Slika 2.42. Ovlašćenja pravne službe

Na slici 2.43. imamo predstavljena ovlašćenja službenika u službi finansija:



Slika 2.43. Ovlašćenja radnika službe finansija

Na slici 2.44. se vide ovlašćenja operatera u ograncima ZU Apoteka Vranje.



Slika 2.44. Ovlašćenja operatera u ograncima

2.9. DIGITALNI CERTIFIKATI TELEKOMA SRBIJA

Usluge web hostinga Telekoma Srbija organizovane su po principu *shared* web hostinga odnosno više korisnika (više web sajtova) smeštaju se na jedan web server. HTTPS konekcija je podržana, ali sa *self-signed* sertifikatom servera.

Za zaštitu saobraćaja ka web serverima Telekom Srbija koristi IBM *Intrusion Prevention System* i Cisco sisteme zaštite (*Guard/Detector*), tehnologija sertifikata je Microsoft CA na Windows 2003 telu a koristi se i poseban bezbednosni hardver (HSM).

2.9.1. IBM sistem za sprečavanje upada

Kompanija Telekom Srbija i IBM potpisale su ugovor još 2007. godine o partnerstvu kojim će Telekom Srbija postati provajder novog bezbednosnog sistema (MSS), koga podržava IBM-ov internet bezbednosni sistem (ISS – IBM). Telekom Srbija bezbednosna platforma podržana ISS – IBM softverom i opremom, pratiće i rešavati ugroženosti mreže i brzo reagovati na potencijalne pretnje pre nego što se dese.

IBM sistem za sprečavanje upada (*Intrusion Prevention System* –IPS) mreža je dizajnirana tako da spreči pretnje na internetu koje bi ometale poslovanje presuzeća. IBM IPS služi kao bezbednosna platforma koja redukuje troškove, složenost pokretanja i upravljanja i primenu tački rešenja. Prilikom procene sprečavanja upada teži se da se uspostavi ravnoteža i optimizacija sledećih šest ključnih oblasti a to su: osiguranje, bezbednost, pouzdanost, primena, upravljanje i poverenje. IBM *securiti* mreža IPS ispunjava svih šest tačaka, i vodeća je u preventivnoj zaštiti od pretnji, ima visok nivo dostupnosti, pojednostavljenu primenu i upravljanje kao i uverenje da dolazi kao podrška od strane jedne od vodećih firmi svetske klase, IBM-a. Organizacije koje žele da prenesu teret zaštite mogu da se oslone na bezbednog partnera.

Namenski IBM sigurnosna mreža IPS nudi visoku propusnu moć niskom latencijom i maksimalnom dostupnošću za održavanje efikasne mrežne operacije. Ovo uključuje sposobnost da koristi pun spektar zaštite i bezbednosti eliminišući potrebu da bira između najviših nivoa bezbednosti i performansi koje su zahtevale da se održi nivo za kritičnu poslovnu aplikaciju.

Ovaj modul uključuje IBM *Security* mreže IPS koje štite organizacije (korisnike) od širokog spektra pretnji između kojih su:

- *Malware* uključujući „crve“ i „špijune“,
- Napadi na botnet,
- Instant poruke i povezane *peer-to-peer* rizike kao što je gubitak podataka,
- *Denial of Service* (DOS) i distribuirani *Denial of Service* (DDoS)
- Ciljani napadi na web aplikacije, kao što su *cross-site scriping* i *SQL injection*
- Gubitak osetljivih podataka,
- Buffer napad,
- Napad od strane klijenata na ciljane web pretraživače.

Mrežni i bezbednosni administratori mogu lako da izaberu neki od tri režima rada uključujući:

- Aktivnu zaštitu (*Intrusion Prevention* režim),
- Pasivno otkrivanje (režim za detekciju upada) i
- Inline simulaciju (simulira inline prevenciju).

IBM IPS proizvodi su dizajnirani da blokiraju napade u data centrima uključujući:

- Servere,
- Mrežna infrastrukturna oprema kao što su ruteri i prekidači,
- Voice over IP aplikacija i oprema,
- Privatne telefonske centrale (PBKS),
- Nadzor kontrola i podataka,
- *Ackquisition* (SCADA) sistemi.

Po obezbeđenju data centra, IBM IPS pomaže smanjenju vremena zastoja sistema i aplikacije isključenjima koja su rezultat Internet napada. IBM IPS uklanja štetne pakete iz važećih aplikacija i pomaže u održavanju kontinuiteta podataka.

Da bi sprečili gubitak osetljivih podataka IBM IPS može da radi u inline ili pasivnom režimu i da vrši kontrolu saobraćaja u oba smera. U pasivnom režimu, mrežni IPS može generisati upozorenje u *Management Console*, vrati TCP korisniku sistema ili oboje. U inline režimu preporučuje se na segmentima gde poverljive informacije treba da budu šifrovane u svakom trenutku, IBM IPS može da blokira prenos podataka.

Počevši sa *firmware* 4.1 na IBM bezbednosti mreže *Intrusion Prevention* aparati, primenjuju bezbednosnu politiku mnogo lakšu za korišćenje. Različite vrste osetljivih informacija zahtevaju rešenje koje je fleksibilnije i prilagodljivije. IBM IPS može generisati upozorenje, blokirati saobraćaj ili oboje. Ova fleksibilnost omogućava administratorima niz kriterijuma pretrage i otkrivanja mogućnosti da odgovaraju različitim situacijama ili da podrže zahteve revizije.

Osnova za jedinstveni oblik bezbednosti leži u IBM PAM (*Protocol Analiza Modul*). Sa svojim modularnim nadogradivim okvirom, PAM se konstantno razvija kako bi blokirao najveće izazove i pretnje bezbednosti. PAM pruža zaštitu mreže koja prevazilazi tradicionalni IPS i sada sa klijentske strane uključuje zaštitu aplikacije, bezbednosti podataka, zaštitu i kontrolu aplikacija.

Protection moduli unutar PAM-a uključuju:

- IBM virtuelna *patch* tehnologija – zaštita ranjivosti od eksploatacije
- Klijent-strana zaštita aplikacije – štiti krajnje korisnike protiv napada koji ciljaju aplikacije koje se koriste svakodnevno kao što su: Microsoft Office datoteke, Adobe PDF fajlove, multimedijalne fajlove i web browsere,
- Napredna mrežna zaštita – monitoring i identifikacija kriptovanih informacija za ličnu identifikaciju (PII) i drugi poverljivi podaci,
- Bezbednost web aplikacija
- *Application Control – Reclaim* propusni opseg i blok *Skipe*, *pepr-to-peer* mreže i tunelovanje

PAM radi preventivno kako bi zaustavio više tipova napada. PAM omogućava IBM IPS na obezbedi zaštitu na *Session Initiation Protocol* (SIP9, X.323 protokol, protokol teksta (GTP) i više od 140 drugih.

2.9.2. Sistem za detekciju i sprečavanje upada

2.9.2.1. Ciljevi IDPS

Osnovna svrha jednog sistema za detekciju i sprečavanje upada (*Intrusion Detection and Prevention Systems* -IDPS je otkrivanje mogućih incidenata. Mnogi IDPSs mogu da budu podešeni tako da prepoznaju povredu bezbednosti organizacije i prihvatljivo korišćenje politike, na primer transfera neodgovarajućeg materijala u mreži kompanije ili preuzimanje velikih baza podataka na notebook računarima. Neki IDPS su takođe u stanju

da identifikuju izviđačke aktivnosti, što može da ukazuju da je napad neizbežan. Na primer, neki oblici zlonamernih programa mogu obavljati skeniranje portova i tako identifikovati moguće mete za napad. IDPS može da blokira ove izviđačke aktivnost i da obavesti administratore bezbednosti, koji onda mogu omogućiti druge bezbednosne kontrole i zaustaviti napad.

Pored identifikovanja bezbednosnih incidenata, IDPS tehnologija može poslužiti nizu drugih razloga:

- Identifikovanje problema bezbednosne politike. IDPS može biti konfigurisan sa nizom *firewall* pravila i vrši proveru saobraćaja, obaveštava administratore kada je detektovan saobraćaj, koje bi trebao biti blokiran od strane *firewall*, ali nije bio, verovatno zbog pogrešne konfiguracije.
- Dokumentovanje postojećih pretnji organizacije. Detekcija upada omogućava prikupljanje informacija koje su korisne u razumevanju tehnike upada i frekvencija i karakteristika pretnji kojima je izložena organizacija kao i preduzimanje mera bezbednosti u skladu sa tim.
- Odvrćanje pojedinaca od povrede bezbednosne politike. Svesni da se njihova delatnost prati, pojedinci mogu biti manje skloni da krše politiku te organizacije u strahu od otkrivanja.

2.9.2.2. Klasifikacija IDPS

IDPS tehnologije mogu se klasifikovati prema različitim parametrima, odnosno:

- Metodologija koja se koristi za detekciju upada: potpis na bazi detekcije, anomalija na bazi detekcije i *Stateful* protokol analiza.
- Funkcionalnosti koje one nude, na kraju razlikuju pasivne sisteme (IDSs) od reaktivnih sistema (IPSs).
- Tipovi događaja koji nadgledaju, usko su vezani za vrstu sistema koji čuvaju: žičnu mrežu, bežičnu mrežu ili jedan host. Pored ovih, četvrti tip IDPS koji je identifikovan poznat je kao analiza mrežnog ponašanja (NBA) IDPS.

2.9.2.3. Uobičajene metode za detekciju

Osnovne klase metodologija za detekciju su:

- **Potpis na bazi detekcije.** Potpis je model koji karakteriše poznatu opasnost. Primeri potpisa uključuju sledeće: telnet pokušaj sa korisničkim imenom korena, što predstavlja povredu bezbednosne politike organizacije; niz TCP SYN paketa koji se šalju na mnogim različitim portovima velikom brzinom sukcesije, što može ukazivati na to da se vrši skeniranje porta; poznata je e-pošte sa temom „*ringtones*“, koja je karakteristika poznatih oblika zlonamernih programa.
- **Anomalija na bazi detekcije.** Temelji ove tehnike za detekciju su u odnosu na događaje posmatrane na mreži ili hostu sa onim što se smatra normalnim aktivnostima za njih, kako bi se identifikovala značajna odstupanja. Moguća su dva pristupa : prag detekcije i detekcija profila.
- ***Stateful* protokol analiza.** *Stateful* protokol analiza je donekle sličan anomaliji na bazi detekcije. Razlikuje se od drugih po tome što mreža ili host ne koriste specifične profile generisane od strane same IDPS, već se *Stateful* analiza oslanja na vendorov univerzalni profil kojim se određuje koliko se pojedinih protokola treba a koliko ne treba koristiti. Profili omogućavaju da IDPS razume i prati stanje od mreža, saobraćaja i primena protokola. Tako mogu da se identifikuju nizovi neočekivanih komandi, kao što je izdavanje iste komande više puta ili

izdavanje komande bez prethodnog izdavanje druge komande na osnovu koje ona zavisi. Za protokole koji zahtevaju autentifikaciju, IDPS može pratiti i snimati autentifikator koji se koristi za svaku sesiju i autentifikator koji se koristi za sumnjive aktivnosti, što je korisno kada se istražuju nesreće. Neki IDPSs su takođe u stanju da naprave razliku između više korisnika ili klasa korisnika i da definišu prihvatljive aktivnosti.

2.9.2.4. IDPS arhitektura i komponente

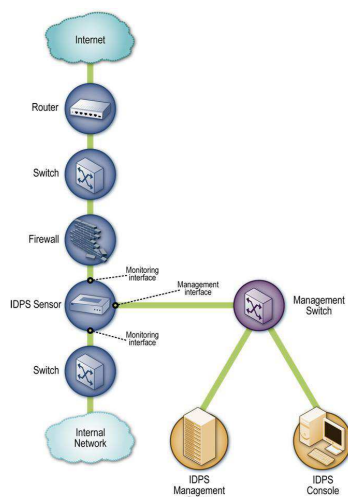
Sve vrste IDPS rešenja dele iste osnovne komponente, mada nije svaka od njih fundamentalna u svim slučajevima. Glavne komponente su sledeće:

- **Senzori ili agenti.** Oni su zaduženi za praćenje i analizu aktivnosti. Reč senzor se normalno odnosi na IDPSs monitor mreže, dok se zastupnik obično koristi za *Host-based* IDPSs. U prvom slučaju senzor može biti softverski program, ali uglavnom su *ad-hoc* aparati, dok je u drugom slučaju stražar deo softvera koji radi na it hostu.
- **Management servera.** Oni su centralizovani uređaji koji upravljaju senzorima ili agentima, koji obrađuju informacije prikupljene od strane senzora. Neke vrste senzora ili agenata su u stanju da obavljaju osnovnu analizu događaja koje otkriju, upravljanje serverima, s druge strane, mogu da obavljaju nekoliko vrsta analize i korelacijama događaja koji odgovaraju informacijama iz različitih senzora. Menadžment serveri su dostupni i kao aparati i kao sam softver. Za mala IDPSs rešenja može biti dovoljan jedan server za upravljanje, ali kod većih zahteva potrebno je uključiti više servera; obimnija angažovanja snaga obično imaju višestruke servere za upravljanje a u nekim slučajevima postoje dva nivoa.
- **Server baze podataka.** Koristi se kao spremište za informacija o događajima snimljenim od strane senzora ili agenta ili su obrađene za upravljanje serverima. To nije vitalni deo IDPS, iako su mnogi IDPS rešili da ga podrže.
- **Konzola.** Konzola je program koji obezbeđuje interfejs za korisnike IDPS i administratore. Obično se instalira na desktop ili notebook računare i može da pruži podršku administraciji, kao što su konfigurisanje senzora ili agente i primenu softvera ispravke, ili obe administracije i praćenje sposobnosti.

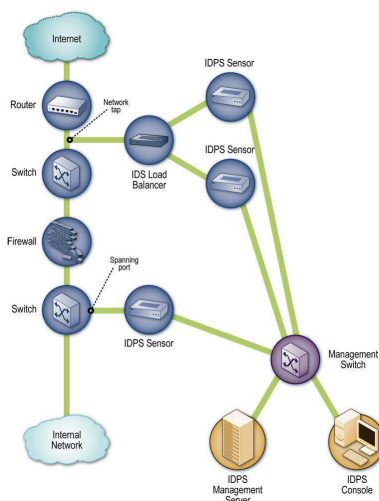
2.9.2.5. Vrste IDPS tehnologija

Četiri glavne vrste IDPS tehnologija su:

- **Mreža na bazi IDPS.** Mreža na bazi IDPS (NIDPS) prati saobraćaj žične mreže za određene mrežne segmente ili uređaje i analizira mrežu, transportne protokole i aplikacije koje identifikuju sumnjive aktivnosti. Većina analize vrši se na nivou aplikativnog sloja. Transportni i mrežni slojevi se takođe analiziraju kako bi se identifikovali napadi na te slojeve i da se pomogne analizi na nivou aplikativnog sloja (npr. TCP port broj mogao bi ukazati na aplikaciju koja se koristi). Hardverski sloj se ponekad analizira u ograničenoj meri. Senzori mogu da budu raspoređeni u jednom od dva režima: inline ili pasivno.

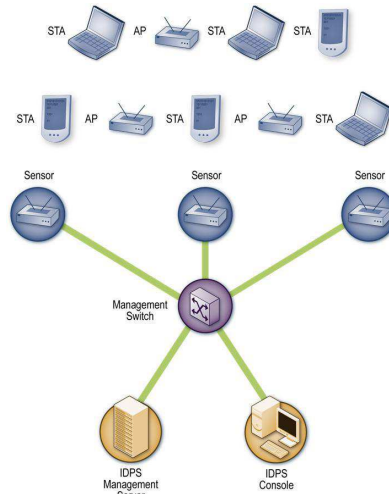


Slika 2.45. Mreža zasnovana na IDPS senzorima: inline raspoređivanje. [34]



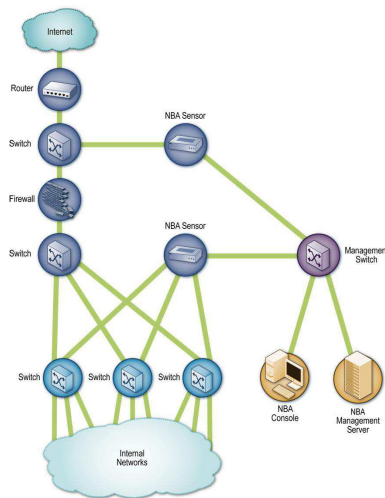
Slika 2.46. Mreža zasnovana na IDPS senzorima: pasivno raspoređivanje [34]

- **Wireless IDPS.** Bežični IDPS prati saobraćaj bežičnih mreža i analizira svoje bežične mrežne protokole za identifikaciju sumnjivih aktivnosti. Pretnje kod bežičnih mreža i žičanih mreža su uglavnom iste, ali relativni rizik od nekih pretnji značajno varira. *Wireless* napadi obično zahtevaju da napadači budu u neposrednoj blizini bežične mreže, dok mnogi napadi na žičane mreže mogu da se vrše daljinski sa bilo koje lokacije. Međutim, mnoge WLAN mreže su konfigurisane tako da zahtevaju samo slabe oblike autentifikacije, ako ih ima, čineći posao za lokalne napadače mnogo jednostavnijim. Tako lako može se sprovesti čovek-u-sredini napada ili napade koji se oslanjaju na ubrizgavanje dodatne poruke u mrežnim komunikacijama.



Slika 2.47. Razmeštanje bežični zasnovanih IDPS senzorov [34]

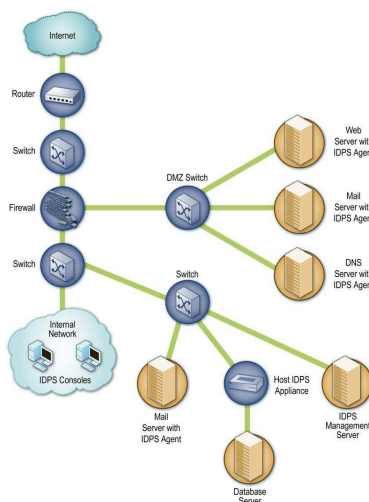
➤ **Sistem analiza ponašanja mreže (NBA).** Protok se kao posebna komunikaciona sesija javlja između domaćina (hostova). Sistem analiza ponašanje mreže (NBA) ispituje mrežni saobraćaj ili statistiku i identifikuje neobične tokove, kao što su distribuiranje uskraćivanja usluga napada, pojedini oblici zlonamernih programa i kršenja politike. Razlika sa mrežom zasnovanom na rešenju IDPS ne deluje upečatljivo: oni zajednički služi u iste svrhe, uz NBA sistem tehnika zasnovana na anomalijama ima sve širu upotrebu.



Slika 2.48. *NBA IDPS raspoređivanje [34]*

- **Host-based IDPS.** Za razliku od drugih tipova rešenja IDPS, koji su namenjeni da nadgledaju celokupan saobraćaj na mreži, bez obzira na njen izvor, *host-based* IDPS prati karakteristike jednog hosta i događaje koji se javljaju u tom hostu a predstavljaju sumnjive aktivnosti. *Host-based* IDPS može na primer pratiti dolazni i odlazni saobraćaj žične i bežične mreže, sistema za logovanje, pokrenute procese, pristup i modifikovanje datoteka, sistemskih aplikacija i promene konfiguracije.

Istu vrstu monitoringa često pružaju brojni anti-virusni softveri i lična *firewall* rešenja. Razlika između ovih alata postaje vrlo nejasna, jer mnogi od njih se preklapaju u funkcionalnosti.



Slika 2.49. *Host-based IDPS raspoređivanje [34]*

Četiri osnovna tipa IDPS tehnologija predstavljaju svaki za sebe fundamentalno različite načine prikupljanje informacija, evidentiranje, otkrivanje i sprečavanje mogućnosti napada. Svaki tip tehnologije pruža prednosti u odnosu na druge, kao što je otkrivanje nekih događaja koje ostali ne mogu, otkrivanje nekih događaja sa znatno većom preciznošću nego druge tehnologije, kao i obavljanje detaljnih analiza bez značajnog uticanja na performanse zaštićenih hostova. Svaka organizacija bi trebala da razmisli o korišćenju više tipova IDPS tehnologija čime se postiže sveobuhvatna i precizna detekcija i sprečavanje zlonamernog delovanja, sa nižim stopama lažnih uzbuna i lažnih negativ.

Sistemi za detekciju upada se razvijaju kao proizvodi. Istraživanje je počelo sredinom 1980-ih, a od pojave prvih proizvoda sredinom 1990-ih, ova oblast je nastavila da se menja kao novo istraživanje i dizajn proizvoda. Nedavni trendovi pokazuju da se na čelu ka integraciji tehnologija za detekciju upada u okviru TCP / IP, stvaraju takozvani stek-bazirani IDPS-ovi.

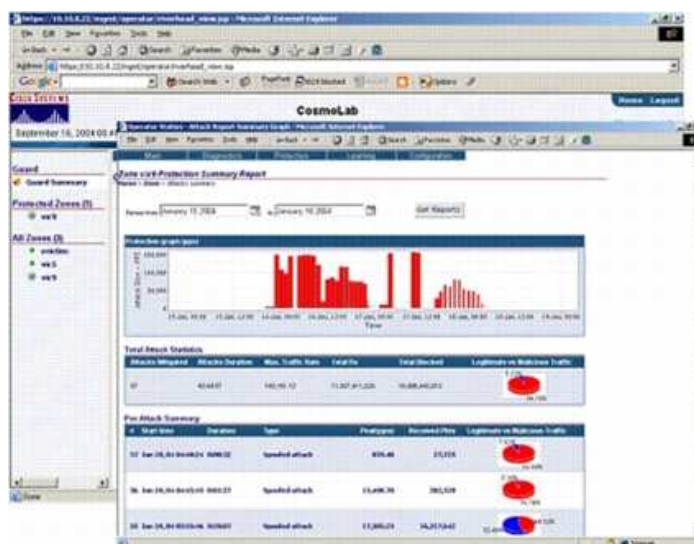
2.9.3. Cisco sistem zaštite

Cisco modul detekcije anomalija je pasivni monitoring uređaj koji stalno traži pokazatelje o DDoS napadu na zaštićenoj destinaciji kao što je server, *firewall* interfejs ili ruter interfejs. Ovaj modul analizira kopije svog dolazećeg saobraćaja namenjenog zaštićenim zonama. Kada se detektuje moguć napad, modul detekcije anomalije obaveštava modul zaustavljanja anomalije koji preusmerava sav saobraćaj u zoni pod napadom na čišćenje. Modul zaustavljanja anomalija podvrgava ovaj saobraćaj analizi i tu pravi razliku između napadnutog saobraćaja i legitimnog saobraćaja. Kada napad opadne, modul zaustavljanja anomalija legitiman saobraćaj upućuje u planiranu zonu.

