



**UNIVERZITET SINGIDUNUM**

**-MASTER STUDIJSKI PROGRAM-  
SAVREMENE INFORMACIONE TEHNOLOGIJE**

**Šifrovanje i zaštita u okviru u SAP  
sistema  
- Master rad -**

**Mentor:  
Prof. dr. Mladen Veinović**

**Student:  
Miloš Martinović  
Br. indeksa: 410044/2015**



Beograd, 2016

# Šifrovanje i zaštita u okviru u SAP sistema

**Sažetak:** U ovom radu predmet razmatranja biće načini na koje se vrše napadi u okviru cyber prostora sa akcentom na napade na SAP ERP sisteme, kao i njihova ranjivost i vidovi zaštite. U prvom delu rada glavni osvrt će biti na vrste napada, a pogotovo na one koje se mogu primeniti na SAP sistem kako bi se ugrozila njihova bezbednost. Razmatraće se način na koji se ti napadi sprovode kao i primer u kome je uspešno izvršen napad na SAP sistem i posledice koje je taj napad ostavio. Drugi deo rada biće posvećen samom principu i načinu funkcionisanja SAP sistem, kako je taj sistem kroz verzije napredovao i koje su metode korišćene kako bi se stepen bezbednosti i zaštite podigao na veći nivo. Pored same zaštite SAP-a, izvršiće se kratak pregled i u načinu funkcionisanja mreže koja se odnosi na SAP sistem i kako funkcioniše zaštita u okviru nje.

**Ključne reči:** SAP, cyber napad, zaštita, bezbednost, ERP sistemi, javni ključevi, digitalni potpis

## Encryption and protection within the SAP system

**Summary:** In this paper, the subject of discussion will be ways in which attacks within the cyber space are carried out with a focus on attacks on SAP ERP systems, as well as their vulnerability and security options. In the first part of this paper the main emphasis will be on different types of attacks, especially those that can be applied to the SAP system in order to endanger information and documents security. The paper will also review the way in which these attacks are carried out as well as an example of successfully executed attack on the SAP system and the consequences of this attack. The second part will be dedicated to the functioning of the SAP system, reviewing the way the system progressed through different versions over time and what methods are used to raise levels of security and protection to the higher standards. In addition to the protection of the SAP, a brief overview will be made of the means networks function in relation to SAP systems and how the protection within it actually works.

**Keywords:** SAP, cyber-attack, protection, security, ERP systems, public keys, digital signature

# Sadržaj

|                                                                        |    |
|------------------------------------------------------------------------|----|
| 1. Uvod .....                                                          | 3  |
| 2. SAP i njegova primena.....                                          | 4  |
| 2.1. ERP Sistemi i način rada SAP ERP .....                            | 6  |
| 2.1.1. SAP NetWeaver .....                                             | 8  |
| 3. Savremeni oblici ugrožavanja bezbednosti na internetu .....         | 9  |
| 3.1. VRSTE CYBER NAPADA NA INFORMACIONE SISTEME .....                  | 10 |
| 3.1.1. BACKDOOR .....                                                  | 11 |
| 3.1.2. BRUTE FORCE Napadi .....                                        | 12 |
| 3.1.3. Keystroke Logging .....                                         | 13 |
| 3.1.4 Phishing .....                                                   | 14 |
| 4. RANJIVOST SAP-a.....                                                | 15 |
| 5. ZAŠTITA SAP ERP SISTEMA .....                                       | 16 |
| 5.1. Prijavljivanje i šifre kao zaštita u SAP sistemu.....             | 17 |
| 5.1.1. Inicijalna šifra i pravila provere .....                        | 18 |
| 5.1.2. Secure Network Communications i Single Sign-On.....             | 19 |
| 6. SAP R/3 KONCEPT AUTORIZACIJE .....                                  | 21 |
| 6.1. Profile Generator .....                                           | 23 |
| 6.2. Authorization Infosystem .....                                    | 24 |
| 7. Zaštita mreže .....                                                 | 25 |
| 8. SSF mehanizmi i digitalni potpisi .....                             | 26 |
| 8.1. Infrastruktura javnih ključeva .....                              | 27 |
| 9. Zaštita SAP R/3 Internet aplikacija .....                           | 28 |
| 10. SAP S/4 HANA.....                                                  | 29 |
| 11. SAP S/4 HANA zaštita mreže i komunikacija.....                     | 31 |
| 11.1. SSL protokol kao sistem zaštite .....                            | 32 |
| 12. Tipovi korisnika i kreiranje korisnika u okviru SAP S/4 HANA ..... | 32 |
| 13. Zaključak .....                                                    | 35 |
| Spisak referenci .....                                                 | 36 |