Modul zaustavljanja anomalije nije normalno raspoređen kao inline uređaj. On koristi preusmeravanje saobraćaja na putu kako bi ublažio napad. Primena modula zaustavljanja anomalije „inline-na-zahtev“ omogućava efikasnije obezbeđivanje koji mora imati dovoljne kapacitete kako bi mogao da procesuirava sav saobraćaj. Ovo takođe omogućava otporniju mrežnu topologiju.

Modul detekcije anomalija saobraćaja se logično nalazi nizvodno od modula zaustavljanja, ali uzvodno od bili kog *firewall*-a. Modul zaustavljanja anomalija treba da bude što dalje od zaštićenih zona i što bliže izvoru mogućeg napada saobraćaja. Ovo omogućava modulu zaustavljanja anomalija da zaštiti sve resurse nizvodno od DDoS napada. Ovi resursi mogu se sastojati od servera, rutera, prekidača, zaštitnih zidova (*firewall*-ova) kao i sistema za detekciju upada (IDSs). Ovaj modul takođe mora biti postavljen uzvodno od *firewall*-a kako bi štitio i sam *firewall* od DDoS napada.

Cisco modul detekcije anomalija koristi modul baziran na Web-GUI koji prikazuje informacije na jednostavan i intuitivan način, drastično pojednostavljuje kofigurisanje, rad, identifikaciju napada i analiza. Modul detekcije anomalija može da se konfiguriše tako da se proaktivno pošalje upozorenje mrežnim operaterima i modulu zaustavljanja anomalije kako bi inicirali brzo reagovanje u uslovima napada, uključujući usluge automatskog ublažavanja i osujećivanja napada.



Slika 2.50. Praćenje i izveštavanje u realnom vremenu [38]

Tabela 2.6. Informacije o radu i kapacitetu saobraćaja Cisco modula detekcije anomalija

Odlika	Opis
Performanse	Opcija # 1: 1 Gbps • 1 Gbps protok po modulu • 1.5 miliona istovremenih konekcija • 500 zaštićenih zona • 90 istovremenih zona u zaštiti • Manje od 1 ms kašnjenje Opcija # 2: 2 Gb • 2 Gb protoka po modulu • 3 miliona istovremenih konekcija • 500 zaštićenih zona • 150 istovremenih zona u zaštiti • Manje od 1 ms kašnjenje

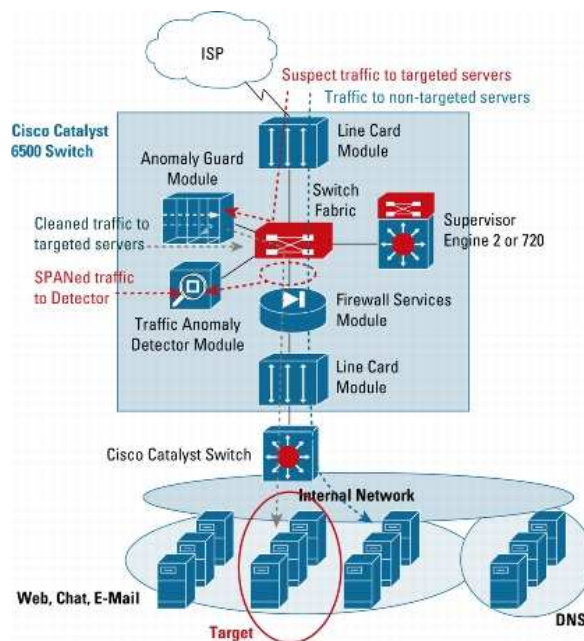
Tabela 2.7. Osobine Cisco modula detkcije anomalija

Odlika	Opis
Prepoznavanje napada	• lažni i nonspoofed napad • TCP napad • UDP napadi (<i>Random Port</i> poplave, fragmenti) • <i>Internet Control Message Protocol</i> (ICMP) napadi (nedostižnom, ECHO, fragmenti) • <i>Domain Name Sistem</i> (DNS) napada • Kljent napadi • HTTP GET napad • Granični <i>Gatevai Protocol</i> (BGP) napad • <i>Session Initiation Protocol</i> (SIP), <i>Voice over IP</i> (VoIP) napad
Kontinuirano učenje i otkrivanje	• može da radi u stalnom načinu detekcije • Istovremeno podešava pragove i detektuje napade • automatski prelazi između režima učenja i otkrivanja
Traffic Analysis	• Sposobnost da zarobi pakete koji su prošli pored čuvara i sačuva ih kao datoteke PCAP • GUI omogućava široku analizu zarobljenih paketa • korisnik može da filtrira snimanje koristeći <i>tcpdump</i> izraz
Protokoli za komunikacije	• <i>Secure Shell</i> (SSH), <i>Secure Sockets Laier</i> (SSL), <i>File Transfer Protocol</i> (FTP), <i>Secure FTP</i> (SFTP)
Upravljanje	• Konzola interfejs komandne linije (CLI) • SSH na CLI • SSL-u Cisco Device Manager • Jednostavni protokol za upravljanje mrežom (SNMP) MIB, MIBII, i zamke
Autentifikacija, autorizacija i računovodstvo (AAA) Podrška	• Integriše se sa AAA kroz TACACS + • Privilegija nivoa i komanda nivoa autorizacije i računovodstvo
Bezbednost	• IP sto i samo-DDoS zaštita za upravljanje interfejsa
Prijava	• Sveobuhvatna sislogging i događaji

Postoje dve vrste topologije mreže :

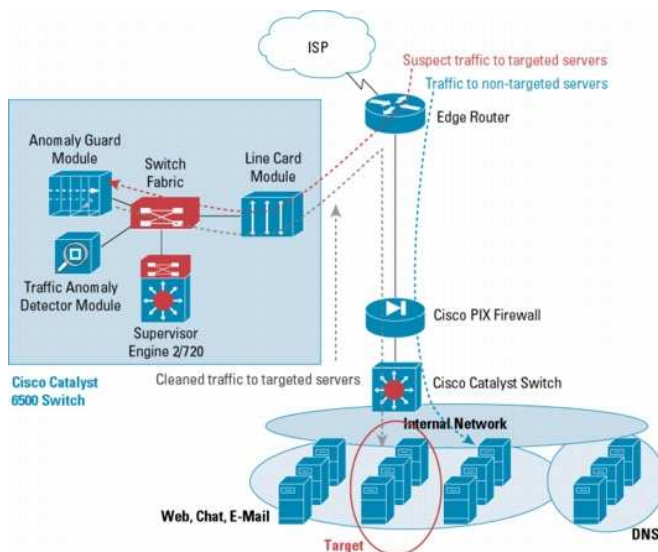
- a. Integrisana i
 - b. Namenska
- a. Integrisana topologija – saobraćaj normalno teče kroz cisco prekidač koji sadrži modul zaustavljanja anomalija. U integrisanoj konfiguraciji, ovaj modul koristi RHI dodatu statičku rutu na tabeli rutiranja prekidača koji otima saobraćaj. Zona

saobraćaja se preusmerava onda „interno“ iz supervizora motora do modula zaustavljanja anomalije. Saobraćaj takođe dolazi iznutra, iz modula zaustavljanja anomalije nazad na supervizor motora.



Slika 2.51. Integrirana topologija [39]

- b. Namenska (*out-of-out*) – u posvećenoj konfiguraciji modul zaustavljanja anomalije se nalazi u prekidaču koji nije u normalnom saobraćaju na putu u zaštićenu zonu. Preusmeravanje saobraćaja počinje tako što modul zaustavljanja anomalije šalje RHI poruku do supervizora motora, ali u drugom koraku supervizor motora raspodeljuje ovaj statički put uzvodno do rutera pomoću protokola rutiranja kao granični *gatevai protocol* (BGP) ili *open shortest path first* (OSPF). Namenska konfiguracija je namenjena za izgradnju namenskog aparata sa jednim ili više modula zaustavljanja anomalija unutar cisco šasije.



Slika 2.52. Namenska topologija [39]

Moduli detekcije anomalija i moduli zaustavljanja anomalija kod hosting provajdera, u ovom slučaju to je Telekom Srbija, obezbeđuju DDoS zaštitu za sve hostovane klijente.

2.9.4. Microsoft Windows Server 2003 – upravljanje web serverom

Informacioni servis interneta (*Internet Information Services*, IIS) isporučuje se sa Windows Serverom 2003, ali nije instaliran kao podrazumevan. Verzija Windows Servera 2003 koja je napravljena samo za opsluživanje web strana zove se *Web Edition*. Osnovna funkcionalnost IIS-a je da uslužuje web strane, bilo da to radi za klijente koji se povezuju udaljeno preko interneta ili da se osnovni računari povezuju preko LAN-a. IIS može da se koristi za mnogo više od toga. IIS može da se koristi kao platforma koja će biti podrška .NET web servisima, servisima Windows Media, servisa za sertifikate i za HTML usamljeno administriranje sistema pod Windows Serverom 2003. IIS takođe podržava FTP servis, koji može da se koristi za prenos datoteka između udaljenih osnovnih računara i servera. IIS podržava i servis protokol za prenos mrežnih konferencija (*Network News Transfer Protocol*, NNTP), dozvoljavajući da se konferencije ugošćuju na serveru i da ih mogu čitati klijenti kao što su Outlook Express i ostali klijenti za konferenciju.

Pristup IIS-u može da se podesi na nekoliko načina. Pristup može biti ograničen ili dozvoljen na osnovu IP adrese, DNS imena ili mrežne adrese. On može biti ograničen i samo na one osnovne računare koji imaju ispravan sertifikat ili pomoću Windowsove provere autentičnosti, ograničavajući pristup samo na one korisnike koji imaju naloge na sistemu ili unutar domena. Ove vrste ograničenja i pristupa nisu međusobno isključive, na primer: od klijenata se dalje može tražiti da obezbede kredibilitet za proveru autentičnosti čak i ako dolaze sa klijent mašina koje se nalaze unutar dozvoljenog mrežnog opsega.

Broj veza sa web lokacijom takođe može biti ograničen. Ovo može biti korisno iz nekoliko razloga: prvi je da se zaustavi da previše korisnika optereti server usled čega bi došlo do pada performansi; drugi je da se smanji uticaj web servera na vezu sa internetom u slučaju velikog saobraćaja.

Osnovni procesi koji se odvijaju kada klijent pristupi resursu iz IIS-a su:

- Klijent ulazi u URL u bilo kojoj od navedenih formi
- *Domain Name Service* zamenjuje ime IP adresom i vraća adresu klijentu
- Klijent se povezuje sa IP adresom servera koristeći port koji je karakterističan za taj servis (obično je to port 80 za HTTP i port 21 za FTP)
- URL ne predstavlja fizičku putanju ka resursu na serveru, već virtuelizaciju putanje. Server prevodi dolazni zahtev u fizičku putanju i obezbeđuje klijentu odgovarajući resurs
- Proces se može odigrati praćenjem identiteta (akreditiva, uključujući ime i lozinku korisnika) i autorizacijom (kontrolom pristupa preko ovlašćenja)

Bezbednost datoteka kojima se pristupa preko IIS-a spada u nekoliko kategorija: provera identiteta, autorizacija preko NTFS ovlašćenja i IIS ovlašćenja. Provera identiteta je, naravno, proces vrednovanja akreditiva u formi korisničkog imena i lozinke. Podrazumevano je da sve zahteve IIS-u upućuje oličenje korisnika čiji je IUSR nalog *_imeračunara*. Pre nego što se određenim korisnicima ograniči pristup resursima potrebno je napraviti domenske ili lokalne korisničke naloge i zahtevati nešto više od podrazumevanog, anonimne provere identiteta.

Web opcije za proveru identiteta:

- *Anonymous authentication* – korisnici mogu da pristupaju javnim područjima web prezentacije bez korisničkog imena i lozinke

- *Basic authentication* – zahteva da korisnik ima lokalni ili domenski korisnički nalog. Akreditivi se šalju u formi čistog teksta.
- *Digest authentication* – nudi istu funkcionalnost kao i osnovna provera identiteta, a dodatna bezbednost se postiže time što se korisnikovi akreditivi šalju preko mreže. Sažeta provera identiteta oslanja se na protokol HTTP 1.1
- *Advanced Digest authentication* – radi samo kada je korisnički nalog deo aktivnog direktorijuma. Uzima korisnikove akreditive i čuva ih na kontroloru domena. Unapređena sažeta provera identiteta zahteva da korisnik upotrebljava Internet Explorer 5 ili noviji i protokol HTTP 1.1
- *Integrated Windows authentication* – skuplja informacije sigurnom formom provere identiteta (koju nekada zovu Windows NT *Challenge/Response* provera identiteta), gde se korisničko ime i lozinka heširaju pre slanja preko mreže.
- *Certificate authentication* – dodaje sloj bezbedne logičke konekcije (*Secure Socket Layer*, SSL) preko klijenta ili sertifikata servera, ili oboje. Ova opcija je na raspolaganju samo ako imate *Certificate Services* instaliran i konfigurisan.
- *.NET Passport authentication* – nudi jedinstven servis za prijavljivanje preko SSL-a, HTTP preusmeravanja, kolačića, Microsoft J-Scripta i javnog šifrovanja simetričnim ključem.

FTP opcije za proveru identiteta:

- *Anonymouse FTP authentication* – daje korisnicima pristup javnim područjima korisnikove FTP prezentacije bez traženja korisničkog imena i lozinke.
- *Basic FTP authentication* – zahteva da se korisnik prijavi pod korisničkim imenom i lozinkom koji odgovaraju validnom Windows korisničkom nalogu.

Kada se provera identiteta konfiguriše, ovlašćenja se dodeljuju datotekama i direktorijumima. Uobičajeni način definisanja pristupa resursima kod IIS-a je preko NTFS ovlašćenja. NTFS ovlašćenja, pošto su priključena datoteci ili direktorijumu, dejstvuju da bi definisala pristup tom resursu bez obzira na to kako se resursu pristupa.

IIS takođe definiše ovlašćenja na prezentacijama i virtuelnim direktorijumima. Iako NTFS ovlašćenja definišu specifičan nivo pristupa za postojeće Windows korisničke i grupne naloge, bezbednosna ovlašćenja direktorijuma konfigurisana za prezentaciju ili virtuelni direktorijum primenjuju se na sve korisnike i grupe.

Tabela 2.8. IIS direktorijumske dozvole

Ovlašćenje	Objašnjenje
<i>Read</i> (podrazumevana)	Korisnici mogu da gledaju datoteku i svojstva
<i>Write</i>	Korisnici mogu da menjaju sadržaj i svojstva datoteka
<i>Script Source Access</i>	Korisnici mogu da pristupaju izvornom kodu datoteka, kao što su skriptovi u <i>Active Server Pages</i> (ASP) aplikaciji. Ova opcija je raspoloživa samo ako su dodeljene ili ovlašćenje <i>Read</i> ili ovlašćenje <i>Write</i> . Korisnici mogu da pristupaju izvornim datotekama. Ako je dato ovlašćenje <i>Read</i> , izvorni kod se može čitati. Ako je dodeljeno ovlašćenje <i>Write</i> , može se pisati i po izvornom kodu. Dozvoljavanje pristupa izvornom kodu korisnicima radi čitanja ili pisanja može da dovede u pitanje bezbednost servera.
<i>Directory browsing</i>	Korisnici mogu da gledaju liste i kolekcije datoteka.

Ovlašćenja Execute upravljaju bezbednosnim nivoom izvršenja skripta i opisana su u sledećoj tabeli.

Tabela 2.9. Aplikaciona ovlašćenja Execute

Ovlašćenje	Objašnjenje
<i>None</i>	Stavljanjem ovlašćenja za neku aplikaciju na <i>None</i> sprečava se da bilo koji program ili skript bude pokrenut
<i>Scripts only</i>	Zadavanjem ovlašćenja neke aplikacije kao <i>Scripts only</i> omogućava se da aplikacije mapirane kao interpretator rade u ovom direktorijumu bez zadatih ovlašćenja za izvršne datoteke. Zadavanje ovlašćenja <i>Scripts only</i> je sigurnije nego zadavanje <i>Scripts & Executables</i> pošto može da se ograniči koje aplikacije mogu biti pokretane u ovom direktorijumu.
<i>Scripts & Executables</i>	Stavljanjem ovlašćenja za neku aplikaciju da bude <i>Scripts & Executables</i> dozvoljava se da bilo koja aplikacija radi u ovom direktorijumu, uključujući aplikacije mapirane kao interpretatori i kao Windows binarne (.dll i .exe datoteke).

2.9.5. HSM

Zaštita tajnosti podataka se vrši primenom simetričnih kriptografskih algoritama, dok se ostali servisi realizuju primenom asimetričnih kriptografskih algoritama. Savremena rešenja sistema zaštite karakteriše višeslojna arhitektura, sa upotrebom hardverskih bezbednosnih modula (*Hardware Security Module*). Upotrebom hardverskih bezbednosnih modula se najčešće ostvaruje zaštita bezbednosno kritičnih podataka, kao što su kriptografski ključevi, korisničke šifre i privatni algoritmi zaštite, bezbednosna realizacija kriptografskih algoritama i drugih funkcija zaštite nezavisno od ostalih programa na računaru i ubrzavanje izvršavanja kriptografskih algoritama u odnosu na sisteme bazirane na isključivo softverskim postupcima zaštite.

Hardverski bezbednosni moduli, realizovani u vidu računarskih koprocesora, predstavljaju veoma bitnu karakteristiku savremenih rešenja zaštite računarskih mreža. Ovi moduli povećavaju performanse sistema tako što se vremenski kritične kriptografske funkcije izvršavaju na specijalizovanom hardveru a ne u softveru hosta računara. Postojanje hardverskog koprocesorskog kriptografskog modula od suštinske je važnosti za realizaciju kvalitetnog i performantnog sistema zaštite, kao i za ispunjenje poverljive aplikacije u punom smislu.

Svi bezbednosni mehanizmi (kriptografski algoritmi i funkcije kontrole pristupa) smešteni su na hardverskom modulu i nikada se ne učitavaju u radnu memoriju korisnikovog računara. Osnovne funkcije navedenih proizvođača su povećanje bezbednosti sistema i ubrzavanje kriptografskih funkcija, kao što su asimetrični i simetrični kriptografski algoritmi.

Primena HSM modula je neophodan uslov za bezbednu realizaciju funkcija sertifikacionog tela. HSM uređaju uglavnom realizuju standardne javne asimetrične i simetrične kriptografske i hash algoritme, kao što su: RSA, DSA, DES, 3-DES, RC2, RC4, SHA-1, MD2, MD5, itd.

Postoje eksterni kriptografski moduli, koji mogu imati bolje performanse u smislu brzine i zaštite velike količine podataka. Interni kriptografski moduli su optimalni u slučaju

kriptografskih sistema koji koriste princip rada sa porukama i primenjuju tehnologije digitalnog potpisa. Hardverski kriptografski koprocesori se predviđaju za korišćenje u serverskim aplikacijama i eventualno u klijentskim aplikacijama gde se zahteva visok nivo bezbednosti (državni organi, vojska, policija, SMIP, specijalizovane službe).

Sa druge strane, za najširi vid korišćenja sistema zaštite (npr. pojedinci), korišćenje smart kartica kao poverljive hardverske platforme je primerenije. U stvari, svi ti sistemi sa povišenim nivoom bezbednosti predstavljaju uglavnom kombinovane softversko-hardverske sisteme, pri čemu je hardverski deo ili koprocesor ili smart kartica. Sistemi sa najvišim nivoom bezbednosti koriste kombinovani softversko-hardverski sistem koji se sastoji od softverske aplikacije, kriptografskog koprocesora za realizaciju kriptografskih algoritama i smart kartica, kao bezbednih nosioca ključeva digitalnih sertifikata.

HSM moduli u okviru sertifikacionih tela imaju sledeću funkcionalnost:

- Generisanje ključeva na HSM – generisanje para ključeva asimetričnog kriptografskog algoritma, kao i zahtevanog broja simetričnih ključeva (opciono), realizuje se unutar HSM.
- Bezbedno čuvanje kriptografskih parametara – ključevi i ostali kriptografski parametri se bezbedno čuvaju (u šifrovanom obliku) na HSM modulu.
- Bezbedni back-up kriptografskog materijala – ključevi i drugi kriptografski parametri se mogu bezbedno sačuvati (*back-up-ovati*) na smart karticama ili drugim HSM modulima.
- HSM mora realizovati funkciju detekcije pokušaja zlonamernog pristupa modulu (*tamperproof*) – modul treba da obezbedi detekciju zlonamernog pristupa i uništenja bezbednosnog materijala na modulu ako je detektovan pristup.
- Modul mora biti sposoban da realizuje kriptografske funkcije – ovo je jedna od osnovnih namena HSM i ovi moduli su optimizovani za realizaciju funkcija generisanja ključeva, kao i realizaciju simetričnih i asimetričnih kriptografskih algoritama mnogo efikasnije nego u softveru ili na smart karticama.
- Bezbedno korišćenje PIN broja – modul se aktivira unošenjem PIN broja.

2.10. AUTENTIFIKACIJA U OKVIRU ZU APOTEKA VRANJE

U cilju autentifikacije ovlašćenih korisnika ZU Apoteka Vranje za pristup sistemu koriste se korisničko ime i lozinka koji su jedinstveni za pristup bazi i na osnovu kojih je za svakog korisnika definisano koja prava ima i kojim podacima može da pristupi.

Korisničko ime i lozinka za pristup sistemu se bezbedno dostavljaju do Web servera korišćenjem aplikativne zaštitne komponente u okviru *SWT* sistema i procedure jake autentifikacije. Na bazi tako, pouzdano i bezbedno, prenešenih podataka Web server Telekom Srbije proverava u bazi korisničkih profila da li je dati korisnik validan, tj. da li mu je izdati digitalni sertifikat u važećem periodu i nije povučen i da li je ovlašćen da koristi zahtevane servise. Ukoliko je verifikacija uspešna, Web server prosleđuje korisnički zahtev na bezbedan način do baze podataka Telekoma na dodatnu obradu zahteva.

Obzirom na neophodnost da korisničko ime i lozinka budu jedinstveni u sistemu, kompletni korisnički profili sa ovim podacima kao i podacima o pravima i privilegijama pristupa koje dati korisnik ima, čuvaju se na jednom mestu i to na *LDAP* serveru. Na ovom serveru se čuva i baza izdatih sertifikata i lista povučenih sertifikata – *CRL*. Na opisan način, usluge *LDAP* servera se koriste i od strane sertifikacionog tela.

Mehanizmi zaštite u okviru Telekoma Srbija baziraju se na X.509 standardnim digitalnim sertifikatima koje izdaje odgovarajuće sertifikaciono telo. U okviru Telekoma Srbija i korisnika ZU Apoteka Vranje moguća je realizacija sopstvenog *CA* u okviru Telekoma Srbije, za potrebe izdavanja digitalnih sertifikata ovlašćenih učesnika u sistemu.

Osnovni razlog za ovaj način poslovanja leži u činjenici da Komisija za hartije od vrednosti, u ovom trenutku, ne raspolaže potrebnim kadrovskim i tehničkim potencijalima za realizaciju CA. Iz navedenih razloga odlučeno je da se formira sertifikaciono telo u okviru samog Telekoma Srbija.

Osnovni principi na kojima se bazira rad CA Telekoma Srbija su sledeći:

- Arhitektura PKI sistema Telekoma Srbija se sastoji od jednog CA,
- CA Telekoma Srbija izdaje digitalne sertifikate i generiše odgovarajuće ključeve. Asimetrični ključevi su dužine minimalno 1024 bita, a mogu biti i duži i to 2048. ili 4096 bita, dok su simetrični ključevi minimalne dužine 256 bita,
- CA Telekoma Srbija je potpuno fleksibilno i skalabilno, kako softversko, tako i hardversko rešenje, koje je u potpunosti u skladu sa važećim međunarodnim standardima,
- CA Telekoma Srbija ispunjava sve uslove za rad sertifikacionog tela koji su navedeni u preporukama Evropske unije o elektronskom potpisu. Obzirom da je CA samostalno, podneće zahtev za akreditacijom nadležnom organu u skladu sa Zakonom o elektronskom potpisu kada se za to budu stekli uslovi, odnosno kada budu doneta sva potrebna podzakonska akta,
- CA Telekoma Srbija svoj rad bazira na primeni najviših proceduralno-fizičkih mera bezbednosti, kao i najviših tehničkih mera zaštite tajnih ključeva CA. Takođe su korišćeni hardverski kriptografski moduli – HSM kao i distribuiran sistem odgovornosti za tajni ključ CA.

U Telekomu Srbija formirano je kompletno sertifikaciono telo čiji je rad u potpunosti u skladu sa Zakonom o elektronskom potpisu.

2.11. MICROSOFT SQL SERVER

O kriptografskoj zaštiti podataka u SQL Serveru 2003 vodilo se računa od samog početka. SQL Server koristi jake kriptografske tehnike kako bi zaštitio podatke. SQL Server je u stanju da sam vrši upravljanje ključevima, a to upravljanje može da prepusti i samom korisniku. Implementirana je hijerarhija ključeva, koja omogućava kreiranje tri tipa ključeva koji se kasnije koriste u zaštiti podataka [11].

2.11.1. Kriptografija u SQL Serveru 2003

Kriptografija ugrađena u SQL Server podržava tri tipa kriptografije, svaki tip koristi različit tip ključa i svaki sa višestrukim algoritmima i dužinama ključa.

Kriptografija sa simetričnim ključem koristi isti ključ i za šifrovanje i za dešifrovanje. Zahtev je da entitet koji vrši šifrovanje ima isti ključ kao i entitet koji će te podatke da dešifruje. To znači da je ključ kojim se podaci šifruju i dešifruju deljena tajna koju je moguće sačuvati ako se čuva unutar SQL Servera.

Nisu svi kriptografski algoritmi podržani na svim Microsoftovim platformama. Microsoft preporučuje korišćenje AES algoritma ako on postoji na serveru, a ako ne onda 3DES.

Kod asimetrične kriptografije ključevi za šifrovanje i dešifrovanje su različiti. SQL Server podržava RSA algoritam sa ključevima od 512, 1024 i 2048 bita.

Sertifikati su još jedna forma asimetrične kriptografije. Sertifikati koriste digitalni potpis kako bi par privatni i javni ključ pridružili njihovom vlasniku. SQL Server koristi IETF X.509 specifikaciju, može koristiti interno generisane sertifikate, kao i sertifikate generisane od CA. Sertifikati koriste RSA algoritam za enkripciju.

2.11.2. Šifrovanje u Transact-SQL

Da bi šifrovanje bilo potpuno podržano na serveru, bilo je potrebno modifikovati SQL kako bi šifrovanje i dešifrovanje kao i upravljanje ključevima bilo dostupno dizajnerima sistema. Ovde će biti prikazani zajednički elementi, počev od dozvola.

Sve CREATE naredbe sadrže iskaz AUTHORIZATION koji daje vlasništvo nad objektom određenom korisniku. Pre davanja vlasništva potrebno je dobro razmisliti kome se daje to pravo, imajući na umu bezbednost servera. Iskaz AUTHORIZATION je važan kod kriptografije jer da bi šifrovao i dešifrovao podatke korisnik mora da bude vlasnik nekoliko ključeva potrebnih za izvršenje aktivnosti. Alternativno, korisnik mora da ima dozvolu CONTROL nad ključevima i sertifikatima.

Centralno mesto gde se odvija kriptografija u serveru su nove Transact-SQL funkcije. Sve funkcije koje implementiraju algoritme sa simetričnim ključem mogu da vrate podatke tipa *varbinary* maksimalne dužine od 8000 bajta. To znači da nije moguće šifrovati onaj tip podataka čija veličina prevazilazi ovo ograničenje. U takvim prilikama potrebno je ulazne podatke podeliti na manje celine, čiji će izlaz iz krypto funkcije biti manji od 8000 bajta. Slično je i prilikom dešifrovanja, funkcije koje dešifruju vraćaju niz od najviše 8000 bajta.

Kako funkcije za dešifrovanje (kao i funkcije za šifrovanje) kao izlazni podatak vraćaju podatak tipa *varbinary*, potrebno je eksplicitno izvršiti konverziju izlaznih rezultata u odgovarajući tip, kako ne bi došlo do kolizije pri upotrebi tih podataka.

Funkcije koje šifruju, koristeći asimetrični ključ ili sertifikat, za ulaz mogu da prime niz čija se dužina računa po formuli: [dužina ključa] mod 8 – 11.

2.11.3. Razmatranja

Prilikom odlučivanja o korišćenju kriptografije potrebno je razmisliti o performansama koje se tom prilikom degradiraju. Enkripcija je procesorski intenzivna operacija. Uopšteno govoreći, što je algoritam sigurniji, a ključ duži, to se zahteva veća procesorska snaga. To znači da će kriptografska zaštita svih podataka u imalo većoj bazi, blokirati rad servera bez obzira na hardversku platformu. Sledeći problem je što određeni algoritam kod šifrovanja daje niz čija je dužina veća od ulaznog niza. Koliko će to povećanje biti zavisi od samog algoritma, dužine ključa, i od otvorenog teksta koji se šifruje. Postoje znatne razlike u tome koliko koji algoritam uvećava ulazne podatke i to od 43% pa do 2460%. Ovako visok procenat uvećanja je dobijen kada se niz od 10 znakova šifrovao RSA algoritmom sa ključem od 2048 bita, čime se dobija šifrovani niz od 256 bajta. Prilikom implementacije kriptografske zaštite podataka treba imati na umu i ovaj problem.

2.11.4. Hijerarhija ključeva

Zaštita i čuvanje ključeva je jedna od najvažnijih stvari u zaštiti podataka. Sa izuzetkom javnog ključa kod asimetrične kriptografije, ključ treba da bude zaštićen od neautorizovanog korišćenja. Bez obzira na kvalitet algoritma, on postaje bezvredan u slučaju da ključ dospe u pogrešne ruke. SQL Server implementira hijerarhiju ključeva gde svaki nivo štiti ključeve na sloju ispod sebe.

Na vrhu hijerarhije je *Data Protection API*, ili skraćeno DPAPI, koji je deo operativnog sistema i nalazi se u podsistemu Crypto32. DPAPI štiti serverov master ključ koji je glavni ključ za svaku instancu SQL servera koji je instaliran na računaru. Servis master ključ štiti master ključ baze podataka, koji je potreban za svaku bazu podataka koja se nalazi na serveru. Master ključ baze podataka štiti sve ključeve koje korisnik kreira,

sertifikuje, i asimetrične ključeve. Svaki od ovih ključeva može da štiti simetrične ključeve, a simetrični ključevi mogu da štite ostale simetrične ključeve. Dodatno, svaki od ključeva na nivou baze podataka korisnik može štititi lozinkom, i na taj način preuzeti zaštite lozinke na sebe. Prilikom dizajna sistema kriptografske zaštite treba imati na umu ovu hijerarhiju jer se prilikom svakog ključa generisanog u bazu treba odlučiti kojim ključem ga štitimo.

2.11.5. Master ključ SQL servera

Servis master ključ je na vrhu hijerarhije svih ključeva kojima SQL server upravlja. Pošto taj ključ štiti svoje ključeve unutar SQL servera, on ima veoma značajnu ulogu. On se automatski kreira prilikom instalacije SQL servera i ne zahteva nikakvo upravljanje, osim što bi ga trebalo arhivirati na sigurno mesto van servera. Postoji samo jedan servis master ključ za svaku instaliranu instancu servera. Korisnik ga ne može ni kreirati ni uništiti. Sam ključ je pod zaštitom DPAPI (*Data Protection API*) iz Windows operativnog sistema. Kao i svi ključevi koju su pod zaštitom DPAPI, ključ se štiti korišćenjem akreditiva ulogovanog korisnika. Što se tiče SQL servera „korisnik“ je ustvari servis nalog pod kojim SQL servis radi. To znači da bilo ko, ko ima pristup tom nalogu može da pristupi servis master ključu, što još jednom naglašava strogu kontrolu ko može da ima pristup nalogu pod kojim SQL server radi.

Servis master ključ direktno štiti različite interne podatke uključujući lozinke na linkovane servere, master ključeve baze podataka kao i mapirane akreditive naloga. Ne postoji direktan pristup servis master ključu unutar servisa, jedina stvar koja se može uraditi je njegovo održavanje. Jedna od prvih stvari koju treba uraditi posle instaliranja SQL servera je arhiviranje, i to se može uraditi sledećom naredbom:

```
BACKUP SERVICE MASTER KEY TO FILE = 'C:\KLJUC.DAT'  
ENCRYPTION BY PASSWORD = '(/&jzgaWoG1J_)*(&lkjKwH,4kBYg;J\'
```

Lozinka u ovoj naredbi šifrue master ključ, tako da master ključ ne napušta server u otvorenom obliku. Potrebno je da lozinka bude kvalitetna i da može da se upamti (što je u kontradikciji jedno sa drugim, teško da može da se zapamti lozinka koja je data u primeru).

```
RESTORE SERVICE MASTER KEY TO FILE = 'C:\KLJUC.DAT'  
DECRYPTION BY PASSWORD = '(/&jzgaWoG1J_)*(&lkjKwH,4kBYg;J\'
```

Osim arhiviranja i povraćaja, servis master ključa se može i regenerisati. Ovu akciju bi trebalo izvesti samo u slučaju kompromitovanja master ključa. Proces regeneracije se odvija u više koraka. Svi ključevi ispod servis master ključa se dešifruju starim ključem, generiše se novi servis master ključ, pa se njime šifruju svi ključevi ispod njega. Ako postoji veliki broj ključeva ispod servis master ključa, ovakva situacija može da bude procesorski intenzivna, pa se preporučuje da se uradi u vreme slabe aktivnosti servera.

2.11.6. Master ključ baze podataka

Sledeći ključ koji je u hijerarhiji niže od SQL servera je master ključ baze. Master ključ baze štiti sve ključeve unutar određene baze. To je simetrični ključ koji se koristi direktno od strane samog servera, a ne od strane korisnika odnosno aplikacija. Postoji samo jedan master ključ po bazi, pokušaj da se kreira još neki prouzrokuje grešku.

Master ključ baze podataka se ne kreira automatski po kreiranju baze podataka, nego se mora kreirati ručno, pre kreiranja ključeva za šifrovanje unutar baze:

```
USE bps
CREATE MASTER KEY ENCRYPTION BY PASSWORD =
'KoR@n0R4n1Ce0DaHZ3wa'
```

Proverom se može ustanoviti da je ključ zaista kreiran:

```
Select name from sys.symmetric_keys;
go
name
-----
##MS_DatabaseMasterKey##
```

Iako je poznato da se master ključ baze šifrjuje master ključem servera (servis master), postavlja se pitanje čemu služi opcija PASSWORD pri kreiranju master ključa baze. To je zbog toga što se master ključ baze podataka šifrjuje i smešta u bazu sa imenom master. Druga kopija se šifrjuje algoritmom 3DES a ključ se generiše na osnovu date lozinke i smešta se u samu bazu. Ako master ključ baze postoji, moguće je isključiti njegovu zaštitu servis master ključem korišćenjem naredbe ALTER MASTER KEY. Ova naredba uklanja ključ iz baze master :

```
ALTER MASTER KEY DROP ENCRYPTION BY SERVICE MASTER KEY
```

To praktično znači da se master ključ baze podataka ne može otvoriti sa master ključem servera, i mora se eksplicitno otvoriti pre upotrebe. Ako se kasnije odlučimo da vratimo master ključ baze podataka pod zaštitu servis master ključa to se može uraditi naredbom:

```
ALTER MASTER KEY ADD ENCRYPTION BY SERVICE MASTER KEY
```

Zaštita master ključa baze podataka lozinkom je korisna stvar kod premeštanja baze podataka sa jednog servera na drugi. Prilikom odvajanja baze podataka od servera, iz master baze se uklanja stavka vezana za bazu koja se premešta, a istovremeno se uklanja i kopija master ključa baze koja je pod zaštitom servis master ključa. Kada se baza prebaci na novi server, na tom novom serveru master servis ključ je drugačiji, i zaštita master ključa baze podataka se ne uspostavlja automatski. Da bi se zaštita master ključa baze uspostavila sa novim servis master ključem, potrebno je otvoriti master ključ baze sa lozinkom koju smo dali prilikom njegovog kreiranja. Posle toga treba upotrebiti naredbu ALTER MASTER KEY da bi se master ključ baze šifrovao servis master ključem, i da bi

se tako zaštićeni ključ smestio u bazu sa imenom master. To je obrazloženje zašto je zgodno imati master ključ baze podataka i samu bazu šifrovanu lozinkom.

2.11.7. Korisnički ključevi

Sledeća vrsta ključeva u SQL serveru su korisnički ključevi. Postoje četiri vrste korisničkih ključeva i to su:

- Sertifikati – podrazumevaju korišćenje asimetričnih ključeva, odnosno parova tajnog/javnog ključa. Sertifikat je u stvari digitalno potpisan objekat, koji pridružuje javni ključ entitetu koji poseduje tajni ključ. SQL server je u stanju da kreira sertifikate koji se mogu koristiti jedino unutar servera. Sertifikati se oslanjaju na specifikaciju IETF X.509. Treba znati sa SQL server ne vrši proveru kod eksternog sertifikacionog tela, i ne podržava opoziv sertifikata. Naredba CREATE CERTIFICATE se koristi da bi se sertifikat uneo u bazu podataka gde će biti dostupan za šifrovanje podataka.
- Asimetrični ključevi – koriste se u slučaju da nam nisu potrebne sve mogućnosti koje nude sertifikati, ali i dalje imamo potrebu da koristimo sistem sa javnim ključevima. Ako nemamo potrebu za migracijom ključeva, a sva kriptografija se završava unutar baze podataka asimetrični ključevi su dovoljni za taj posao. Šifrovanje asimetričnim ključem se vrši korišćenjem funkcije *EncryptByAsymKey*, prosleđivanjem identifikatora asimetričnog ključa i otvorenog teksta koji se šifrue.
- Simetrični ključevi – nisu u stanju da odgovore izazovu u većini okruženja gde se zahteva razmena podataka. To je zbog toga što obe strane moraju imati isti ključ, što predstavlja veliki izazov za sigurnu razmenu ključeva. U tim slučajevima simetrični ključ se šifrue asimetričnim ključem kako bi se rešio problem razmene simetričnog ključa. Šifrovanje simetričnim ključem je idealno kod serverskih aplikacija kakva je i SQL server, gde je potrebno podatke smestiti u obliku šifrovanog teksta. Pošto podatke ne treba iznositi van servera, ova vrsta šifrovanja nudi dobru zaštitu uz dobre performanse. Simetrični ključ se ne može štititi korišćenjem master ključa baze podataka. To je jedina vrsta ključa koja se može zaštititi ključem istog tipa. Sa svim mogućim opcijama naredba CREATE SYMMETRIC KEY je istovremeno i fleksibilna i kompleksna.
- Ključevi lozinke – koriste se kada nije potrebno snimati ključeve u bazi podataka. Ako želimo da sami rukujemo ključevima, bez oslonca na SQL server, i time preuzmemo čuvanje tajne na sebe, koristićemo funkcije *EncryptByPassPhrase* i *DecryptByPassPhrase*. Ovim funkcijama je dovoljna lozinka kao prvi parametar, i otvoreni tekst kao drugi parametar kod šifrovanja, odnosno šifrovan tekst kod dešifrovanja.

3. ANALIZA REZULTATA

3.1. ANALIZA REZUTATA

U procesu posmatranja i testiranja informacionog sistema i računarske mreže ZU Apoteka Vranje identifikovani su sledeći glavni nalazi:

Glavne slabosti:

1. U Sektoru infrastrukture i zaštite ustanove jedan zaposleni pokriva više uloga u celokupnom radu sistema. Ova činjenica bitno utiče na formalizaciju aktivnosti, za koju zaposleni pored redovnih radnih obaveza nemaju vremena, odnosno za formalno planiranje aktivnosti, dokumentovanje dnevnih radova značajnih radnih sastanaka, dokumentovanje analiza izveštaja, arhiviranje i dokumentovanje rezultata analize stanja procesa i sl. Na taj način ova slabost je opšta preporuka za podizanje svih OP na viši nivo.
2. Tekući procesi koji se primenjuju u radu nisu konkretno definisani i opisani kao standardni procesi ustanove. Relativno dobro su opisani procesi koji podržavaju primenjivane PKI tehnologije na nivou tehničke dokumentacije na bazi Microsoft tehnologija i Windows platformi. Standardni procesi nisu adekvatno dokumentovani i sistematizovani u određenu biblioteku standardnih procesa. Ovakva praksa rada je ključna prepreka za implementaciju i insitucionalizaciju generičkih praksi (GP) i podizanja izvršavanja svih BP i OP na viši nivo.
3. Politika/program zaštite na nivou ustanove, kao strateški dokument za zaštitu, nije formalno definisana, napisana i dokumentovana. Nedostaju formalne politike upravljanja brojnim komponentama zaštite, kao i za upravljanje dokumentacijom zaštite i konfiguracijom – bekapovanjem osnovne konfiguracije sistema zaštite (*security baseline*). Takođe, nedostaju formalna politika zaštite koja bi trebala biti izrađena prema preporukama standarda ISO IEC 17799. Ovim bi se stvorile pretpostavke za uspostavljanje OP za upravljanje bezbednosnim rizikom.
4. Metrike PKI zaštite nisu eksplicitno planirane i dokumentovane. Ne postoji izjava u razvijenim politikama komponenti sistema o uvođenju i korišćenju systemske i procesne metrike za stvaranje argumenata garantovane bezbednosti i kontinualno poboljšavanje procesa. Iako se brojni metrički podaci sklapljaju u izvršavanju standardnih procedura, ne vrši se regularna analiza sakupljenih podataka o bezbednosnom stanju sistema. Filtrirani bezbednosno relevantni log podaci prenose se nezaštićenim linijama. Ova slabost je opšta preporuka za implementaciju i insitucionalizaciju GP na CL2 i CL3 za sve inženjerske OP.
5. Oblasti procesa za upravljanje bezbednosnim rizikom ne izvršavaju se, neformalno ni *ad hock*, nisu planirane ni dokumentovane na bilo koji način. ESS ne koristi ni jednu formalnu ili neformalnu metodu za analizu rizika, procenu ranjivosti, procenu pretnji i procenu uticaja (iskoristivost) pretnji na identifikovane ranjivosti sistema, poslove i ugled ustanove. Implementaciju PKI sistema ESS vrši na bazi standardnih Microsoft definisanih politika, tehničkih procedura i Microsoft najbolje prakse zaštite, pa podrazumeva da su relevantni faktori bezbednosnog rizika već ublaženi takvim rešenjima. Ne postojanje i ne izvršavanje procesa upravljanja bezbednosnim rizikom, za ovu organizaciju, može se smatrati najvećom slabosti i opštom preporukom za podizanje ovih OP na viši nivo.
6. Izgradnja argumenata bezbednosne garancije formalno se ne planira i ne izvršava u celini. Međutim, BP koje generišu argumente bezbednosne garancije neformalno se izvršavaju u okviru izvršavanja standardnih Microsoft procedura i monitorisanja

operativnog rada, ali nisu pokrivene formalnom politikom niti su eksplicitno dokumentovane kao procedure ili proces izgradnje argumenata garantovane bezbednosti. Ova slabost u izvršavanju BP opšta je prepreka za podizanje ove OP na viši nivo.

Snaga organizacije:

1. Iako se metrika procesa ne planira, na nivou procesa praktično se u okviru aktivnosti monitorisanja operativnog rada i korisničkog izveštavanja o incidentima primenjuju tri tipa metrika:

- Heurističko merenje nedostataka i defekata
- Automatski (e-mail) dostavljanje metričkih podataka u XML formatu o stanju bezbednosti i incidentima sistema i
- Korisničko izveštavanje o incidentima u sistemu

Generalno, u procesu monitorisanja brojni metrički podaci se sakupljaju automatizovanim sistemima, ili fizičkim opservacijama (izveštajima korisnika). Ovakva praksa je dobra osnova za opšte povećanja kvaliteta izvršavanja BP, odnosno uvođenja metrike na višim nivoima.