# 1. Uvod

Moderno vreme donosi velike promene u tempu i načinu života čemu u velikoj meri doprinosi brži razvoj nove, moderne i lako dostupne tehnologije. Promene u brzini razvoja tehnologije koja je dostupna i samo poslovanje razlikuje se u odnosu na prošli vek. Kako u IT industriji tako i u drugim oblastima u poslovnom svetu sve više stvari i procesa možemo naći koje počinju sa prefiksom "i" što ukazuje na sve veću upotrebu tehnoloških stvari u svetu poslovanja.

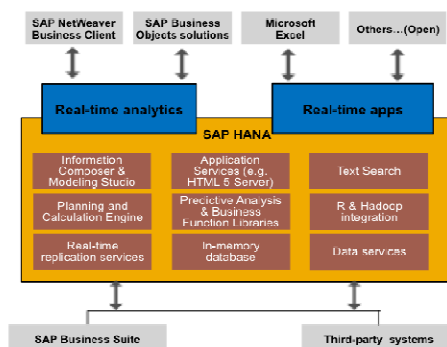
Primer sistema koji je doživeo potpunu ekspanziju u svetu poslovanja jeste SAP - „Systems, Applications and Products in Data Processing” (kasnije samo preveden u skraćenoj formi kao „Systems, Applications, and Products” ili „Systems, Applications, and Programs”, kada je kompanija dobila i međunarodnu ekspanziju). SAP je integrisani poslovni paket i informacioni sistem, koji obuhvata najbolju poslovnu praksu zemalja širom sveta u poslednjih skoro 44 godine. SAP integriše sve funkcionalne oblasti (module) u jedan osnovni proizvod i upravo pristup integrisanosti i zajednički rečnik podataka za sve oblasti ga izdvaja od drugih velikih ERP sistema (ERP – Enterprise Resource Planning).

MySAP ERP (Enterprise Resource Planning) je softversko rešenje koje se bazira na principu objedinjenog menadžmenta ključnih operacija i distribucije podataka u sistemu (<http://searchsap.techtarget.com/definition/SAP>, 2009). Ovo rešenje pruža kompletan set funkcionalnosti za poslovnu analitiku, finansije, upravljanje kadrovskim resursima logistiku i korporativne servise. SAP kao sistem se trenutno najviše koristi u upravljanju finansijama, logistikom, distribucijom i proizvodnim procesima u nizu različitih industrija. Paket obuhvata različite poslovne oblasti, definisane opsegom projekta, u zavisnosti od potreba kupca. Može se implementirati na više jezika, sa više valuta, ispunjavajući različite zakonske regulative za poslovanje širom sveta. Postoji veliki broj objavljenih knjiga (npr. Anderson i ost. 2009; Martinez i McKibbin, 2009; von Aspen 2014), gde se može dobiti više detalja o SAP-u i njegovom pristupu.