3.2. IZRADA LISTE PREPORUKA ZA OSTVARENJE ICT BEZBEDNOSTI

Identifikovani i ocenjeni bezbednosni rizici u ustanovi podeljeni su u tri kategorije, prema veličini negativnog uticaja na:

- Visok (*high*) – ocena evaluacije rizika od 300 do 450
- Srednji (*medium*) – ocena evaluacije od 150 do 299
- Nizak (*low*) – ocena evaluacije od 0 do 149

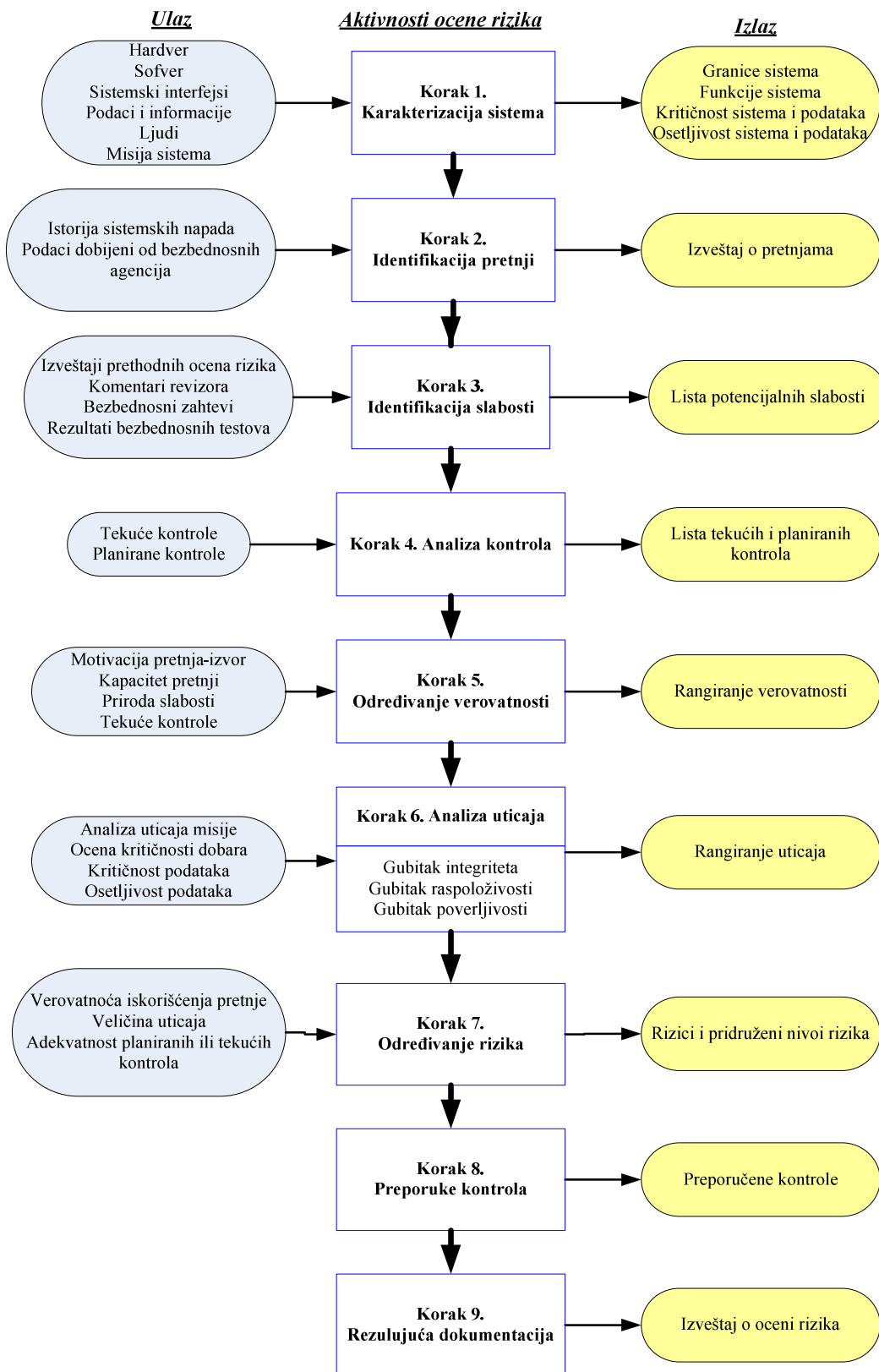
Pristup oceni bezbednosnih rizika u ustanovi sastoji se od:

- Identifikacije pogodne metodologije ocene rizika
- Utvrđivanja kriterijuma za prihvatanje rizika
- Identifikacija prihvatljivih nivoa rizika
- Obezbeđenja da ocena rizika proizvodi uporedive i ponovljive rezultate

Odluka o metodi ocene rizika koja će se primeniti je u odgovornosti menadžmenta kompanije.

Izabrani metod ocene rizika treba da pokrije bezbednosne rizike koji se odnose na:

- Organizacione aspekte
- Kontrolu zaposlenih
- Poslovne procese
- Procese i procedure operativnog rada i održavanja
- Pravne, regulatorne i ugovorne aspekte
- Opremu za procesiranje informacija



Slika 3.1. Dijagram toka procesa ocene bezbednosnih rizika

Ovde predlažemo i rešenja za umanj enje identifikovanih rizika. Rešenja se generalno dele na predloge:

- Implementacije odgovarajuće tehničke bezbednosne kontrole
- Izrade odgovarajuće administrativne bezbednosne kontrole.

3.2.1. Predlog skupa tehničkih bezbednosnih kontrola za implementaciju

Predložene tehničke kontrole su poređane u odnosu na nivo uticaja odgovarajućeg bezbednosnog rizika, i to od najvišeg ka najmanjem uticaju.

Lista tehničkih kontrola:

- **SAP ruter** – Izbaciti SAP ruter. Pristup korisnika SAP-u obezbediti putem posebnog VLAN-a i ACL na centralnom L3 switch-u i/ili kompletan SAP sistem pozicionirati u posebnu zonu na ASA *firewall* uređaju sa najvišim nivoom bezbednosti u odnosu na korisnike interne korporativne mreže. Pristup korisnika iz spoljne mreže obezbediti samo putem VPN-a koji se terminira na spoljnom ASA interfejsu.
- **BCP (*Business Continuity Plan*)** – Uvesti BCM (*Business Continuity Management*) proces u kompaniji koji podrazumeva odgovarajuću analizu rizika i BIA (*Business Impact Analizu*) koliko mogući incidenti prekida poslovanja mogu uticati na kritične poslovne procese ustanove, kao i koliko nedostatak određenog poslovnog procesa može negativno uticati na poslovanje ustanove. Na osnovu tih analiza izraditi BCP (*Business Continuity Plan*) za kritične procese u kompaniji. Neophodno je pokrenuti proces definisanja i karakterisanja važnosti poslovnih procesa u ustanovi – BPM (*Business Process Management*).
- **DRP (*Disaster Recovery Plan*)** – Na osnovu prethodno navedenih BCM procesa, analiza i aktivnosti izraditi plan oporavka od katastrofa – *DRP (Disaster Recovery Plan)* za kritične procese u ustanovi, i to pre svega za slučaj nedostatka ICT infrastrukture kompanije.
- **Loša bezbednosna mrežna izolacija** – Konsolidovati računarsku mrežu ustanove po pitanju bezbednosti. Definirati novu konfiguraciju ASA *firewall* uređaja i definisati nove zone (DMZ i eventualno više internih zona). U okviru interne zone, izvršiti dodatnu bezbednosnu izolaciju putem konfiguracije VLAN mreža. Razmotriti mogućnost da se svi serveri sa javnom IP adresom prebace u DMZ i NAT-uju u javne IP adrese na eksternom interfejsu ASA uređaja. Administracija pomenutih servera bi se tada vršila iz interne zone putem internih IP adresa.
- **Terminacija VPN tunela na ruteru** – VPN tunele za spoljne korisnike terminirati na spoljnom interfejsu ASA *firewall* uređaja. Za interne korisnike, VPN tuneli se mogu terminisati na ruteru u internoj mreži ukoliko je kompletna mreža korisničkih računara i komunikacionih uređaja sa internim IP adresama. U postojećoj situaciji, kada se interna mreža povezuje preko Interneta ili odgovarajućih servisa drugog provajdera, VPN tunele *remote office*-a za interne korisnike terminirati na eksternom interfejsu ASA *firewall* uređaja ili na odgovarajućem ruteru u posebnoj eksternoj zoni na ASA *firewall* uređaju.
- **Interne WEB aplikacije** – Obezbediti SSL/TLS zaštitu pristupa internim WEB aplikacijama – po mogućstvu, i gde je to prikladno, sa uključenom klijentskom

autentifikacijom na bazi smart kartica i digitalnih sertifikata izdatih zaposlenima kompanije.

- **Nepostojanje *firewall* zaštite pristupu korporativnim informacionim sistemima (tehnički sistem) sa javne mreže** – Pristup tehničkom sistemu obezbediti u internoj mreži putem posebnih VLAN-ova i ACL na L3 *switch*-evima a iz spoljne mreže samo putem VPN-a koji se terminira na spoljnom ASA interfejsu ili na odgovarajućem ruteru u posebnoj eksternoj zoni na ASA *firewall* uređaju.
- **Ažurna tehnička dokumentacija** – Sva dokumentacija mora da bude u jedinstvenoj formi koja će omogućiti konceptualno lak i jednostavan pristup svim traženim podacima autorizovanim zaposlenima. Svaka izmena konfiguracija mora da se ažurira u dokumentaciji od momenta čim se promena u konfiguraciji desi.
- **Centralizovana analiza logova sa opreme i bezbednosno nadgledanje funkcionisanja informacionog sistema kompanije** – Uvesti centralizovan sistem prikupljanja i analize logova sa opreme – SIEM (*Security Information and Events Monitoring*) sistem. Posebno obratiti pažnju na sakupljanje logova sa opreme koja je kritična za poslovanje i bezbednost ustanove.
- **Logovanje aktivnosti sistem administratora** – Uvesti tehničke kontrole putem kojih će se posebno pratiti aktivnosti sistem administratora na sistemu.
- **Dodeljivanje, ukidanje i promena prava korisničkih naloga, kao i redovan pregled korisničkih prava u sistemu** – Implementirati sistem za automatski provisioning i deprovisioning korisnika – Sistem za upravljanje identitetom i pristupom (IAM – *Identity and Access Management*).
- **Dvo-faktorska VPN (IPSec) autentikacija** – Implementirati dvo-faktorsku VPN (IPSec) autentifikaciju na bazi PKI digitalnih sertifikata i smart kartica za korisnike. Implementirati interni PKI sistem u kompaniji za izdavanje digitalnih sertifikata zaposlenima u kompaniji.
- **Autentifikacija računarske opreme u mreži** – Implementirati sistem kontrole pristupa računarskoj mreži kompanije (NAC – *Network Access Control*). Nakon implementacije ovog sistema, biće uvedena kontrola na krajnjim tačkama i neće biti moguće konektovati bilo kakav računar na računarsku mrežu kompanije ukoliko računar nije u saglasnosti sa definisanom politikom bezbednosti. Drugim rečima, pristup neće biti moguć bilo kom uređaju koji nije zadovoljio predefinisane parametre (npr. da su AV licence potpuno ažurirane, da su implementirani svi patch-evi i sl.). Takođe, u kombinaciji sa 802.1x autentifikacijom uređaja, biće sprečena konekcija neautorizovanih računara u računarsku mrežu kompanije.
- **Pristup upravljačkim portovima mrežne opreme** – Implementirati sistem autentifikacije korisnika i zaštite pristupa upravljačkim portovima mrežne opreme u zavisnosti od toga šta dati sistem može da podrži. U tom smislu, primeniti SSH, HTTPS ili sistem dinamičkih password-a (OTP – *One Time Password*) na bazi odgovarajućih hardverskih tokena.
- **Bezbedno logovanje na operativni sistem** – Implementirati sistem bezbednog logovanja korisnika na operativni sistem kompanije putem dvo-faktorske autentifikacije na bazi smart kartica i digitalnih sertifikata (*Windows smart card logon*).

- **Bezbedno logovanje na SAP i ostale aplikativne informacione sisteme kompanije** – Tamo gde je to moguće i opravdano, implementirati sistem bezbednog logovanja korisnika na aplikativne informacione sisteme ustanove putem dvo-faktorske autentifikacije na bazi smart kartica i digitalnih sertifikata.
- **Administracija servera sa privatnih računara** – Zabraniti pristup mreži ustanove sa privatnih računara a posebno aktivnosti administracije računarskih resursa ustanove. Ukoliko je potrebno da se vrši udaljena administracija, datom zaposlenom dodeliti službeni notebook koji će se koristiti kao radna stanica u mreži ustanove, kao i za potrebe eventualne udaljene administracije.
- **Patch management system** – Potrebno je implementirati jedinstven *patch management* sistem za sve tipove opreme i nadograditi sve operativne sisteme na poslednju pouzdanu verziju. Urgentno nadograditi sve bitnije identifikovane sigurnosne propuste. Pre same nadogradnje potrebno je da tehnički tim izvrši detaljna testiranja sistema i kompatibilnosti s postojećim aplikacijama. U tom smislu, oformiti lab okruženje u kome će tehnička ekipa ZU Apoteka Vranje testirati svoje aplikacije nakon primene *patch*-eva i *bug fixes*. Nakon svih potrebnih testiranja i ukoliko se utvrdi da nove zakrpe neće uticati na sistem onda se one implementiraju u produkcijom sistemu.
- **Ne postoji IPS (*Intrusion Prevention System*) sistem** – Implementacija IPS uređaja u okviru korporativne mreže.
- **End point zaštita na radnim stanicama** – Pored antivirusnog softvera, koji je obavezan, na radnim stanicama je potrebna implementacija dodatnih bezbednosnih funkcionalnosti putem odgovarajućeg takozvanog *EndPoint Security* rešenja sa centralizovanim nadgledanjem.
- **Kontrola pristupa Internet resursima i zaštita na nivou GW (*GateWay*) uređaja** – Implementirati sistem *Web Content Filtering*, tj kategorizacije Internet resursa i uvesti punu kontrolu čime bi se postigla i veća produktivnost zaposlenog osoblja. Management ustanove može da dobija redovne mesečne izveštaje o korišćenju Internet resursa. Takođe, takav sistem mora da podrži i antivirusnu i drugu proveru sadržaja sa Interneta, na nivou GW a pre dolaska do korisničkih PC računara, sprečavajući na taj način maliciozne *script* programe da se izvršavaju.
- **Upravljanje incidentima u kompaniji** – Procedure za rešavanje incidenata u okviru informacionog sistema ustanove moraju biti dokumentovane i za proveru njihove ispravnosti moraju se simulirati jednom ili dva puta godišnje. Obično u simuliranim situacijama se može doći do zaključaka i aktivnosti koje mogu da unaprede postojeći plan oporavka što smanjuje potencijano vreme neraspoloživosti sistema.
- **Šifrovanje podataka na prenosnim medijima** – Šifrovanje podataka na prenosnim medijima primenom odgovarajućih softverskih rešenja (za ovo postoje čak i *freeware* softveri). Pored šifrovanja hard disk-a za notebook računare može biti potrebno postaviti i BIOS-lozinku.
- **Zaštita Web aplikacija koje se postavljaju na korporativnom Web serveru ZU Apoteka Vranje** – Korišćenje tzv. *Web Application Firewall* sistema koji štiti on-line aplikacije i podatke od, između ostalih, *SQL Injection* i *Cross Site Scripting* napada (sada čak postoje integrisani sistemi zajedno sa IPS uređajem).

- **Korišćenje SNMPv3 protokola za prenos monitoring podataka** – Implementacija SNMPv3 protokola koji obezbeđuje integritet podataka, šifrovanje i autentifikaciju što je bitno za prenos ovog tipa podataka (nadzor se mora vršiti na svim uređajima u IT sistemu).
- **Zaštita bezbednosno osetljive dokumentacije kompanije** – implementirati kriptografske kontrole zaštite dokumentacije. Razmotriti potrebe i opravdanost uvođenja odgovarajućeg eDMS (*electronic Document Management System*) rešenja.
- **Zaštita postupka razmene informacija** – implementirati kriptografske kontrole zaštite postupka razmene informacija.
- **Administrativne privilegije na serverima** – Implementirati odgovarajuće kontrole koje uključuju principe separacije dužnosti i distribucije odgovornosti za realizaciju kritičnih aktivnosti u vezi administracije servera.
- **Jedinstvena autentifikacija korisnika za pristup korporativnim poslovnim informacionim sistemima** – Razmotriti mogućnost i potrebu uvođenja sistema jedinstvene autentifikacije korisnika (Windows autentifikacija i/ili odgovarajući *Single-Sign-On* sistem) za pristup poslovnim aplikacijama kompanije na osnovu dvo-faktorske autentifikacije korisnika na bazi smart kartica.
- **Konfiguracija zaštite na svič portovima: *configuration portsecurity*** – Svi neiskorišćeni portovi na svičevima moraju biti onemogućeni (na Cisco svičevima to je podešeno ali ovo se odnosi i na eventualno neupravljive svičeve u sistemu) dok se na korišćenim portovima moraju koristiti napredne mogućnosti kao na primer omogućenje porta samo za određenu MAC adresu uređaja (npr. računare, servere, skenere, štampače i sl.). Takođe, potrebno je težiti da se u celom sistemu ZU Apoteka Vranje koriste upravljivi svičevi sa navedenim mogućnostima.
- **Nema protivprovalne zaštite u server sali** – Razmotriti potrebe i opravdanost implementacije sistema protivprovalne zaštite u server sobi.
- **Ne postoji posebna organizaciona jedinica zadužena za ICT bezbednost** – Oformiti posebnu i nezavisnu poslovnu organizacionu jedinicu zaduženu direktno za ICT bezbednost.
- **Mogućnost odavanja domenskih kredencijala putem web maila** – Omogućiti web mail samo ograničenom broju korisnika i to samo sa službenih računara.
- **Izmena lozinke svakih 30 dana** – Razmotriti opravdanost isključivanja ove funkcije kod određenih korisnika i po potrebi revidirati.
- **Implementacija SSL VPN uređaja** – Razmotriti mogućnost, potrebu i opravdanost implementacije SSL VPN sistema u ustanovi. Implementacija SSL VPN uređaja ima sledeće prednosti:
 - Nema potrebe za bilo kakvu konfiguraciju na klijentu,
 - Integracija sa skoro svim važnijim Web browser-ima,
 - Drastično se smanjuje administrativni *overhead*,
 - Transparentan je sa NAT-om ili bilo kojim *Proxy* uređajem,
 - Prekidom SSL VPN sesije svi log-ovi i cach memorije se brišu sa bilo kog uređaja

- Vršiti se provera statusa uređaja koji pristupa i u slučaju postojanja bilo kakvog malicioznog koda tom uređaju nije omogućen pristup
- **Fizički ograničiti pristup serverskoj i komunikacionoj opremi na svim lokacijama ustanove** – Fizički omogućiti pristup opremi samo ovlašćenim licima.
- **Korišćenje najvišeg nivoa šifrovanja za VPN komunikaciju** – Izvršiti rekonfiguraciju opreme i po mogućstvu koristiti algoritme AES256 i hash SHA-2.
- **Integritet konfiguracionih fajlova** – Koristiti odgovarajući softver za nadzor nad promenama i integritetom trenutnih konfiguracionih podataka (smanjuje se rizik od neautorizovane promene podataka i vrlo lako se detektuju nastale izmene).
- **Nisu primenjeni bezbednosni mehanizmi u Web service komunikaciji** – Razmotriti mogućnost uvođenja XML *security* i/ili WS-*Security* mehanizama.
- **Nema SMTP gateway-a za korporativni mail sistem** – Razmotriti mogućnost uvođenja SMTP *gateway*-a u DMZ.
- **Evaluacija izloženosti informacionog sistema ustanove ranjivostima** – Izvršiti evaluaciju i ponavljati je periodično.
- **Outsourcing razvoj softvera** – Implementirati odgovarajuće tehničke kontrole pri razvoju softvera od strane trećih lica.
- **Pristup izvornom kodu aplikacija** – Implementirati odgovarajuće kontrole zaštite pristupa izvornom kodu aplikativnih rešenja ustanove.
- **Proces upravljanja ključevima** – Implementirati odgovarajuće kontrole zaštite svih procesa upravljanja kriptografskim ključevima u ustanovi.
- **Validacija ulaznih podataka u aplikacijama ustanove** – implementirati odgovarajuće kontrole.
- **Zaštita integriteta podataka u aplikacijama ustanove** – Implementirati odgovarajuće kontrole.
- **Validacija izlaznih podataka u aplikacijama ustanove** – Implementirati odgovarajuće kontrole.
- **Osetljivi podaci ustanove** – Izraditi i primeniti odgovarajuće kontrole za postupanje i zaštitu osetljivih podataka ustanove.
- **Rizici pristupa podacima od strane zaposlenih treće strane** – Izraditi odgovarajuće bezbednosne kontrole.
- **NOC na više lokacija** – centralizovati NOC funkcije.
- **Nedovoljno precizno definisani poslovni procesi** – Potrebno je sprovesti BPM (*Business Process Mapping*) proces u ustanovi.
- **Nadzor ICT opreme** – Razmotriti mogućnost optimizacije organizacije ustanove u smislu nadzora ICT opreme.
- **Kvantifikovanje bezbednosnih incidenata** – Definirati i primeniti odgovarajuće mere u smislu kategorizacije bezbednosnih incidenata u informacionom sistemu ustanove.

- **Klasifikacija opreme** – Izvršiti odgovarajuću bezbednosnu klasifikaciju opreme sa stanovišta nivoa kritičnosti po bezbednost informacionog sistema ustanove.
- **Security awareness program** – Izraditi odgovarajući program obuke zaposlenih u domenu ICT bezbednosti.
- **Oticanje informacija** – Implementirati odgovarajuće kontrole u aplikativnim rešenjima ustanove radi zaštite od oticanja informacija.
- **Sprovođenje tehničkih kontrola** – Periodično vršiti proveru sprovođenja implementiranih tehničkih kontrola.
- **Autentifikacija OSPF protokola** – Konfigurisati MD5 autentikaciju koristeći MD5 *hash*-ovanu lozinku (kao što je odrađeno za iBGP) ili koristiti neki drugi *hash* algoritam ukoliko je raspoloživ.
- **Pozdravna poruka prilikom logovanja na komunikacionu opremu** – Konfigurisati pozdravne poruke, tzv. *banner*-e, koje upozoravaju na pravnu odgovornost (u praksi je potrebno koristiti lokalni jezik i engleski).
- **Informacije o aktuelnim ranjivostima informacionih sistema** – Obezbediti dobijanje ažurnih informacija o trenutno aktuelnim tehničkim ranjivostima informacionih sistema.
- **Provera sprovođenja administrativnih mera bezbednosti** – Proveravati sprovođenje donetih administrativnih kontrola bezbednosti, kako u normalnom radu (periodično, npr. jednom godišnje) tako i posle značajnih promena.
- **Korišćenje alata za reviziju informacionog sistema** – Implementirati adekvatne tehničke kontrole primene odgovarajućih alata za reviziju informacionog sistema ustanove.
- **Zahtevi za informatičkom bezbednošću** – Implementirati odgovarajuću kontrolu praćenja legalnih i regulatornih zahteva u vezi ostvarenja bezbednosti informacija u ustanovi.
- **Bezbednosni zahtevi u specifikacijama za nove sisteme** – Uvesti bezbednosne zahteve u sve specifikacije zahteva za novim sistemima.
- **Svi korisnici imaju izlaz na internet** – Uvesti restriktivan pristup prilikom dozvoljavanja zaposlenim da pristupaju Internetu.
- **Raznorodni mail klijenti** – Ujednačiti *mail* klijente u ustanovi.
- **Ponovna ocena pristupa ICT bezbednosti nakon značajnih promena** – Ponovo ocenjivati adekvatnost pristupa ostvarenju sistema ICT bezbednosti uvek nakon značajnih promena u sistemu.
- **Interna revizija ICT bezbednosti** – Redovno vršiti internu reviziju ICT bezbednosti, po mogućstvu jednom godišnje, kao i nakon značajnih promena i bezbednosnih incidenata.
- **Zaštita kablova** – Implementirati adekvatne mere.
- **Održavanje opreme** – Konsolidovati proces održavanja opreme, pre svega one koja je kritična za bezbednost ustanove.
- **Zahtevi bezbednosti u ugovoru o radu** – U ugovore o radu uvesti članove koji propisuju zahteve bezbednosti koje treba da ispune zaposleni.