U cilju da isprati nove IT trendove i tehnologije, SAP je unapredio softverska rešenja koja nudi na Cloud platformi koja omogućava jednostavniju adaptaciju svih uređaja bez obzira na kojoj su platformi bazirani. Četvrta generacija SAP HANA rešenja je dizajnirana da efikasno ubrza, organizuje i umreži poslovne procese, uređaje i zaposlene u realnom vremenu (<http://scn.sap.com/docs/DOC-60338>, 2015).

## SAP HANA

In-Memory Data Platform for Real-Time Analytics & Applications, Available via Appliance and Cloud Deployment



© 2015 SAP AG. All rights reserved.

Image 1 - SAP HANA – platforma za novu klasu aplikacija i analitike u realnom vremenu

SAP ERP rešenje omogućava da se procesi iz različitih oblasti povežu, olakšaju funkcionisanje jedinstvenog poslovnog sistema i ostavlja prostora za unapređenje i pojednostavljanje svakodnevnih radnih procesa, međutim takođe otvara i niz ranjivosti kompanije. Sa širinom mogućnosti i novim razvojem Cloud tehnologije koje SAP pruža, u poslednje vreme se povećava broj identifikovanih i dobro poznatih problema u kontroli pristupa SAP-u. Jedan od ključnih problema jeste upravo pitanje bezbednosti podataka i lakoća kojom SAP sistem može da se hakuje.

Deo problema potiče od samih malicioznih delova koda u kastomizaciji SAP modula sistemu (Blume, 2015) a napadi se takođe javljaju na mrežnim nivoima kao i na nivoima baze podataka.

Uzimajući sve to u obzir kao i samu prirodu SAP ERP sistema, stvara se idealna podloga za cyber criminal i cyber teroriste. Kompromitovanjem SAP platforme jedne organizacije dolazi se u mogućnost za korporativnu špijunažu, sabotažu, finansijske prevare i napade na poslovanje organizacije. Studije sprovedene tokom poslednjih nekoliko godina prikazuju značajne finansijske gubitke koje kompanije trpe kao posledice cyber napada uz kritične bezbednosne incidente (Blume, 2015).

Glavna tema u ovom radu je pregled načina na koji SAP funkcioniše i korišćene tehnologije kao i bezbednosne probleme koje objedinjuju sve vidove i oblike cyber pretnji i napada na SAP ERP rešenje. Cilj je da na jednom mestu objedinimo pregledno sve potencijalne pretnje i sigurnosne propuste koji mogu da doprinesu bezbednosnim rizicima poslovanja i potencijalnim finansijskim gubitcima.

## 2. SAP i njegova primena

Pet izuzetnih vizionara, poučeni iskustvom koje su stekli u IBM-u se udružilo 1972. godine i osnovalo novu kompaniju koja je imala viziju kako tehnologija može da doprinese razvoju potencijala u biznisu. Na taj način SAP je krenuo putem koji ne samo da je transformisao svet informacione tehnologije već je drastično promenio način na koje kompanije posluju. Danas SAP može da se pohvali sa bazom od preko 300.000 korisnika u 190 zemalja sveta, godišnjim prihodom od preko 20,8 € milijardi i preko 43 godine kontinuiranog ulaganja u razvoj i poboljšanje proizvoda. (<http://go.sap.com/corporate/en/company/history.html> , 2016).

Prvi koraci SAP ERP sistema počinju sa samom idejom i vizijom funkcionisanja softvera u relanom vremenu, što postepeno i postaje moguće krajem 70-ih godina dizajniranje R/2 platforme i sopstvenim serverom i prvim SAP data centrom

(<http://go.sap.com/corporate/en/company/history.html> , 2016). SAP R/2 je sledeće unapređeno softversko rešenje koje radi na principu procesiranja integrisanih podataka potrebnih za poslovanje, koje je daleko naprednije od svog prethodnika i koje ima mnogo jaču pozadinsku podršku data centara i brojnim serverima. Tokom 80-ih godina se širi i ponuda modula koje SAP obuhvata. Sledeća generacija R/3 se bazira na standardizovanom pristupu koji omogućava efikasnije poslovanje i brzi procesiranje informacija.

Takođe, u ovoj fazi razvoja kompanije SAP se otvara ka Internet tržištu i postaje zapravo otvoreni interfejs gde korisnici mogu da povežu i koriste online aplikacije na svom R/3 sistemu.

## SAP Product Overview

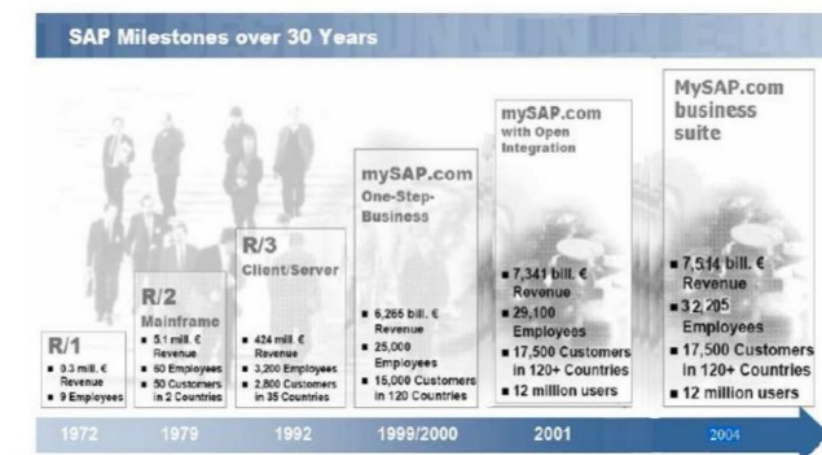


Image 2 - Razvoj SAP ERP sistema kroz istoriju

MySAP ERP u obliku koji je danas dostupan klijentima je objavljen 2004. godine kao naslednik dotadašnjih radova kompanije SAP što je predstavljalo odgovor na konstantnu potrebu za unapređenjem poslovanja od strane klijenta. Tada je načinjena kompletna promena u arhitektonskog sistema infrastrukture tako što je niz dotadašnjih proizvoda poput SAP Buisness Warehouse, SAP Stratigic Enterprise Management i Internet Transaction Server objedinjeni u jedinstvenu ERP centralnu komponentu, SAP ECC (Boeder&Groene, 2014). Takođe, sistem je postao otvoren za Web aplikacije, Cloud rešenja, mobilne aplikacije koje se sve odigravaju u realnom vremenu i kojima se može pristupiti sa bilo koje odobrene lokacije. U periodu najveće ekspanzije SAP preuzima definitivnu ulogu lidera na tržištu ERP sistema koju i danas uspešno održava i definiše trendove na tržištu ERP sistema (Ricadela, 2015). Kao lider na tržištu, SAP uviđa potrebu kao i prostor da ozbiljno proširi poslovanje i na segment MSP (mala i srednja preduzeća) i razvija alate u skladu sa potrebama manjih sistema. Danas su SAP ERP sistemi dostupni u nekoliko oblika u zavisnosti od veličine kompanije i samih potreba poslovanja, te je korisnicima na raspolaganju:

- *MySAP All-In-One* - najkompleksnija ponuda koja se može prilagoditi svim potrebama klijenata
- *MySAP Business Suite* - najčešće korišćen sistem, globalni lider, daje veliku širinu u kastomizaciji
- *SAP Business One* – jednostavan za korišćenje i kastomizaciju, namenjen za male kompanije gde postoji do 100 korisnika u sistemu
- *MySAP ERP* - najjednostavniji oblik, bazične standardne funkcije sa vertikalnom integracijom

## Different Products for Different Companies



Image 3 - Ponuda SAP proizvoda u skladu sa potrebama i veličinom kompanije

Svaki od ovih oblika je promenljiv i fleksibilan i dozvoljava da se prave brze promene u skladu sa zahtevima poslovanja tako što se koristi zajednički set programa. Upravo je ta fleksibilnost i mogućnost da brzo odreaguje ono što čini SAP toliko privlačnim u poređenju sa tradicionalnim One-fits-all sistemima. (<http://www.erpgreat.com/sap-introduction.htm>, 2016.).