- **Evidencija informacionih dobara** – Voditi posebnu evidenciju informacionih dobara u kompaniji.
- **Kontakti sa interesnim grupama u domenu ICT bezbednosti** – Ostvarivati kontakte sa interesnim grupama u domenu ICT bezbednosti.
- **Provera kandidata pre zaposlenja** – Sprovoditi adekvatnu bezbednosnu proveru kandidata pre zaposlenja, posebno ukoliko se zaposleni prima na radno mesto sa ingerencijama u domenu ICT bezbednosti.
- **Eksterna revizija ICT bezbednosti** – Periodično vršiti eksternu reviziju implementiranog sistema ICT bezbednosti.

3.2.2. Predlog skupa administrativnih bezbednosnih kontrola za izradu

Ovde je navedena lista predloženih administrativnih bezbednosnih kontrola u cilju umanjenja identifikovanih bezbednosnih rizika.

Predložene administrativne kontrole su poređane u odnosu na nivo uticaja odgovarajućeg bezbednosnog rizika, i to od najvišeg ka najmanjem uticaju.

Lista administrativnih kontrola koje treba izraditi:

- **Kontinuitet poslovanja** – Definirati program upravljanja kontinuitetom poslovanja u ustanovi
- **Identifikacija događaja koji mogu da naruše kontinuitet poslovanja ustanove** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu u vezi sprovođenja analize uticaja kritičnih poslovnih procesa na poslovanje ustanove (BIA – *Business Impact Analysis*).
- **Metodologija kontinuiteta poslovanja** – Izraditi metodologiju upravljanja kontinuitetom poslovanja ustanove.
- **Izraditi BCP i DRP** – Izraditi plan kontinuiteta poslovanja (BCP – *Business Continuity Plan*) i plan oporavka nakon katastrofe (DRP – *Disaster Recovery Plan*).
- **Testiranje BCP i DRP** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu za testiranje BCP i DRP.
- **Upravljanje incidentima u ustanovi** – Procedure za rešavanje incidenata moraju biti dokumentovane i za proveru njihove ispravnosti moraju se simulirati jednom ili dva puta godišnje.
- **Propisivanje odgovornosti za upravljanje incidentima** – Implementirati odgovarajuću administrativnu bezbednosnu kontrolu.
- **Propisivanje kontrola u vezi sakupljanja informacija o incidentima** – Implementirati odgovarajuću administrativnu bezbednosnu kontrolu.
- **Otvorena vrata serverske sobe dok nekoga ima u njoj** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu u kojoj precizirati postupanje u serverskoj sobi.
- **Mogućnost gubitka ključeva serverske sobe na terenu** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu u kojoj treba precizirati postupanje sa ključevima od serverske sobe, u smislu da se ne mogu iznositi na teren.

- **Back-up – administrativna kontrola** – Izraditi odgovarajuće i adekvatne administrativne bezbednosne kontrole.
- **Dodeljivanje i ukidanje korisničkih naloga** – Izraditi odgovarajuću administrativnu kontrolu.
- **Dodeljivanje, ukidanje i promena prava i privilegija** – Izraditi odgovarajuću administrativnu kontrolu.
- **Redovan pregled prava pristupa** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Kriterijumi za prihvatanje sistema** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Propisivanje načina zaštite bezbednosno osetljive dokumentacije ustanove** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Propisivanje zaštite postupka razmene informacija** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Propisati administrativne privilegije na serverima** – Izraditi odgovarajuće administrativne kontrole.
- **Upravljanje promenama** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Pristup informacijama kompanije od strane eksternih korisnika** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Ugovori sa spoljnim stranama i bezbednosni zahtevi** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Administrativne kontrole za bezbednost računarske mreže ustanove** – Izraditi odgovarajuće administrativne kontrole.
- **Propisivanje zaštite memorijskih medijuma** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Upotreba domenskih i local admin naloga** – Izraditi odgovarajuću administrativnu kontrolu.
- **Propisati administrativne privilegije na radnim stanicama** – Izraditi odgovarajuće administrativne kontrole.
- **Nadležnost oko uređaja i prostorija** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu i propisati jasne nadležnosti.
- **Rad sa prenosivim računarima** – Implementirati odgovarajuću administrativnu bezbednosnu kontrolu.
- **Pristup aplikativnim sistemima kompanije** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Jedinstvena autentifikacija korisnika** – Izraditi odgovarajuće administrativne bezbednosne kontrole.
- **Disable-ovanje i ukidanje prava za one koji napuštaju kompaniju** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Maliciozni kod** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.

- **Iznošenje opreme van prostorija kompanije** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Zahtev za ICT podršku** – Izraditi odgovarajuću administrativnu kontrolu.
- **Propisivanje zahteva prilikom *outsourcing* razvoja softvera** – Implementirati odgovarajuću administrativnu bezbednosnu kontrolu.
- **Propisivanje zahteva u vezi pristupa izvornom kodu aplikacija** – Implementirati odgovarajuću administrativnu bezbednosnu kontrolu.
- **Kontrola izmena u informacionom sistemu** – Implementirati odgovarajuću administrativnu bezbednosnu kontrolu.
- **Kontrola izmena u domenu operativnih sistema** – Implementirati odgovarajuću administrativnu bezbednosnu kontrolu.
- **Propisivanje zahteva u vezi zaštite upravljanja kriptografskim ključevima** – Implementirati odgovarajuću administrativnu bezbednosnu kontrolu.
- **Propisivanje zahteva u vezi zaštite tajnosti podataka** – Implementirati odgovarajuću administrativnu bezbednosnu kontrolu.
- **Propisivanje postupka validacije ulaznih podataka** – Implementirati odgovarajuću administrativnu bezbednosnu kontrolu.
- **Propisivanje zahteva za zaštitom integriteta podataka** – Implementirati odgovarajuću administrativnu bezbednosnu kontrolu.
- **Propisivanje zahteva u vezi validacije izlaznih podataka** – Implementirati odgovarajuću administrativnu bezbednosnu kontrolu.
- **Propisivanje rada sa udaljenog mesta** – Implementirati odgovarajuću administrativnu bezbednosnu kontrolu.
- **Separacija mrežnih segmenata** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Ograničavanje konekcije na računarsku mrežu** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Autentifikacija korisnika na operativni sistem kompanije** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Autentifikacija korisnika na aplikativne sisteme kompanije** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Izbor lozinke** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Oprema bez nadzora** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Politika praznog stola** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Politika praznog ekrana** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Korišćenje računarskih mrežnih servisa** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.

- **Autentikacija korisnika kod udaljenog pristupa** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Automatska identifikacija računarske opreme** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Centralizovana analiza logova** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Monitoring računarskih resursa** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Zaštita log informacija** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Odvojeno logovanje sistem administratora** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Sinhronizacija sistemskih vremena** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Kontrola pristupa podacima ustanove** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Zaštita opreme van prostorija ustanove** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Klasifikacija informacija** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Security awareness program** – Izraditi odgovarajući program.
- **Prekid rada zaposlenih** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Razdvajanje test, razvojne i produkcijske opreme** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Sistem fizičke kontrole pristupa na osnovu beskontaktnih kartica** – Izraditi odgovarajuću dokumentaciju i administrativnu bezbednosnu kontrolu.
- **Razdvajanje dužnosti** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Zaštita privatnosti podataka** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Praćenje sprovođenja administrativnih kontrola** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Bezbednosna pravila upravljanja telekomunikacionom opremom** – Izraditi odgovarajuću administrativnu bezbednosnu kontrolu.
- **Disciplinski postupci za zaposlene** – Izraditi adekvatnu administrativnu kontrolu koja će propisati disciplinske postupke.
- **Zaštita od mobilnog koda** – Izraditi adekvatnu administrativnu kontrolu.
- **Korišćenje UPS uređaja i agregata** – Izraditi adekvatnu administrativnu kontrolu.

- **Promptno izveštavanje o bezbednosnim slabostima** – Izraditi odgovarajuću administrativnu kontrolu.
- **Ograničenje vremena konekcije** – Izraditi odgovarajuću administrativnu kontrolu.
- **Bezbednosni zahtevi u specifikacijama za nove sisteme** – Uvesti bezbednosne zahteve u sve specifikacije zahteva za novim sistemima.
- **Zaštita prava intelektualnog vlasništva** – Izraditi odgovarajuću administrativnu kontrolu.
- **Upravljanje kapacitetom** – Izraditi adekvatnu administrativnu kontrolu.
- **Propisivanje zahteva za informatičkom bezbednošću** – Izraditi odgovarajuću administrativnu kontrolu.
- **Propisivanje korišćenja alata za reviziju informacionog sistema** – Izraditi odgovarajuću administrativnu kontrolu.
- **Revizija informacionog sistema** – Izraditi odgovarajuću administrativnu kontrolu.
- **Zaštita kablova** – Izraditi adekvatnu administrativnu kontrolu.
- **Održavanje opreme** – Izraditi adekvatnu administrativnu kontrolu.
- **Oprema koja se odlaže** – Izraditi adekvatnu administrativnu kontrolu.
- **Modifikacije softverskih paketa** – Izraditi odgovarajuću administrativnu kontrolu.

Kontakti sa autoritetima u domenu bezbednosti – Izraditi odgovarajuću administrativnu kontrolu.

Neke od pripremljenih dokumenata u vidu procedura i pravilnika možete videti u delu Prilozi.

4. DISKUSIJA

Osnovni problem koji se javio prilikom izrade ovog rada i koji je isključivo vezan za rizike konkretnog informacionog sistema (a koji se može proširiti i na rizike ostalih informacionih sistema naročito u našem okruženju) bio je potpuno odsustvo bilo kakvih nagoveštaja i zapisa o postojećoj tematici. Radi se o tome da se do sada u praksi govorilo samo o četiri tzv. klasična načina smanjenja rizika u bilo kojem području nauke, tehnike i tehnologije (prihvatanje, prenos na treće lice, smanjenje i izbegavanje) dok se mali broj osvrnuo na još jedan element rizika – njegovu strukturu.

Prilikom proučavanja materijala koji sam koristila za izradu ovog rada posebno sam obratila pažnju na deo koji se odnosi na prekidačke složene mreže i pouzdanost sistema višeg reda. Primenjujući pročitano u praksi došla sam do zaključka da je moja pretpostavka tačna a to je da niz parametara celokupnog složenog sistema isključivo zavisi od njegove strukture i stanja parametara koji tu strukturu čine.

Sada se ova činjenica treba primeniti i na terenu čime bi omogućili potpuno nov način smanjenja rizika a time i kompletnog upravljanja rizicima složenih sistema, prvenstveno kada su u pitanju složeni informacioni sistemi.

Međutim, to se pokazalo kao veoma krupan zalogaj koji nije bilo lako savladati odjednom i u relativno kratkom vremenskom intervalu. Kada tu uzmemo u obzir i ljudski faktor (koji u ovom delu Srbije nije baš najbolje informatički pismen) vidimo da se nalazimo pred velikom preprekom koju treba savladati. Zbog toga je bilo neophodno dobro analiziranje i proučavanje sledećih oblasti:

- Kompletnog poslovno-informacionog sistema *Hubi-e*
- Analiza i sinteza celokupnog poslovno-informacionog sistema ZU Apoteka Vranje koji pokriva teritoriju celog Pčinjskog okruga i samim tim čini jedan veoma složen sistem
- Teoriju rizika i sve pripadajuće aspekte vezane uz rizike.

Svemu tome treba dodati i neophodnost poznavanja svih temeljnih zakona, standarda, preporuka i najbolje prakse koja strogo propisuje ponašanje i tretman u navedenim oblastima.

Standardi, pogotovo međunarodni, ne dozvoljavaju bilo kakvo ispadanje izvan propisanih granica, definicija i odrednica, što je sve skupa dodatno usložnjavalo istraživanja. Pri tome treba da vodim računa i o činjenici da nije reč o dva ili tri standarda po oblasti, već su u pitanju cele serije, tzv. familije standarda i niz smernica koje ih prate. Neispunjavanje strogih direktiva u standardima značilo bi istovremeno i potpuno obezvređivanje celog istraživanja, što je bilo nedopustivo.

Kada se doda i neosporna potreba kombinacija navedenih oblasti, sve skupa je postiglo takav nivo koji je prerastao u višegodišnji poseban projekat. U tom vremenskom periodu bilo je potrebno obaviti sledeće operacije:

- Planiranje
- Prikupljanje dokumentacije
- Proučavanje, analiza i sinteza problema,
- Izgradnja hipoteza,
- Izgradnja modela,
- Realizacija i testiranje modela,
- Potvrda modela u obliku programskih rešenja,
- Dobijanje rezultata,
- Formiranje konačnih zaključaka

Kao i svako kretanje po nepoznatom području, projekat je često bio opterećen naizgled nerešivim problemima, višemesečnim zastoјima, ispitivanjima i ponavljanjem pojedinih delova projekta. Možda je najveći problem bio što, uz nedostatak potrebne literature, nije bilo pravog odziva u samoj osnovi pa čak i onemogućavanje bavljenjem problematikom projekta od strane novoformiranog menadžmenta. Sa dolaskom novog direktora na čelo ustanove javljaju se dodatni problemi koji uzrokuju povremeno a ponekad i privremeno obustavljanje rada na samom projektu, što iz neznanja što iz loših međuljudskih odnosa. Kao dokaz tome imamo Izvod iz zapisnika sa sednice Upravnog odbora ZU Apoteka Vranje gde je jedna od tačaka bila i odluka o usvajanju „Politike bezbednosti IKT sistema ZU Apoteka Vranje“ što se vidi na sledećoj slici:

Upravni odbor je doneo jednoglasno sledeće

O D L U K E

1. Usvaja se Izvod iz zapisnika sa XVII sednice Upravnog odbora Apoteke Vranje.
Usvaja se Izveštaj Centralne popisne komisije o popisu na dan 31.12.2009.godine. Na sledećoj sednici dostavi Vrednost otpisanih lekova po Apotekama i Zalihe lekova.
2. Popis knjižiti na sledeći način: Manjkovi idu na teret Ustanove, dok se ne dobije izveštaj nadležnog organa u vezi provalne krađe u Apotekarskoj jedinici. Vlase.. Viškovi se prihoduju.
3. Da se u svim apotekama gde je utvrđen manjak sačeka izveštaj konsultanske kuće, koja bi nakon sprovedene analize predložila određene mere u cilju nadoknade manjka.. Ostaje odluka na teret odgovornih lica računopolagača za naknadu manjka.
4. Usvaja Izveštaj pacijentovog advokata – zaštitnika pacijentovih prava.
5. Usvaja se Plan nabavki za 2010.godinu.
6. Menja se odluka sa prethodne sednice u vezi angažovanja revizorke kuće i glasi:
Da se angažuje konsultanska kuća, koja u sastavu ima revizora i iskustva u radu sa zdravstvenim ustanovama. Pri izboru bodovaće se koliko cena toliko i referentna lista – rada u zdravstvenim ustanovama.
Komisija će obavestiti Upravni odbor o izboru konsultanske kuće.
7. Usvaja se Politika bezbednosti IKT sistema ZU Apoteke Vranje.
8. Usvaja se Plan stalnog unapređenja kvaliteta rada Apoteke Vranje za 2010.godinu.
9. U vezi nedostavljanjem dopisa- zapisnika, službene beleške ili potvrde od strane PU Vranje obratiti se Gradskoj Upravi, Gradskom veću, kao osnivaču.

Predsednik
Upravnog odbora Apoteke Vranje
Dr Goran Arsić, spec pedijatrije, s.r.

Slika 4.1. Izvod iz zapisnika Upravnog odbora ZU Apoteka Vranje

Tom prilikom usvojena je prvobitna verzija politike bezbednosti IKT sistema ZU Apoteka Vranje koju ovim predstavljam u celosti :

Република Србија
АПOTEKA ВРАЊЕ
Број 92
Датум 02.02. 2010. год.
Стефана Првовенчаног 43
ВРАЊЕ

Politika bezbednosti IKT sistema ZU Apoteka Vranje

Zahtevi ZU Apoteke Vranje za bezbednost informacija

Ovom politikom ZU APOTEKA VRANJE ističe značaj i obavezu zaštite ljudi, materijalnih resursa i svih osetljivih informacija koje nisu klasifikovane kao javne. Ove informacije tretiraju se kao važna i privatna imovina ustanove.

Rukovodstvo ZU APOTEKA VRANJE ulaže veliki napor da održi visok nivo bezbednosti informacija, ali u tome može uspeti samo ako svi zaposleni razumeju svoju ulogu i odgovornost za zaštitu informacija.

Osnovni zahtevi Politike bezbednosti ZU APOTEKA VRANJE su:

1. Održavanje kontinuiteta kritičnih poslovnih procesa uz minimalno prekidanje rada
 - 1.1. *Uspostaviti planove, procedure, uputstva i organizovati i održavati redovnu obuku zaposlenih za situacije iznenadnih prekida poslovanja ili nekog vanrednog događaja.*
2. Kontrola zaštite
 - 2.1. *Da bi se maksimalno sprečili poslovni i materijalni gubici i kompromitovanje poslovnog ugleda, implementirati u ZU APOTEKA VRANJE adekvatnu fizičku i logičku zaštitu pristupa imovini ZU APOTEKA VRANJE, zaštitu informacija, ljudi i ostalih materijalnih resursa.*
 - 2.2. *Kontrole zaštite implementirati u skladu sa poslovnim ciljevima i zahtevima, standardima, relevantnim zakonima i ugovornim obavezama.*
3. Obuka i odgovornost za zaštitu
 - 3.1. *Svi zaposleni moraju neprekidno razvijati svest o potrebi zaštite i biti svesni štetnih posledica koje mogu nastati zbog slabe ili neadekvatne zaštite informacija u ZU APOTEKA VRANJE*
 - 3.2. *Svi zaposleni moraju da efektivno koriste uputstva i procedure zaštite koje su im namenjene*
 - 3.3. *Svaki zaposleni preuzima ličnu odgovornost za zaštitu informacija, koja mu je pripisana politikom funkcionalne komponente sistema zaštite*
4. Obavezna primena politike zaštite
 - 4.1. *Svi zaposleni moraju da se pridržavaju ustanovljenih standarda, politika, procedura i uputstava za zaštitu.*
 - 4.2. *Za povredu ove politike predviđena je materijalna, prekršajna ili krivična odgovornost u skladu sa pravilnicima ZU APOTEKA VRANJE i relevantnim zakonima Republike Srbije.*
5. Usklađenost sa relevantnim standardima i zakonima
 - 5.1. *Ova politika je je usklađena sa misijom, strategijom razvoja, poslovnim ciljevima i standardima poslovanja ZU APOTEKA VRANJE, kao i sa Zakonom o borbi protiv visokotehnološkog (kompjuterskog) kriminala, Zakonom o elektronskom potpisu i drugim relevantnim zakonima Republike Srbije.*
 - 5.2. *Sve politike zaštite funkcionalnih komponenti sistema zaštite LANE moraju se uskladiti sa ovom politikom i sa najšire prihvaćenim međunarodnim i domaćim standardima zaštite informacija.*

Ova politiku odobrava Upravni odbor i direktor ZU APOTEKA VRANJE .

Direktor ZU Apoteka Vranje



Bez obzira na gore navedeno rad na projektu je otežavan samom činjenicom da zaposleni kao i menadžment ne shvataju neophodnost definisanja zaštite poslovno-informacionog sistema kao i strogo pridržavanje zakonskih regulativa koje definišu ponašanje svakog korisnika u sistemu.

Pored toga imamo i problem nedostatka stručne literature iz razloga što su ovde obuhvaćene nekoliko naučnih i stručnih oblasti. Navedimo sasvim konkretne primere:

- Već sama definicija informacionog sistema prema raznoj dostupnoj literaturi stvara nedoumice. Razlog je u činjenici da ne postoji jedinstvena definicija informacionog sistema. Zbog tog razloga trebalo je napraviti novu definiciju koja bi odražavala specifičnost područja primene upravljanja sistemima i sigurnošću.
- Analiza složene strukture bila je na veoma teškom testu, jer je bilo potrebno zaštititi prenos podataka i informacija koji se svakodnevno skupljaju sa servera iz glavnih apoteka celog Pčinjskog regiona na glavnom serveru koji se nalazi u Vranju, a istovremeno ne iscrpljivati memorijske kapacitete koji bi mogli dovesti do zagušenja.
- Tek kada je primenjena kombinacija softvera navedenog u radu došlo se do „programskog paketa“ koji u razumnom vremenu daje tražene rezultate

Jednom potvrđene hipoteze i modeli još su bili daleko od cilja kompletnog projekta. Sve skupa moralo je proći kroz oštre zakonske i druge normativne filtere sa posebnim osvrtnom da se ne iskoči iz granica koje propisuju postojeći standardi. Istovremeno, ma kako se to činilo, jednako velike a možda i najveće poteškoće bile su potpuno odsustvo zakona, standarda, preporuke i najbolje prakse.

5. ZAKLJUČCI

1. Samo prepoznavanje i ocena rizika je prva faza za glavnu namenu rada koji se bavi rizicima: radi se o mogućem smanjivanju na nivo koji odgovara politici upravljanja rizicima organizacije bez obzira da li je reč o proizvodnji ili pružanju usluga, industriji, javnim funkcijama, prosveti, administraciji ili poljoprivredi. Sve ove aktivnosti daju saznanja koja su praktično uvek od neprocenjive vrednosti za donošenje odluka bilo kog menadžmenta na bilo kojem hijerarhijskom nivou.
2. Postoje četiri osnovna načina obrade rizika :
 - Prihvatanje postojećeg rizika
 - Smanjenje na prihvatljiv nivo
 - Izbegavanje hazardne situacije
 - Prenosjenjem na treće

Van ovih načina standardi ne poznaju ni jednu drugu primenjivu metodu ili tehniku.