Ono što je zajedničko za sve verzije SAP ERP sistema, nezavisno od veličine sistema gde je implementiran jeste upravo činjenica da SAP prepoznaje poslovni proces kao celinu kroz niz različitih organizacionih segmenata od početka do kraja. Na taj način proces može da teče neometano i da u različitim organizacionim jedinicama (npr. finansijama, distribuciji, prodaji) istovremeno daje tražene informacije na osnovu jednog inputa (Hernandez, 2000).

## 2.1. ERP Sistemi i način rada SAP ERP

Uspeh svake kompanije zavisi od proizvoda koji nudi, ljudskih resursa i samih procesa, a ono što podstiče na inovativnost i promene jeste najčešće problem koji se može rešiti postojećim rešenjima (Chetan, 2006). Kompaniji nije neophodan ERP sistem da bi uspešno poslovala, međutim ERP sistem će „naterati“ kompaniju da poslovne procese dovede do izuzetno visokog nivoa čime se smanjuju troškovi, operativne ljudske greške a povećava brzina ispunjenja zadataka i efikasnost poslovanja (Olson and Kesharwani, 2010). Chetan (2006) takođe navodi da uspeh poslovanja i kvalitet poslovnih procesa ako posmatramo sa aspekta troškova, reaktivnosti, fleksibilnosti i pouzdanosti u velikoj meri zavise od informacionih sistema dizajniranih da podrže poslovanje.

ERP sistem poput SAP-a povezuje sve poslovne procese u jedinstveni tok podataka i jedinstvenu objedinjenu bazu, gde svaka funkcionalna poslovna jedinica na osnovu zadatih inputa i ovlašćenja dobija potrebne informacije, izveštaje i podatke (Berry, 2016). To u realnosti znači da se svi zaposleni oslanjaju na iste podatke oblikovane u skladu sa njihovim potrebama (<http://www.netsuite.com/portal/resource/articles/erp/what-is-erp.shtml>, 2016). Takođe, ERP sistemi nude određene mogućnosti automatizacije izveštavanja i predefinisanih izveštaja. što daje mogućnost zaposlenima i menadžmentu da na brz i jednostavan način dobiju ključnu metriku i podatke poslovanja.

Međutim, da bi se jedan ERP sistem uspešno koristio u punom potencijalu, potrebno je da zaposleni i menadžment jasno razumeju šta je razlog i cilj implementacije ERP sistema i šta je ono što će on dugoročno doneti kompaniji.



Image 4 - ERP Sistem kroz oblasti funkcionisanja

Šta SAP ERP razlikuje od drugih ERP sistema i čini planetarno popularnim nije samo razlika u pristupu poslovanja i arhitekturi sistema već upravo lakoća integracije sa postojećim, nezavisnim aplikacijama koje mogu da nastave uspešno da funkcionišu u sistemu kompanije. Poslovna analitika, raznolikost izveštavanja i mogućnost prilagođavanja različitim industrijama je dodatni benefit koji SAP ERP sistem pruža u poređenju sa konkurentima (<http://www.technofunc.com/index.php/erp/145-how-sap-works>, 2012). Takođe, ono što je možda i najvažnije naglasi jeste da SAP ERP funkcioniše na principu već dokazane metodologije i dobrih praksi iz poslovanja, bazirane na naprednim softverskim alatima kao i brzu opciju reagovanja u skladu sa poslovnim promenama, blagovremeno pružajući podršku za svaki kritični proces u kompaniji.