3. Dobijeni rezultati pokazuju da je obrada rizika a time i upravljanje njima moguća ne samo na četiri klasična načina već i kroz novi, peti: izmenama u strukturi sistema
4. Rezultati celog navedenog višegodišnjeg rada doveli su do stvaranja odgovarajućih hipoteza koje su se morale dokazati i koje su testirane na postojećem realnom sistemu. Pri tome se celokupno istraživanje strogo držalo oficijelnih definicija i direktiva datih kroz usvojene međunarodne standarde i rešenja najbolje prakse.
5. Mrežna infrastruktura igra veoma važnu ulogu u zaštiti kompletne računarske mreže pa i u zaštiti mail servera, zato što je to prva linija odbrane između Interneta i mail servera. Kakva će biti mrežna infrastruktura koja podržava mail server zavisi ne samo od potrebe za zaštitom već i od materijalnih mogućnosti organizacije (u ovom slučaju ZU Apoteka Vranje), potrebnih performansi i pouzdanosti sistema. Mrežna infrastruktura ne može sama zaštititi mail server, jer frekvencija, sofisticiranost i različitost današnjih „napada“ na mail sisteme utiču na to da zaštita mora biti implementirana na različitim segmentima sistema i na različitim slojevima familije Internet protokola. Sprovođenjem zaštite mail servera, na nivou mrežne infrastrukture smanjuje se mogućnost neželjenih upada u sistem a time se povećava dostupnost podataka na mail serveru. Zaštitom na mrežnom nivou mail server nije zaštićen od napada na SMTP, POP3 i IMAP aplikacije, neželjene pošte (*spam-a*) i virusa. Zaštita mail servera je neprestan proces koji zahteva konstantno prisustvo truda, sredstava i budnosti.
6. Novi tipovi pretnji za web aplikacije zasnovane na virtuelizaciji klijentske i serverske strane otvaraju nove tipove napada na web aplikacije i zahtevaju novu paradigmu zaštite informacione imovine poslovnih sistema. Organizacije, pa i ZU Apoteka Vranje, često imaju pogrešnu predstavu da tradicionalne kontrole zaštite krajnjih tačaka poslovnog IS pružaju adekvatnu zaštitu od web zasnovanih pretnji. Modeli napada se menjaju, uključujući načine prenosa i infekcije malicioznim programima i postaju sve sofisticiraniji. Web napade je sve teže zaustaviti, a posledice postaju sve ozbiljnije. Tradicionalna zaštita je još uvek važna, ali ne može potpuno zaustaviti nove web napade, jer nije usmerena na prave objekte. Potrebne su nove kontrole zaštite. Zaštita web servisa i aplikacija mora se proširiti na ponašanje korisnika, kao i na zaštitu računarskih programa i konfiguracija. Metode zaštite moraju se stalno usavršavati i redovno testirati postojeći sistem zaštite.
7. Skeneri zaštite integriteta računarskih mreža po konceptu su slični skenerima zaštite računarskih sistema, s tim da se otkrivaju ranjivosti računarske mreže. Arhitektura skenera ranjivosti računarske mreže uključuje *modul za skeniranje, bazu podataka sa definicijama poznatih ranjivosti, modul za generisanje i prezentaciju izveštaja i*

korisnički interfejs. Modul za skeniranje implementira politiku zaštite, koja omogućava prilagođavanje procesa skeniranja zahtevima okruženja, skenira računarsku mrežu, otkriva i poredi tekuće ranjivosti sa poznatim iz baze podataka i daje podatke na izlazu. Rezultati se prikazuju preko korisničkog interfejsa za izveštavanje. Analitičar zaštite ili menadžer, na osnovu ovih rezultata, mogu brzo proceniti podložnost poznatim bezbednosnim ranjivostima.

8. Skeneri telefonskih veza su komercijalni razvoj hakerskih alata tzv. *war dialing* programa, koji se koriste za identifikovanje potencijalnih ranjivosti sistema preko telefonske linije. Konceptualno su sasvim slični skenerima ranjivosti računarskih mreža; biraju seriju telefonskih brojeva, vrše određeni broj bezbednosnih provera, izveštavaju o rezultatima i na taj način prave bezbednosnu mapu telefonskog sistema organizacije, dok skeneri ranjivosti računarske mreže mapiranjem IP adresa prave mapu uređaja lokalne mreže. Telefonski skeneri detektuju ranjive puteve u računarskoj mreži organizacije koji su pristupačni sa javne telefonske mreže (PSTN). Posebno oni detektuju neovlašćene i nepoznate modeme prisutne na LAN-u i koji mogu prihvatiti dolazne pozive. Principi rada telefonskih skenera zasnivaju se na kombinaciji tehnika probe (pingovanja) i prepoznavanja zahteva za izveštavanje (prompts) o ranjivostima na nivou operativnog sistema i na nivou aplikacija (npr. udaljeni pristup sistemu bez pasvorda). Ovu vrstu skenera ZU Apoteka Vranje nema, tako da ostaje kao predlog radi poboljšanja zaštite računarske mreže u okviru organizacije.
9. Detektori upada u računarski sistem – IDS (*Intrusion Detection Systems*) koriste se za prepoznavanje indikacija nekog pokušaja upada i da upozore korisnika ili izvrše korektivne akcije. Savremeni koncept IPS (*Intrusion Prevention Systems*) sistema omogućava, pored funkcija IDS, određene vrste inteligentnih zamki za napadača (tipa čupa meda – *hony pot*), kojima skreću njihovu pažnju i izučavaju osobenosti u cilju preventivne zaštite od sledećeg napada.
10. Planiranje vanrednog događaja i nastavljajanja poslovanja najsloženiji je deo posla. Kada organizacija odluči kako će nastaviti poslovanje, primena plana je tada relativno lak zadatak. Proces planiranja vanrednih događaja odvija se u šest faza.
11. U cilju autentifikacije ovlašćenih korisnika ZU Apoteka Vranje za pristup sistemu koriste se korisničko ime i lozinka koji su jedinstveni za pristup bazi i na osnovu kojih je za svakog korisnika definisano koja prava ima i kojim podacima može da pristupi. Mehanizmi zaštite u okviru Telekom Srbija baziraju se na X.509 standardnim digitalnim sertifikatima koje izdaje odgovarajuće sertifikaciono telo. U okviru Telekom Srbija i korisnika ZU Apoteka Vranje moguća je realizacija sopstvenog CA u okviru Telekom Srbija, za potrebe izdavanja digitalnih sertifikata ovlašćenih učesnika u sistemu.

6. PREGLED POSTIGNUTIH REZULTATA

1. ZU Apoteka Vranje je pre neku godinu imala havariju na serverima prilikom kojih je došlo do delimičnog gubitka podataka i tek tada je menadžment utvrdio potrebu i značaj *back-upa*. Iz tog razloga trenutno se vode pregovori oko pružanja poverenja iStor DataVault sistemu koji predstavlja novinu na našem informatičkom tržištu. iStor DataVault je sistem za sigurno čuvanje kritičnih podataka na udaljenoj lokaciji. Podaci sa servera su enkriptovani i kopirani na iStor sigurne data centre koji su raspoloživi 24 časa dnevno. iStor DataVault je dizajniran za najviši nivo sigurnosti i dostupnosti. Omogućava izuzetno napredne funkcije optimizovane za sigurno bekapovanje i povraćaj podataka, u skladu sa svim zakonskim regulativama. iStor DataVault obezbeđuje sve vidove zaštite podataka, od automatskog izvršavanja i šifriranja, prenosa podataka na udaljene loakcije i brzog oporavka podataka.
2. Još jedan način poboljšanja zaštite računarske mreže koji nema ZU Apoteka Vranje i koji je u ovom radu dat kao predlog je virtualizovano računarsko okruženje. Virtualizovana računarska okruženja mogu se jednostavno povezati sa realnim računarskim okruženjem organizacije, u ovom slučaju ZU Apoteka Vranje. Ova karakteristika je veoma značajna jer omogućava migriranje napada sa realnog na virtualno računarsko okruženje. Tačka u kojoj će se migracija izvršiti trebala bi da bude *firewall* sistem kroz koji napadač pokušava da pristupi realnom okruženju organizacije. Odluka o preusmeravanju napadača u virtualno okruženje samo je posledica uspešnog prepoznavanja da je u pitanju napad a ne regularan mrežni saobraćaj. Ona se može doneti na osnovu zaključka IDS/IPS sistema ali su mogući i jednostavniji koncepti. U situaciji ZU Apoteka Vranje gde imamo rad sa protokolima namenjenim za udaljenu administraciju računara (*Remote Desktop*, SSH i sl.) veoma lako se mogu dovesti u sumnju zahtevi za ove i druge protokole koji se izvršavaju na serveru u realnoj internoj mreži organizacije. S druge strane, u opisanoj situaciji i zahtevi pod HTTP protokolom mogu se preusmeriti u virtualizovano računarsko okruženje, i to upravo ka virtualizovanim instancama web servera na kojima su namerno napravljeni bezbednosni propusti (koji odgovaraju identifikovanim tipovima napada) sa svrhom da prikupljaju podatke o cilju, izvoru i karakteristikama napada. Uspešno prepoznavanje napada i preusmeravanje napadača u virtualno okruženje predstavlja izolovanje potencijalne faze incidenta.
3. Još jedna aplikacija koju ZU Apoteka Vranje ne koristi a koji bi se mogao koristiti kao dodatni alat u povremenom proveravanju bezbednosnih ranjivosti računara u mreži je *fuzzing* tehnika. Analiza i testiranje sigurnosti programske podrške vrlo je važan proces kojim je moguće pravovremeno uočiti i otkloniti sigurnosne propuste u računarskom sistemu. *Fuzzing* tehnika i metoda otkrivanja sigurnosnih propusta, analizirana u radu, može se primeniti na bilo kojoj aplikaciji čija je sigurnost ključna za pouzdano i nesmetano izvršavanje određenih zadataka. Ipak, iako je jednostavna i sa veoma dobrim rezultatima, korišćenje ove tehnike zahteva određeni nivo znanja i iskustva osobe koja sprovodi ovu analizu. *Fuzzing* metoda prvenstveno se odlikuje svojom jednostavnošću i efikasnošću kao i mogućnosti automatizacije što znatno ubrzava postupak otkrivanja bezbednosnih ranjivosti. Metoda je pogodna za veliki broj različitih programskih rešenja i proizvoda i samim tim može se koristiti kao dodatni alat u povremenom proveravanju bezbednosnih ranjivosti računara u mreži ZU Apoteka Vranje.
4. Sve što je predloženo u radu kao neki vid rešenja sasvim zadovoljava sve kriterijume kompatibilnosti sa poslovno-informacionim sistemom *Hubi-e* čime se omogućava njegov nesmetan rad, a to je ono što je neophodno za rad kompletne ustanove. Samim

tim, dolazimo do zaključka da svaka nekompatibilnost sa navedenim sistemom dovodi u pitanje rad poslovno-informacionog sistema *Hubi-e* čime je svako dalje razmatranje po tom pitanju bezpredmetno, jer osnovna i polazna tačka za ceo ovaj rad bila je zaštita navedenog sistema a samim tim i rad celokupne ZU Apoteka Vranje.

7. PRILOZI

PRILOG br. 1



POSLOVNI SISTEM **ZU APOTEKA VRANJE**

Periodični poslovi unutar poslovnog sistema

Biling: se izvršava svakog drugog meseca, i traje od petnaestog do kraja meseca. Ceo proces se izvršava kao pozadinski posao i potpuno se automatizovano izvršava posle zadavanja parametara i puštanja u rad.

Fakturisanje: se obavlja svakog petog u mesecu i traje dva-tri dana. Način izvršavanja procesa fakturisanja definisan je uslovima koje izdaje RFZO. Nakon zadavanja početnih parametara i pokretanja datog procesa u rad, celokupno fakturisanje nastavlja da se izvršava kao pozadinski posao na SAP sistemu.

Izvoz i štampa, faktura: Nakon završenog procesa fakturisanja, potrebno je uraditi eksport faktura i recepata. Eksport se obavlja iz SAP-a. Sve fakture za dati period izvoze se na fajl sistem SAP aplikativnog servera u obliku tekstualnih fajlova. Posle obrade fajlova pomoću *shell* skripti i Hubi-e programa, koji je specijalno prilagođen za obradu tih podataka, pristupa se generisanju PDF fajlova koji služe za kontrolu ispravnosti celog procesa. Nakon što se utvrdi da su fakture pravilno kreirane, pristupa se masovnoj štampi.

Backup procedura

Centralni deo *backup* sistema predstavlja iStor Secure Data Value. *Backup* podataka vrši se svaki dan za produkcione servere. Ciklusi *backup*-a se smenjuju na taj način, da su u svakom trenutku dostupne tri smaknute kopije podataka, od kojih je svaka prethodna starija za jedan dan. Osim što u svakom trenutku postoje tri smaknute kopije podataka, najstarija od kopija smešta se u vatrostalni sef, koji se nalazi na fizički različitoj lokaciji, od one na kojoj su smešteni serveri i *backup* sistem. Sef se nalazi na određenoj lokaciji, a zamena traka se vrši dva puta u nedelji od strane zaposlenih u IT sektoru.

Korporativna mreža poslovnog sistema

Centralni deo poslovnog sistema predstavljaju, SAP *database* i aplikativni serveri.

Jezgro korporativne mreže SAP poslovnog sistema, povezano je preko LAN *switch*-a sa ostalim delovima korporativne mreže.

Gradovi kao što su Vranje, Vranjska Banja, Vladičin Han, Surdulica, Bosilegrad i Preševo, povezani su sa korporativnom mrežom ZU Apoteka Vranje preko korporativne optike. Trgovište je povezano preko *Frame-Relay*-a. Jedino ovaj grad, koji je povezan preko *frame-reley*-a, komunikaciju sa SAP sistemom vrši preko SAP ruteru. SAP ruter automatski prosleđuje konekciju SAP serverima, u zavisnosti od toga koji je server izabrao korisnik. Ostali gradovi koriste Telekomovu optičku mrežu za povezivanje sa korporativnom mrežom ZU Apoteka Vranje.

SAP ruter je postavljen kao most, između korisnika koji su sa korporativnom mrežom povezani preko *Frame-Relay*-a, i poslovnog SAP sistema. Na samom SAP ruteru, postoje dve LAN mrežne konekcije, od kojih je jedna sa javnom IP adresom. Operativni sistem SAP ruteru je Windows XP Professional sa instaliranim *Sygate personal firewall*-om. Pristup preko *remote* desktop-a nije omogućen.

Ukoliko dođe do potrebe za intervencijom na SAP serverima, od strane kompanije Telekom koja je ugovorom određena za pružanje tehničke podrške, potrebno je prvo da se o tome obaveste zaposleni u IT sektoru, kako bi se izmenile pristupne šifre na samom SAP ruteru.

LAN u poslovnim jedinicama

Korporativna mreža ZU Apoteka Vranje, geografski se prostire na 7 gradova Pčinjskog regiona. Što se tiče brojčanog stanja radnih stanica koje su rapoređene po poslovnim jedinicama ispod je kratak pregled:

Grad	Broj radnih stanica	Vrsta OS-a
Vranje	35	Win XP
Vranjska Banja	3	Win XP
Vladičin Han	5	Win XP
Surdulica	8	Win XP
Bosilegrad	6	Win XP
Preševo	3	Win XP
Trgovište	3	Win XP



PRAVILNIK O PRIMENI INFORMACIONIH TEHNOLOGIJA

UVODNE ODREDBE

Član 1.

U cilju obezbeđenja uslova za efikasno obavljanje posla i poboljšanje kvaliteta usluga, zaposleni u Zdravstvenoj ustanovi Apoteka Vranje (u daljem tekstu: ZU Apoteka Vranje), dužni su da koriste informacione tehnologije (u daljem tekstu: IT), koje obuhvataju sve hardversko-softversko-komunikacione sisteme na kojima se kreiraju, obrađuju i čuvaju poslovni podaci ZU Apoteka Vranje.

Član 2.

Svi zaposleni u ZU Apoteka Vranje, imaju obavezu da koriste IT resurse na profesionalan, moralan i zakonit način.

KORIŠĆENJE

Član 3.

Svi poslovni podaci koji su kreirani i/ili se obrađuju i pohranjuju na IT opremi ZU Apoteka Vranje, isključivo su vlasništvo ZU Apoteka Vranje.

Član 4.

Nesmetan i permanentan pristup svim podacima na radnoj stanici zaposlenog, uključujući tu i celokupnu elektronsku poštu, pored zaposlenog, u cilju nadzora, može vršiti i neposredni rukovodilac zaposlenog. U slučaju odsutnosti neposrednog rukovodioca zaposlenog, pristup podacima može biti omogućen, na osnovu odluke direktora ili pomoćnika direktora, i drugim rukovodiocima iznad u hijerarhijskom nizu.

Član 5.

U slučaju otkrivanja zloupotrebe korišćenja IT resursa ZU Apoteka Vranje, ugrožavanja bezbednosti podataka ZU Apoteka Vranje ili poslovanja ZU Apoteka Vranje, IT služba je ovlašćena da bez upozorenja delimično ili potpuno, privremeno ili trajno, isključi radnu stanicu zaposlenog iz računarske mreže ZU Apoteka Vranje, za kojeg se utvrdi, ili za kojeg postoji osnovana sumnja da preko nje vrši zloupotrebu, ili da postoji opasnost po podatke, ili poslovanje ZU Apoteka Vranje, i da protiv zaposlenog, pokrene odgovarajući postupak.

ZLOUPOTREBE

Član 6.

IT ZU Apoteka Vranje se ne mogu koristiti za neovlašćeno i svojevolsno slanje, primanje i/ili skladištenje bilo kakvih podataka, dokumenata i datoteka koji:

- otkrivaju poslovnu tajnu ili lične podatke korisnika usluga ZU Apoteka Vranje, osim u svrhe obavljanja radnih dužnosti, i/ili koji mogu da nanesu bilo kakvu materijalnu ili nematerijalnu štetu ZU Apoteka Vranje
- diskriminišu ili zlostavljaju
- pogrđni su u odnosu na bilo kog pojedinca ili grupu
- obsceni su, seksualno eksplicitni ili pornografski
- klevetnički su ili zastrašujući prema bilo kome
- u suprotnosti su sa licencom za korišćenje bilo kog softvera
- koriste se u svrhe koje su protivzakonite, ili su u suprotnosti sa ovim Pravilnikom i drugim aktima ZU Apoteka Vranje, ili poslovnim interesima ZU Apoteka Vranje.

Zaposlenom koji zloupotrebljava ovlašćenja u primeni IT ZU Apoteka Vranje i koji se ne pridržava odredbi iz ovog Pravilnika može usled ovakvog ponašanja prestati radni odnos i/ili biti pokrenut drugi odgovarajući postupak.

PROVERA I NADZOR

Član 7.

Po pravilu, podaci u elektronskoj formi koji se prosleđuju i/ili skladište od strane zaposlenog, preko e-pošte, procesora za obradu teksta, tabela, crteža i dr., pomoćnih programa, ne nadgledaju se od strane ZU Apoteka Vranje.

Član 8.

U cilju provere načina korišćenja IT-a, ZU Apoteka Vranje periodično skuplja dnevnik događaja (logove) elektronskih komunikacija.

ZU Apoteka Vranje može da preuzima mere nadzora nad korišćenjem IT resursa, a u svrhe:

- analiziranja troškova,
- raspodele resursa,
- optimalnog tehničkog upravljanja IT resursima,
- otkrivanja šablona koji mogu da ukažu da pojedini zaposleni, krše odredbe ovog Pravilnika i/ili druge akte ZU Apoteka Vranje ili se bave nezakonitim radnjama.

Član 9.

ZU Apoteka Vranje ne odgovara za privatne dokumente i datoteke koje zaposleni prima, upotrebljava i/ili smesta na IT opremi ZU Apoteka Vranje i isti se, u slučaju opterećenja ili stvaranja manjka resursa mogu otkloniti od strane IT službe.

ZU Apoteka Vranje zadržava pravo da, po sopstvenoj diskreciji, izvrši reviziju bilo kog elektronskog podatka i/ili poruke, odnosno fajla u kome su ti podaci zabeleženi, bilo da se nalaze na serverima, ili na radnim stanicama, do one mere, do koje je neophodno obezbediti da se IT i servisi ZU Apoteka Vranje koriste u skladu sa zakonom, ovim Pravilnikom i drugim aktima ZU Apoteke Vranje.

Član 10.

Zaposleni ne smeju samostalno preduzimati nikakve mere i aktivnosti da primenom IT ZU Apoteka Vranje šifriraju podatke. Zaposleni mogu da koriste mehanizme za šifriranje koji su im omogućeni isključivo od strane IT podrške za svrhu zaštite osetljivih i/ili poverljivih informacija. Ovi zaposleni, dužni su da omoguće mehanizme za pristup takvim podacima ovlašćenim licima IT službe i svom neposrednom rukovodiocu.

Zaposleni pristupaju od IT službe unapred određenim resursima i servisima korišćenjem dodeljenog korisničkog naloga. Otkrivanje dodeljenog korisničkog naloga i bilo kojih mehanizama njegove zaštite (lozinka, ključ za šifriranje i dr.) bilo kom drugom licu predstavlja povredu radne obaveze i povlači odgovornost zaposlenog, izuzev u slučaju kada je ovakvo okrivljanje odobreno od strane neposrednog rukovodioca, u cilju hitnog obavljanja radnog zadatka.

Korišćenje, ili pokušaj korišćenja tuđeg korisničkog naloga predstavlja, povredu radne obaveze i povlači odgovornost zaposlenog, sa izuzetkom iz prethodnog stava.

UPOTREBA SOFTVERA

Član 11.

U cilju sprečavanja širenja „zlonamernog“ koda preko IT ZU Apoteka Vranje, zabranjeno je preuzimanje (*download*) bilo kakvog softvera sa Interneta. Isključivo softver koji je registrovan i odobren od strane ZU Apoteka Vranje, može biti instaliran na IT sistemima i opremi ZU Apoteka Vranje.

Softver u IT-u ZU Apoteka Vranje može da bude preinstaliran od strane proizvođača ili isporučioća opreme, a kasnije instaliranje softvera je dozvoljeno samo ovlašćenim zaposlenima IT službe, daljinski, ili neposredno na samim radnim stanicama, ili ovlašćenim licima isporučioća softvera uz prisustvo i nadzor ovlašćenih lica iz IT službe.

Član 12.

Demonstracioni softveri koji se nalaze na reklamnim prenosnim medijumima (CD, DVD, *FlashDisk*, eksterni HDD i sl.), pregledaju se i testiraju od strane ovlašćenih lica iz IT službe i postavljaju na Intranet sajt kako bi bili dostupni zaposlenima.

Reklamni sadržaji na prenosnim medijumima sa tzv. "pasivnim sadržajem", koji ne zahtevaju instalaciju na lokalnom ili mrežnom hard disku, odnosno koji za pokretanje i prikaz na radnoj stanici ne zahtevaju administratorska ovlašćenja, mogu se pokretati od strane zaposlenih.

Član 13.

Skup raspoloživih aplikativnih softvera koji koristi zaposleni definisan je konkretnim radnim mestom na koje je zaposleni raspoređen. Promenom radnog mesta menja se i grupa raspoloživih softvera.

Zaposleni su dužni da, u odnosu na radne potrebe, kontaktiraju korisnički servis IT službe i, uz odobrenje svog nadležnog rukovodioca, zatraže korišćenje, ili instaliranje na radnim stanicama na kojima rade, pojedinačnog softvera, ili dodelu bilo kog prava za koje smatraju da su im neophodni za obavljanje posla, a nisu definisani profilom njihovog radnog mesta.

Član 14.

Korisnici IT ZU Apoteka Vranje dužni su da poštuju poverljivost IT-a i servisa drugih lica u i/ili izvan ZU Apoteka Vranje. Bez odobrenja od strane nadležnog rukovodioca, zaposlenima se zabranjuje da se bave:

- ✓ nadgledanjem ili presretanjem fajlova ili elektronskih komunikacija zaposlenih ili trećih lica;
- ✓ hakerisanjem ili pristupanjem sistemima i/ili nalogima za koje nemaju ovlašćenja za upotrebu;
- ✓ korišćenjem tuđih naloga, lozinki ili sredstava za primenu IT;
- ✓ probijanjem, testiranjem ili nadgledanjem računarskih i/ili mrežnih bezbednosnih mera,
- ✓ unošenjem „zlomernog“ koda u informacioni sistem.

Član 15.

U cilju obavljanja radnih dužnosti zaposlenom se dodeljuje na korišćenje službena elektronska adresa koja sadrži sufiks@open.telekom.rs. Korišćenje ove adrese nije dozvoljeno u privatne svrhe.

Nisu dozvoljene elektronske poruke, ili drugi elektronski podaci, koji se šalju uz sakrivanje identiteta pošiljaoca, ili se njima pošiljalac predstavlja kao neko drugi.

Zabranjeno je korišćenje P2P programa, kao i „Internet Chat Messenger“ aplikacija, izuzev onih koji su određeni od strane IT službe kao IT resursa za zaposlene.

Zaposleni su dužni da IT ZU Apoteka Vranje, uključujući tu i servise računarske mreže ZU Apoteka Vranje, koriste na način koji neće da proizvede zagušenje računarske mreže, IT resursa i IT servisa, niti da značajno umanju mogućnosti drugim korisnicima IT ZU Apoteka Vranje da pristupe i/ili koriste IT resurse i servise u IT mreži.

Član 16.

Pristup IT resursima i podacima drugog zaposlenog, u cilju pregleda, kopiranja, korišćenja, prepravljanja i/ili prosleđivanja podataka, vrši se isključivo uz odobrenje nadležnog rukovodioca ili na osnovu sudske naredbe javnog tužioca u cilju sprovođenja postupka.

PRELAZNE I ZAVRŠNE ODREDBE

Član 17.

Zaposleni se, prilikom zasnivanja radnog odnosa, upoznaje sa odredbama ovog Pravilnika i daje Izjavu o prihvatanju pravila određenih ovim Pravilnikom.

Zaposleni koji su zasnovali radni odnos pre donošenja ovog Pravilnika, isto su dužni da potpišu Izjavu iz prethodnog stava.

Član 18.

Ovaj Pravilnik stupa na snagu danom donošenja od kada se i primenjuje.

ZU Apoteka Vranje



ZU APOTEKA VRANJE

DIREKCIJA:

Objekat:

Broj:

Na osnovu člana 17. Pravilnika o primeni informacionih tehnologija u Zdravstvenoj ustanovi Apoteka Vranje, (u daljem tekstu: ZU Apoteka Vranje), zaposleni daje sledeću

I Z J A V U

Pročitao sam, razumeo, i prihvatom pravila i uslove iz „Pravilnika o primeni informacionih tehnologija“ ZU Apoteka Vranje koji reguliše korišćenje IT-a i IT servisa ZU Apoteka Vranje.

Svestan sam da nepridržavanje ovih pravila predstavlja povredu radne obaveze usled koje mi može prestati radni odnos i/ili od strane ZU Apoteka Vranje biti pokrenut drugi odgovarajući postupak.

Takođe, ovom Izjavom prihvatom da po predočenju od strane ZU Apoteka Vranje izmena i dopuna ovog Pravilnika, iste odmah primenjujem.

Datum:

<i>Ime i prezime</i>	<i>JMBG</i>	<i>Korisnički nalog</i>	<i>Potpis</i>

PRILOG br. 3



Datum: _____ godine
Ukupno strana: 4

**Pravilnik
o autorizacijama ,dostupnosti informacijama i izveštajima u
SAP-u u Zdravstvenoj ustanovi Apoteka Vranje
Vranje**



Pravilnik o autorizacijama ,dostupnosti informacijama i izveštajima u SAP-u u Zdravstvenoj ustanovi Apoteka Vranje Vranje

I - Opšte odredbe

Član 1.

Ovim Pravilnikom se u Zdravstvenoj ustanovi Apoteka Vranje u Vranju (u daljem tekstu: ZU Apoteka Vranje) utvrđuju načini dodeljivanja autorizacija za upotrebu programskog sistema SAP na produkcijskom klijentu, kao i dostupnost autorizovanih lica informacijama i izrađenim izveštajima.

II – Autorizacija i dostupnost informacijama

Član 2.

Na dan donošenja ovog Pravilnika utvrđuje se da su ovlašćene osobe za inicijalno podnošenje autorizacija Direktor ustanove i rukovodilac IT sektora. Za dalju upotrebu programskog sistema SAP moguće je da se zaposlenima:

- **dodeli autorizacija** (u slučaju da se otvara novo radno mesto u postojećoj organizacijskoj formaciji ili dolazi novi zaposleni na već postojeće radno mesto)
- **proširi polje autorizacije** (u slučaju da se zaposlenom koji već koristi SAP poveća i proširi obim radnih zadataka ili ukoliko dođe do unapređenja zaposlenog)
- **suzi polje autorizacije** (u slučaju da se zaposlenom koji već koristi SAP smanji i suzi obim radnih zadataka)
- **oduzme autorizaciju i u potpunosti zabrani pristup sistemu** (prelazak zaposlenog na radno mesto za koje nije potrebno upotrebljavati SAP ili odlazak zaposlenog iz ustanove)

Da bi zaposlenom bila odobrena bilo koja od opcija navedenih u prethodnom stavu ovog člana neophodno je da neposredno nadređeni zaposlenog, tj. **DIREKTOR USTANOVE**, podnese zahtev za autorizaciju koji čini sastavni deo ovog pravilnika.

III – Zahtev za autorizaciju

Član 3.

Zahtev za autorizaciju se podnosi na taj način što ovlašćeni podnosilac popunjava lične podatke zaposlenog, radno mesto na kojem radi, i zaokružuje opciju svog zahteva koju potom i tekstualno obrazlaže.

Član 4.

Ključni korisnik

Predmetni zahtev se potom šalje ključnom korisniku imenovanom ovim pravilnikom. Ključni korisnik će predložiti da li je zaposlenom neophodno dodeliti, proširiti, ograničiti ili oduzeti autorizaciju.

Kada primi zahtev za autorizaciju ključni korisnik se na isti izjašnjava tako što daje svoje mišljenje o zahtevu i navodi obim ili nabraja transakcije u kojima se navedena ovlašćenja odobravaju ili sužavaju, kao i međusobne veze sa drugim modulima. Preporučljivo je da svoj komentar ključni korisnik detaljno obrazloži.

Član 5.

Rukovodilac IT sektora

Popunjen zahtev ključni korisnik prosleđuje rukovodiocu IT sektora koji na isti daje svoje odobrenje ili odbija zahtev sa eventualnim komentarima.

Zahtev potpisan i pregledan od strane svih odgovornih lica dostavlja se IT Sektoru koji će potvrditi prijem i isti sprovesti u delo, u roku ne dužem od 3 dana, osim zahteva kojim se traži zabrana autorizacije po kojem je IT Sektor dužan da postupi u roku od 1 radnog dana.

IV – Zahtev za autorizaciju SAP *all*

Član 6.

Zahtev za autorizaciju SAP *all*, podnosi se na istom zahtevu kao i prethodni s tim da jedine ovlašćene osobe za podnošenje ovog zahteva su Direktor i Pomoćnik direktora. Zahtev se po potpisivanju od strane ovlašćenih osoba odmah dostavlja IT Sektoru koji isti izvršava u roku od 1 radnog dana.

V – Izveštavanje

Član 7.

U skladu sa autorizacijama koje su zaposlenom date isti je u mogućnosti da prima i da se upoznaje sa informacijama iz obima svoje autorizacije.

Izveštaji se u SAP-u dele na : **taktičke** i **strateške**.

U skladu sa datom autorizacijom zaposleni može da izradi bilo koju vrstu taktičkog izveštaja iz obima primljene autorizacije, a čiji elementi mogu biti informacije dostupne samo uz tu autorizaciju.

U slučaju da postoji potreba za uvidom u već izrađen strateški izveštaj ili pak za izradom takvog izveštaja, koji bi sadržao informacije iz više modula neophodno je da se tada podnese zahtev za izradu izveštaja.

Član 8.

Zahtev za izradu izveštaja sa podnosi na taj način što ovlašćeni podnosilac (**DIREKTOR USTANOVE**) predleže da se izradi određeni izveštaj i obrazlaže svoj zahtev.

Član 9.

Ključni korisnik

Predmetni zahtev se potom šalje ključnom korisniku koji daje svoje mišljenje o osnovanosti zahteva sa obrazloženjem načina izrade izveštaja, kao i to da li je eventualno

potrebno povezivanje sa nekim drugim modulom ili osnovanost/neosnovanost uvida u već izrađeni izveštaj.

Preporučljivo je da svoj komentar ključni korisnik detaljno obrazloži.

Član 10.

Rukovodilac IT sektora

Popunjen zahtev za izradu izveštaja ključni korisnik dalje prosleđuje rukovodiocu IT sektora koji na isti daje svoj sud.

Zahtev potpisan i pregledan od strane svih odgovornih lica dostavlja se Pomoćniku direktora koji je jedini ovlašćen da odobri pristup informacijama.

Samo u slučaju da Pomoćnik direktora da odobrenje za izradu predmetnog izveštaja kao i to da određene informacije postanu dostupne zaposlenom, takav odobreni predlog se dostavlja IT Sektoru koji će dati mišljenje o izvodljivosti kao i primeren rok u kojem je moguće izraditi predmetni izveštaj.

VI – Izmena lozinke korisnika

Član 11.

Postoji mogućnost da se od strane ovlašćenog lica podnese Zahtev za izmenu lozinke korisnika u slučaju promene zaposlenog.

Tada ovlašćeni podnosilac podnosi zahtev IT Sektoru, koji samo na podnetom zahtevu konstatuje da je isti izvršen, rok za postupanje po zahtevu za IT sektor iznosi 1 radni dan.

Član 12.

Popunjeni zahtevi sa potpisima svih ovlašćenih lica arhiviraju se u Pravnoj službi.

Član 13.

Ovaj Pravilnik stupa na snagu danom njegovog donošenja od kada se i primenjuje.

PRILOG br. 4



**ODLUKA O KORIŠĆENJU ADMINISTRATIVNIH
PRIVILEGIJA NA RAČUNARU**

- I.** Usled specifičnosti pojedinih radnih mesta i poslova koji podrazumevaju rad sa određenim softverima i aplikacijama, čija operativnost i funkcionalnost zavise od administrativnih privilegija nad operativnim sistemom računara, pojedinim zaposlenima u ZU Apoteka Vranje biće omogućene jedna ili više administrativnih privilegija na računaru.
- II.** Zahtev za dodeljivanjem administrativnih privilegija zaposlenom podnosi se uz pisanu saglasnost nadležnog rukovodioca. Zahtev se dostavlja IT službi ZU Apoteka Vranje koja proverava postojanje tehničkih mogućnosti, a odluku o dodeljivanju administrativnih privilegija donosi Direktor ustanove.
- III.** Administrativne privilegije mogu se odnositi na mogućnost instaliranja i deinstaliranja softvera na računaru, kao i na vršenje drugih sistemskih promena nad operativnim sistemom računara. Odobrene administratorske privilegije, zaposleni može da koristi isključivo za potrebe posla opisane u zahtevu za dodeljivanje administratorskih privilegija.
- IV.** Zaposleni kome se dodele administrativne privilegije nad računarom, dužan je da se, pored odredbi „Pravilnika za primenu Informacionih tehnologija“ ZU Apoteka Vranje, pridržava i sledećih dodatnih pravila:
 - Zaposleni ne sme da instalira nikakav dodatni softver na računar, bez prethodne konsultacije i odobrenja od strane nadležnih lica iz IT službe.
 - Zaposleni je dužan da koristi softver u skladu sa licencnim ugovorom koji je ZU Apoteka Vranje zaključila sa proizvođačem i/ili distributerom softvera.
 - Zaposleni ne sme da *upload*-uje ili *download*-uje nelegalan sadžaj na Internet odnosno sa Interneta, niti da na računaru instalira, postavlja, pohranjuje, koristi unutar korporativne mreže, distribuira ili reprodukuje softver, odnosno druga autorska dela ili drugi predmet srodnog prava, za koja ZU Apoteka Vranje nije obezbedila licencu, odnosno nije na drugi način regulisao autorska i druga srodna prava.
- V.** Zaposlenom koji zloupotrebljava odobrene administrativne privilegije i koji se ne pridržava ove Odluke, može usled ovakvog ponašanja prestati radni odnos i/ili biti pokrenut drugi odgovarajući postupak.
- VI.** VI Ova Odluka stupa na snagu dana_____. godine, od kada se i primenjuje.

ZU Apoteka Vranje

Direktor



ZU Apoteka Vranje

DIREKCIJA:

Objekat:

Broj:

Saglasno Odluci ZU Apoteka Vranje o korišćenju administrativnih privilegija na računaru, zaposleni daje sledeću

IZJAVU

Pročitao sam, razumeo, i prihvatom pravila i uslove koji regulišu korišćenje administrativnih privilegija na računaru ZU Apoteka Vranje.

Svestan sam da nepridržavanje ovih pravila predstavlja povredu radne obaveze usled koje mi može prestati radni odnos i/ili od strane ZU Apoteka Vranje biti pokrenut drugi odgovarajući postupak.

Takođe, ovom Izjavom prihvatom da po predočenju od strane ZU Apoteka Vranje izmena i dopuna ove Odluke, iste odmah primenjujem.

Datum:

<i>Ime i prezime</i>	<i>JMBG</i>	<i>Korisnički nalog</i>	<i>Potpis</i>



Pravilo o formatu lozinke (Password Policy)

Usled poboljšanja sigurnosti LAN (Lokalne mreže) donešeno je i pravilo o formatu lozinke koje će se primenjivati u buduću na svim radnim stanicama koje pripadaju Apoteka Vranje LAN mreži.

Svim zaposlenim u ZU Apoteka Vranje:

Jednostavne i prazne lozinke predstavljaju preveliki rizik i u mnogome olakšavaju "upade" u vašu korporativnu mrežu. Lozinke koje su u opticaju jednu ili više godina, ili lozinke koje se često ponavljaju takođe olakšavaju upade u korporativnu mrežu i time se dovodi u pitanje privatnost važnih podataka!

U cilju povećanja zaštite vaših korisničkih naloga u lokalnoj mreži, od Vas će se u buduću zahtevati da koristite "jake" lozinke kada pristupate korporativnom računarskom sistemu. Takođe je Vaša dužnost kao zaposlenog da Vašu lozinku menjate periodično, kao i da prilikom promene lozinke ne koristite lozinku koja se podudara sa prethodno korišćenom.

Jaka lozinka se sastoji od najmanje šest karaktera i mora da sadrži karaktere iz najmanje tri od pet, dole navedenih grupa :

Grupa	Primer
Mala slova	a,b,c ...
Velika slova	A,B,C ...
Brojevi	1,2,3 ...
Simboli	() ` ~ ! @ # \$ % ^ & * - + = \ { } [] : ; " ' < > , . ? /
Unikod karakteri	€, Γ, f, i λ

Vaše lozinke će imati mogućnost da sadrže najviše tri uzastopna slova iz vašeg korisničkog imena. Lozinke će se menjati svaka 60 dana, uz napomenu da nije dozvoljeno korišćenje starih lozinki.

Kada promenite lozinku, vaša nova lozinka će automatski biti proverena od strane sistema da bi se utvrdilo da su svi kriterijumi ispunjeni.

- Pojedincima može biti dozvoljen pristup samo onim informacijama koje su neophodne za ispunjenje njihovih svakodnevnih radnih obaveza. Pojedinci moraju dobiti odobrenje Administratora pre bilo kakvog pristupanja korporativnom IT sistemu. Ovo pravilo obuhvata zaposlene u ZU Apoteka Vranje kao i sve ostale pojedince koji su na bilo koji način dobili pravo pristupa korporativnog sistema.
- Šifre moraju biti korišćene na svim korporativnim sistemima kako bi se svaki pojedinac jednolično identifikovao na sistemu.

- Šifre nesmeju biti deljene, korišćene, ili otkrivane drugim licima. Dogovorene ili grupne šifre se nesmeju upotrebljavati.

Da bi se sprečilo slučajno pogađanje šifre omogućeno je automatsko zaključavanje sistema pomoću koga se sistem zaključava posle tri neuspela pokušaja unosa lozinke. Da bi se ovakav sistem otključao potrebna je lična intervencija administratora.

Sve lozinke korisnika, čak i one kreirane privremeno za nove korisnike moraju da se kreiraju po sledećim pravilima:

- Da se sastoje od najmanje šest karaktera;
- Da budu kreirane od prethodno navedenih grupa karaktera i prema prethodno navedenim pravilima;
- Da ne budu reči iz rečnika;
- Da ne budu uzastopni nizevi brojeva ili slova (npr., abc ili 123); i
- Da se ne sastoje od jednostavnih kombinacija tastera sa tastature (npr., QWERTY)

Od korisnika se zahteva da promeni lozinku odmah prilikom inicialnog logovanja na istem.

- Lozinke će biti menjane svaka 60 dana i pri tome nije dozvoljeno korišćenje prethodne 3 lozinke.
- Korisnički nalog koji nije aktivan više od 30 dana će biti isključen. Korisnički nalog koji je isključen više od 60 dana će biti obrisani. Korisnički nalozi zaposlenih koji rade na ugovoru, moraju biti obrisani odmah nako isteka ugovora.
- Lozinke nesmeju biti korišćene u programskim kodovima, korisničkim programima i aplikacijama. Kao npr.: autoexec.bat fajlovima, e-mail klijentima, dokumentima i td.
- Šifra ne sme biti vidljiva na ekranu, kopijama podataka ili na bilo kakvom prenosivom memorijskom uređaju.
- Novi računarski sistemi koji se uvrste u korporativnu mrežu ZU Apoteka Vranje moraju prethodno biti očišćeni od eventualnih korisničkih naloga. Takođe im se prethodno moraju dodeliti nalozi koji će se koristiti u korporativnoj mreži a koji se podudaraju sa prethodno navedenim standardima.
- Administratorske lozinke se moraju promeniti odmah posle eventualne promena osoblja ili ako dođe do sumnje da je postojeća lozinka otkrivena. Takođe se ovo pravilo mora primeniti i na sve ostale korisnike korporativne mreže.

PRILOG br. 6

АПOTEКА ВРАЊЕ

Стефана Првовенчаног 43, 17500 Врање
ПИБ: 100406116, матични број: 17029851
текући рачун: 840-411661-52, 840-411667-34
тел. 017/400-730; 400 731; факс. 017/400-732
e-mail : apotekavranje@open.telekom.rs



Na osnovu člana 17. Pravilnika o primeni informacionih tehnologija u Zdravstvenoj ustanovi Apoteka Vranje u Vranju, (u daljem tekstu: ZU Apoteka Vranje), zaposleni daje sledeću

IZJAVU

Pročitao sam, razumeo, i prihvatom pravila i uslove iz Pravilnika o primeni informacionih tehnologija ZU Apoteka Vranje koji regulišu korišćenje IT-a i IT servisa ZU Apoteka Vranje.

Svestan sam da nepridržavanje ovih pravila predstavlja povredu radne obaveze zbog koje ZU Apoteka Vranje može pokrenuti odgovarajući postupak.

Takođe, ovom Izjavom prihvatom da po predocenju od strane ZU Apoteka Vranje izmena i dopuna ovog Pravilnika, iste odmah primenjujem.

Datum:

<i>Ime i prezime</i>	<i>JMBG</i>	<i>Korisnički nalog</i>	<i>Potpis</i>

PRILOG br. 7

АПOTEKA ВРАЊЕ

Стефана Првовенчаног 43, 17500 Врање
ПИБ: 100406116, матични број: 17029851
текући рачун: 840-411661-52, 840-411667-34
тел. 017/400-730; 400 731; факс. 017/400-732
e-mail : apotekavranje@open.telekom.rs



Saglasno Odluci ZU Apoteka Vranje o korišćenju administrativnih privilegija na računaru, zaposleni daje sledeću

IZJAVU

Pročitao sam, razumeo, i prihvatom pravila i uslove koji regulišu korišćenje administrativnih privilegija na računaru ZU Apoteka Vranje.

sam da nepridržavanje ovih pravila predstavlja povredu radne obaveze usled koje mi može prestati radni odnos i/ili od strane ZU Apoteka Vranje biti pokrenut drugi odgovarajući postupak.

Takođe, ovom Izjavom prihvatom da po predloženju od strane ZU Apoteka Vranje izmena i dopuna ove Odluke, iste odmah primenjujem.

Datum:

<i>Ime i prezime</i>	<i>JMBG</i>	<i>Korisnički nalog</i>	<i>Potpis</i>



PRINCIPI FUNKCIONISANJA IT PODRŠKE I PROCEDURA NABAVKE, REALIZACIJE I ODRŽAVANJA IT RESURSA

Dužnosti i obaveze IT podrške

„IT podrška“ je funkcionalna celina u sektoru IP operativnih poslova i zadužena je za realizaciju novih i održavanje postojećih IT resursa ustanove prema zaposlenima kao korisnika tih resursa. U IT resurse spadaju:

1. PC računarska oprema,
2. Periferije (štampači, skeneri, monitori, miševi, tastature, sve vrste eksternih USB uređaja,...),
3. *Software* i to sve vrste sistemskih, komercijalnih, „*home made*“ i adaptiranih kompanijskih software-a,
4. Licence i prava na korišćenje *software*-a,
5. IT servisi (AD, GFS, CA, Mail system, Web portali, Bekap, ...) za ustanovu,
6. Mrežni resursi (pasivni i aktivni mrežni uređaji i elementi za korporativne namene),
7. IP kompanijska telefonija i korisnički telefoni,
8. Korisnički nalozi i njihova prava za korišćenje kompanijskih IT servisa.

Proces odobrenja, tehničke specifikacije i same nabavke IT resursa pod tačkama 1,2,3 i 4 su u nadležnosti sektora za IT dok su za tačke 5,6,7 i 8 u nadležnosti IT podrške.

Svi poslovi realizacije nabavljenih resursa i njeno operativno funkcionisanje i održavanje svih tačaka IT resursa je u nadležnosti IT podrške.

U cilju efikasnog upravljanja i funkcionisanja IT-a u kompaniji, definisana je procedura za sprovođenje zadataka IT podrške kao i nabavka odgovarajućih IT resursa koja je opisana u ovom dokumentu.

Sektoru za IT se upućuju sledeće vrste zahteva:

A.1 NOVI IT RESURSI

- Zahtev za novim računarom
- Zahtev za dodatnim računarskim periferijama (štampači, miševi, tastature i sl)
- Zahtev za novim *software*-om, *softwarskim* licencama i pravima pristupa
- Zahtev za novim aplikativnim nalogom za zaposlenog (SAP poslovni sistem)

IT podršci se upućuju sledeće vrste zahteva:

A.2 NOVI IT RESURSI

- Zahtev za novim domenskim/e-mail nalogom za novog zaposlenog
- Zahtev za novim IP telefonom, numeracijom i korisničkim profilom
- Zahtev za novu konekciju na korporativnu mrežu (fizičko-logičko priključenje na mrežu)
- Zahtev za zatvaranjem, deaktivacijom ili demontažom IT resursa

B. ODRŽAVANJE IT RESURSA

- Zahtev za rešavanjem IT problema (nedefinisani problem)
- Zahtev za intervencijom nad računarom - *hardware*
- Zahtev za intervencijom nad računarom – *software*, instalacija i deinstalacija dodatnog *softwera* na računaru
- Zahtev za intervencijom nad računarskim periferijama
- Zahtevi za intervencijom na postojećem aplikativnom, e-mail ili domenskim nalogom
- Zahtev za intervencijom na korporativnoj mreži (fizički pristup, selidba, mrežni problem, logička prava pristupa mrežnim resursima i Internetu)
- Zahtev za dodatnim privilegijama nad IT resursima i servisima (računarom, periferijama, mrežnim resursima, pristupom, telefonom, ...)

Zahteve za nabavku ili kreiranje novih IT resursa kao i njihovu demontažu ili deaktivaciju (grupa A) šalje isključivo direkcija (uprava) ili određeni zaposleni delegirani od strane nadređenih rukovodioca direkcije za pojedine pozicije u grupi novih IT resursa.

Zahteve IT podršci (grupa B) šalju svi njihovi korisnici (zaposleni).

Zahtev treba da zadovolji određenu formu i taj deo poslovnog procesa se definiše posebnom procedurom i dokumentima koje definiše IT podrška. Sva dokumentacija i objašnjenja takvih promena ne menjaju ovu proceduru i biće postavljena na samom korporativnom portalu.

Zaposleni kontaktira IT podršku putem internog IT kontakt centra, putem e-mail naloga ili kroz forme i aplikacije na korporativnom portalu. Nijedan od pomenutih komunikacionih kanala nema posebnu privilegiju već se to definiše kroz nivoe prioriteta i redosled prijave.

U slučaju da rešavanje problema ne zavisi direktno od IT podrške, IT podrška će da eskalira problem i delegira rešavanje problema ka drugoj funkcionalnoj celini (odeljenje mreže, IP telefonije, Internet tehničke podrške, IT-SAP tim, eksterni partner) sve do rešavanja konačnog problema ali i dalje sam istupa prema korisniku koji je prijavio problem.

U slučaju prijema zahteva za intervenciju, IT podrška će da odredi prioritete problema na osnovu liste prioriteta i odgovoriti pošiljaocu da je zahtev primljen.

Procesiranje zahteva, brzina intervencije i rešavanja problema u IT podršci zavisi od realnih mogućnosti i broja ljudi u IT podršci kao i složenosti problema (potencijalno učešće eksternih timova) tako da IT podrška nije u mogućnosti da garantuje odgovarajuću raspoloživost servisa za sve slučajeve ali je dužna da svaku prijavu procesira, vodi evidenciju za taj slučaj, omogući uvid korisnika u stanje rešavanja tog slučaja sve do njene konačne realizacije ili zatvaranja slučaja uz saglasnost korisnika.

Način i detalji kontaktiranja IT podrške

Zahtev za intervencijom IT podrške se realizuje kroz sledeće komunikacione kanale:

1. Putem e-maila irena.tasic@open.telekom.rs sa definisanom formom
2. Pozivom službenog telefonskog broja: **064-8982862** ili pozivom ka fiksnoj telefonskoj mreži na broj **017-405397**

Zahtev upućen IT službi treba da sadrži sledeće elemente:

- Kratak i jasno određen SUBJECT maila.
 - Datum kad je zahtev upućen - biće automatski generisan
 - Vreme kad je zahtev upućen - biće automatski generisan
 - Naziv objekta i adresa lokacije na kojoj je potrebna realizacija zahteva
 - Ime i prezime onog ko je direktno u problemu i kontak informacije
 - Računar ili oprema koja je u problemu. U slučaju računara, IP adresa računara i ime.
 - Kratak opis ili informacije o problemu.
- (npr: opis problema i da li je ovo prvi put da se ovo dešava ili je već bilo sličnih problema i kad, ko je u tom slučaju intervenisao i kako je rešen.)

Određivanje prioriteta

Nivo 1 - URGENTNI - Vreme reagovanja IT službe je manje od **15 minuta**.

U pitanju su slučajevi kad je ugrožen rad cele ustanove. U slučaju pojavljivanja problema sa ovakvim prioritetom, svi ostali zahtevi se stavljaju na čekanje dok se ne otkloni problem sa ovim stepenom prioriteta. Primeri ovakvih slučajeva su prestanak ili problemi u radu bitnih serverskih sistema kao što su IP telefonija, Mail servis, *LogOn Network* servisi i sl.

Nivo 2 - HITNI - Vreme reagovanja IT službe u roku **2 sata** od prijema problema.

Slučajevi kad je onemogućen rad određenih delova ustanove ili *top management*-a od čijeg rada zavisi funkcionisanje ostalih sektora. U ovu grupu spadaju i korisnički servisi.

Nivo 3 - NORMALNI - Vreme reagovanja je **8h u toku radnog dana**.

Svi ostali slučajevi spadaju u ovaj nivo prioriteta. Njihovo realizovanje zavisi i od toga da li su rešeni slučajevi sa višim prioritetom.

Trebovanje i održavanje IT opreme

Svako obezbeđivanje IT resursa podrazumeva neko potrebno vreme bez obzira da li se ono obezbeđuje kroz takozvanu sistemsku i projektnu realizaciju ili nabavkom *ad-hoc* na zahtev. *Ad-hoc* nabavka po zahtevu za trebovanje ima svoje budžetske mesečne limite. Služba IT po prijemu zahteva za nabavljanjem računara, računarske opreme, softverskih licenci i ostale periferne opreme, vrši procenu potrebne konfiguracije i opreme na osnovu **radne pozicije za koju se treba opremiti** i potom upućuje zahtev službi nabavke, sem u slučajevima kada se nabavka takve opreme realizuje kroz pojedine projekte tehničko tehnološkog karaktera koja ne spada u standardnu IT office funkciju.

Kad su u pitanju zahtevi za instalacijom određenog softvera, načelnici moraju da imaju u vidu da svaki softver ima određen broj licenci koje su kupljene ili budžetski planirane od strane IT službe ZU Apoteka Vranje i da svoje potrebe što približnije planiraju prilikom pravljenja budžeta u saradnji sa službom za IT i IP operativne poslove. Standardizacija radnog okruženja i software-a koji se koristi za pojedine poslove je u nadležnosti službe IT pa se na osnovu toga i definiše koje licence i *software*-i treba da se koriste u kompaniji.

Načelnici objekata su odgovorni za eventualne zloupotrebe licencnih prava i manipulaciju sa hardverom od strane zaposlenih koji pripadaju njegovom objektu. Definisane

dozvoljenih aktivnosti i načina korišćenja IT resursa i IT tehnologija su opisane kroz poseban pravilnik za primenu IT-a.

U slučaju kvara opreme koja je još uvek pod garancijom ili zahteva intervenciju od strane trećeg lica ili ovlašćenog servisa, IT služba preuzima opremu i šalje u servis. U zavisnosti od mogućnosti i raspoloživosti IT resursa, IT služba obezbeđuje rezervnu zamensku opremu u cilju nastavka funkcionisanja službi sve do povratka opreme sa popravke ili trajne zamene.



PROCEDURA ZA ULAZAK U SERVER SALU

1. Način izdavanja ključeva

Ključevi od server sale čuvaju se kod Pomoćnika direktora u posebnom sefu. Lista radnika kojima je dozvoljen pristup ključevima nalazi se u prilogu.

U sefu se nalazi overeni spisak službenika kompanije ZU Apoteka Vranje koji imaju pristup ključevima.

U sefu se nalazi knjiga evidencije.

U sefu se nalazi primerak "Procedura za ulazak u server salu".

Pomoćnik direktora, izdaje ključ radniku ZU Apoteka Vranje sa spiska uz prethodnu identifikaciju, a u knjigu evidencije upisuje sledeće podatake:

1. Datum
2. Vreme uzimanja
3. Razlog uzimanja
4. Potpis radnika ZU Apoteka Vranje prilikom uzimanja ključeva
5. Potpis lica koji izdaje ključ
6. Vreme vraćanja
7. Potpis lica prilikom vraćanja ključa
8. Potpis radnika ZU Apoteka Vranje prilikom vraćanja ključeva

Ključevi od server sale moraju da se vrate u istom danu.

Ako se javi potreba da se ključevi zadrže više od jednog dana obavezno se obaveštava nadležni šef održavanja tog objekta (usmeno ili telefonom). Pored toga, u roku od 24h od vremena uzimanja ključa, potrebno je da se nadležnom šefu održavanja i nadređenom šefu sektora kome radnik pripada, pismeno ili putem e-maila dostavi izveštaj koji sadrži razloge za duže zadržavanja ključa.

2. Način ulaska, izlaska i ponašanje u server sali

1. Neposredno pred ulazak u server salu obavezno se javiti Upravi ZU Apoteka Vranje.

2. Tokom boravka u server sali koja je opremljena stabilnim sistemom za dojavu i gašenje požara ULAZNA VRATA MORAJU DA BUDU OTVORENA.

3. Prilikom ulaska u server salu izvršiti fizičku inspekciju – svetlo, čistoća, pokušaji provale i sl. O primećenim nedostacima obavestiti Upravu ZU Apoteka Vranje. Radnik Uprave ZU Apoteka Vranje o problemu odmah obaveštava direktora ustanove ili pomoćnika direktora.
4. Zabranjeno je da se dira oprema koja ne spada u domen odgovornosti radnika ZU Apoteka Vranje koji ulazi u server salu.
5. Ukoliko postoji potreba da radnik ZU Apoteka Vranje uključi neki električni uređaj, radi obavljanja svog posla, potrebno je da od načelnika datog objekta dobije odobrenje i upustvo gde može da priključi električni uređaj.
6. Ukoliko postoji potreba da radnik ZU Apoteka Vranje instalira novi mrežni uređaj, potrebno je da se prethodno konsultuje oko načina postavljanja sa načelnikom tog objekta
7. Nakon završenog posla u server sali, treba očistiti eventualne otpatke za sobom, prekontrolisati klimu i propisno zatvoriti vrata.
8. Neposredno nakon izlaska iz server sale obavezno se javiti u Upravu ZU Apoteka Vranje.
9. U slučaju gubitka ključeva na terenu, lice kome su izdati daje pismenu izjavu o tome. Pomoćnik direktora odmah izdaje nalog za zamenu brave.

Vranje, _____.2013.god.

Direktor ZU Apoteka Vranje

PRILOG

Lista radnika ZU Apoteka Vranje kojima je odobren pristup ključevima

1. Ime i Prezime	kontakt telefon
2.	
3.	
4.	
5.	
6.	



PRAVILNIK O KORIŠĆENJU BACKUP PROCEDURE U ZU APOTEKA VRANJE

SAP R/3 i CRM

Procedura za *Backup* - Tape

Backup SAP sistema ZU Apoteka Vranje se izvršava automatski preko iStor Secure Data Value softvera na Tape uređaj.

Na serverima je instaliran iStore SDV klijent koji se putem API-ja rutira *backup* na iStore SDV koji podatke raspoređuje na jednu ili više traka i koji vodi računa o broju kopija koje će da se čuvaju kao i o upotrebi traka. Takođe se bekapuje i iStore baza koja je neophodna za vraćanje podataka.

Politika bekapa je sledeća:

Bekap se istovremeno upisuje na dve trake iz razloga što se dobija na brzini. Ubrzanje je, u ovom slučaju, 2x. Ovo je definisano na iStore SDV-u.

Prilikom pravljenja *backupa* zapis se vrši na trake, a nakon toga se pravi kopija tih traka i te kopije se vade napolje kako bi se stavile u vatrostalni sef. Poslednji *backup* se uvek nalazi u *library*-u dok se **kopije** iznose u vatrostalni sef. U okviru iStore SDV čuvaju se poslednje 2 kopije produkcije, ne računajući poslednji bekap, što znači da imamo poslednja tri bekapa.

Nakon bekapa trake sa produkcionim podacima se preko iStore SDV ristužu na drugom storidžu (za potrebe tehničkog sektora), tako da se istovremeno vrši verifikacija traka i pravi radna kopija u slučaju havarijskog događaja sa storidžom, pri čemu bi se vršilo premapiranje servera na alternativni storidž, dopunila kopija sa dnevnim logovima i nastavio produkcionni rad. Zaduženi za navedene aktivnosti su _____.

Fizička zamena traka se vrši svakog ponedeljka i četvrtka. Trake koje se vraćaju ili vade iz biblioteke određuje iStore SDV koji se, između ostalog, brine i o ravnomernom korišćenju (habanju) traka. Preporučeni radni vek traka je procenjen na 12-14 meseci nako čega se

moraju poručiti nove trake kako bi u svakom trenutku zapis bio siguran. Evidencija o zameni traka se vodi u pisanom obliku u server Sali.

Zaduženi za zamenu traka su _____.

Bekap se izvršava u ONLINE modu što znači da nema prekida u radu SAP sistema.

Provera bekapa se vrši preko logova ili iz SAP-a korišćenjem transakcije DB12, za šta su zaduženi _____. U slučaju neuspešnog bekapa o tome hitno obavestiti rukovodioca IT sektora.

Bekapovi se pokreću preko AIX OS-a tako što je zakazano pokretanje BRBACKUP programa u vreme kako je navedeno u tabeli 1.

Tabela 1.

SSERVER	DANI Backup-a	Vreme	Br. Kopija
	Pon - Ned	23:55	2
	Pon – Ned	23:55	2
	Pon – Ned	23:55	2
	Pon – Ned	23:55	2
	Pon - Ned	23:55	2

8. LITERATURA

- [1] Australian Communications – Electronic Security Instruction 33, *Security Handbook*, <http://www.acsi.com>, 2002
- [2] Bahan, C, *The Disaster Recovery Plan*, <http://www.sans.org>, 2003
- [3] BANJEGLAV, T., DIMITRIJEVIĆ, N., *Istraga aktivnog kompjuterskog incidenta*, ZITEH 2004
- [4] BSI (Federalni IS Nemačke), *IT Baseline Protection Manual*, <http://www.bsi.bund.de/gshb>, juli 2005
- [5] CARNet CERT, LS&S, *Napredne metode otkrivanja sigurnosnih propusta*, Hrvatska akademska i istraživačka mreža, Zagreb 2004
- [6] Computer Security Incident Response Team (CSIRT), *Frequently Asked Questions (FAQ)*, http://www.cert.org/csirts/csirt_faq.html, 2006
- [7] Freeman, W., *Business Resumption Planning: A Progressive Approach*, Version 1.2f, SANS Institute, www.sans.org, 2002
- [8] GRUBOR, G., *Projektovanje menadžment sistema zaštite informacija*, Univerzitet Singidunum; 2012
- [9] HOLME, D., ORIN, *Upravljanje i održavanje okruženja Microsoft Windows servera 2003*, CET Computer Equipment and Trade, Beograd 2004
- [10] ICOVE, D., GEGER. K., VNSTORCH, W: (1995) *Computer crime*, O'Reilly, London.
- [11] ISO/IEC 27001, *Information Security Management System*, <http://www.iso.27001.org>, 2008
- [12] ISO/IEC 27005, <http://www.iso.27005.org>, 2008
- [13] JURANIĆ, L., *Otkrivanje sigurnosnih propusta fuzzing tehnikom*, Infigo information security, Zagreb 2006
- [14] KOVAČEVIĆ, D., *Sigurnosna politika – Fakultet elektrotehnike i računarstva*, Zagreb 2008.
- [15] MILOSAVLJEVIĆ, M., GRUBOR, G., *Osnovi bezbednosti i zaštite informacionih sistema*, Univerzitet Singidunum, Beograd 2007
- [16] MILOSAVLJEVIĆ, M., GRUBOR, G. (2007): *Osnovi bezbednosti i zaštite informacionih sistema - praktikum*, Fakultet za poslovnu informatiku – Univerzitet Singidunum, Beograd 2007
- [17] MILOSAVLJEVIĆ, M., GRUBOR, G., *Istraga kompjuterskog kriminala – metodološkotehnološke osnove*, Univerzitet Singidunum, 2009
- [18] NIST, *A Survey of Access Control Methods*
- [19] NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, <http://www.nist.gov/publications>, verzija 2004
- [20] NIST SP 800-61, *Computer Security Incident Handling Guide*, <http://www.nist.gov/publications/nistpubs/index.html>, 2004
- [21] Petrović, R. Slobodan, *Kompjuterski kriminal*, II izdanje, MUP RS, 2004
- [22] RFC 2196, *Site Security handbook*, <http://www.faqs.org/rfc/rfc2196.html>, 1997
- [23] Ridgway, L. E., *Disaster Recovery: Survivability & Security*, Version 1.4b GIAC Practical Assignment, 2003
- [24] RODIĆ, B., ĐORĐEVIĆ, G., *Da li ste sigurni da ste bezbedni*, Produktivnost AD, Beograd 2004.
- [25] Ross, R., Katzke, S., NIST SP 800-53, A, B, C, *Recommended Security Controls for Federal IS*, <http://www.csrc.nist.gov/publications/nistpubs/800-53/sp800-53.pdf>, 2005
- [26] SANS Institute, *Introduction to business continuity planning*, www.sans.org, 2009

- [27] Stoneburner, G., & all, *Risk Management Guide for Information Technology Systems*, SP 800-30, <http://www.csrc.nist.gov/publications>, 2002
- [28] TASIĆ, I., *Reinženjering sistema zaštite IKT sistema AU Vranje*, Univerzitet Singidunum – Department za poslediplomske studije, Beograd 2009.
- [29] US Department of Homeland Security, *Federal Computer Incident Response Center: Incident Handling Checklists*, <http://www.fedcirc.gov/incidentResponse/IHchecklists.html>, 2003
- [30] VEINOVIĆ, M., JEVREMOVIĆ, A., FRANC, I., STANIĆ, N., *Izolovanje faze incidenta proaktivne digitalne forenzike korišćenjem adaptivnog virtualnog okruženja*, Singidunum revija Vol. 7/No. 2, 2010
- [31] Velliquette, D., *Computer Security Considerations in Disaster Recovery Planing*, GIAC Security Essentials Certification (GSEC) V1.4b Option1, www.gsec.org, 2004

Internet izvori:

- [32] <http://public.dhe.ibm.com/common/ssi/ecm/en/wgd03002usen/WGD03002USEN.PDF>
- [33] <http://www.sasastamenkovic.com/blog/2011/02/02/sigurnost-moodle-lcms-a/>
- [34] <http://www.scribd.com/doc/2096981/Intrusion-Detection-and-Prevention-Systems>
- [35] http://sistamac.carnet.hr/sigurnost/sigurnosna_politika_ustanove.pdf
- [36] http://sistamac.carnet.hr/fileadmin/sem/Politika-ustanove_files/frame.htm
- [37] http://sr.wikipedia.org/wiki/role-based_access_control
- [38] http://www.cisco.com/en/US/prod/collateral/modules/ps2706/ps6236/product_data_sheet0900aecd80220a6e.pdf
- [39] http://www.cisco.com/en/US/prod/collateral/modules/ps2706/ps6236/product_implementation_design_guide0900aecd80223072.pdf
- [40] <http://www.europos.co.rs/pages/naslovna/resenja/trgovina/apoteke.php>
- [41] <http://www.europos.co.rs/pages/naslovna/referentni-projekti.php>
- [42] https://www.google.rs/search?tbm=isch&hl=sr&source=hp&biw=1280&bih=693&q=cloud+computing&gbv=2&oq=cloud+computing&aq=f&aqi=g1g-S9&aql=&gs_nf=1&gs_l=img.3..0j0i24l9.1532.6375.0.6641.17.17.1.7.8.0.94.798.9.9.0.Fu1wGuO9FZI
- [43] https://www.google.rs/search?tbm=isch&hl=sr&source=hp&biw=1280&bih=693&q=taksonomija+cloud+computing&gbv=2&oq=taksonomija+cloud+computing&aq=f&aqi=&aql=&gs_nf=1&gs_l=img.3...1312.8922.0.9500.28.28.0.23.23.0.94.438.5.5.0.i-LS4k4ckMU
- [44] <http://www.gskos.hr/sigurnostGISKO.doc>
- [45] <http://www.istor.net/>