Kako bi ispratili trenutne tehnološke trendove i definitivnu potrebu za procesiranjem velike količine podataka sa različitih lokacija, poslednja promena u SAP ERP arhitekturi se bazira na principu trostrukog sloja gde svaki nivo ima svoju ulogu u funkcionisanju ERP sistema. Osnovna prednost SAP troslojne arhitekture je u tome što se svi procesi odvijaju integrisano u realnom vremenu na razdvojenim serverima i različitim lokacijama (Okungbowa, 2015).

Prvi sloj koji je poznat kao Prezentacioni sloj je ono što korisnik vidi i služi kao ulazni mehanizam koji kontroliše SAP sistem, dok istovremeno služi i kao način da korisniku prikažu izlaznu informaciju u prijatnom grafičkom korisničkom okruženju. Ovaj nivo se često zove i SAP GUI, obzirom da korisnik ovaj sloj koristi kao interfejs za komunikaciju s SAP sistemom (Magal and Word, 2012). Posmatrano sa tehničkog aspekta, Prezentacioni sloj je u direktno povezan sa Aplikacionim slojem, koji predstavlja sledeći dublji nivo u SAP ECC arhitekturi.

Aplikacioni sloj deluje kao posrednik u SAP sistemu, to je mesto gde se odigravaju svi procesi. Aplikacioni sloj možemo još definisati kao centralnu procesorsku jedinicu (CPU). On skuplja sve postojeće informacije iz baza podataka, procesira ih i dostavlja ih korisniku preko Prezentacionog sloja.

Treći, najdublji sloj čine upravo baze podataka koje dozvoljavaju da se svi podaci skupljaju, čuvaju i menjaju u skladu sa potrebama poslovanja. Ovaj poslednji sloj se godinama

unapređuje i pospešuje, u skladu sa potrebama poslovanja sa jedne strane ali takođe i sa unapređenjem tehnologija, te su poslednje promene urađene upravo na Cloud platformi i unutrašnjoj memoriji. Ovo ne samo da je efikasniji način da se procesiraju podaci koji obuhvataju mnogo širu bazu podataka nego individualni serveri i data centri, već je finansijski efikasnije (Missbach et al., 2013).

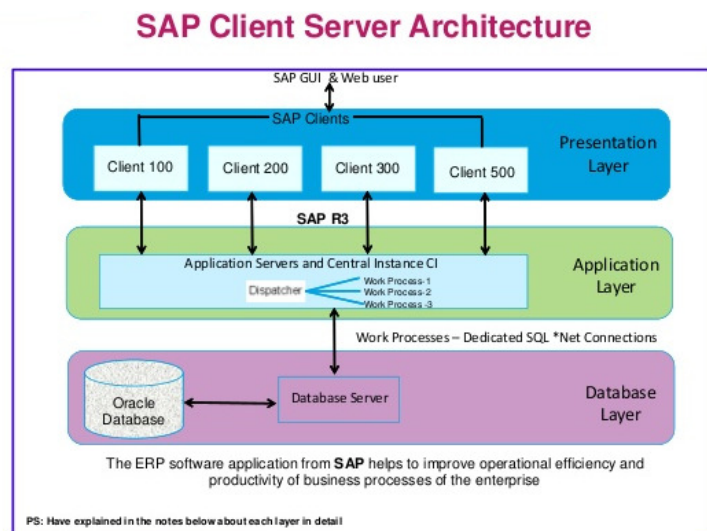


Image 5 - SAP ECC arhitektura

Iako deluje kompleksno, logika kojom se SAP rukovodi u ponudu kastomizovanog softvera jeste kompleksnost današnjeg poslovanja i nemogućnost da se unapred predvide sve individualne potrebe jedne kompanije. Hernandez (2000) zaključuje da je od objave R/3 verzije SAP radio na konstantnom unapređenju ponude koja je dostupna klijentima (poput unapređenja korisničkog interfejsa, kompatibilnosti sa MS Office paketom, komunikacija preko Web aplikacija...) sa ciljem jednostavne upotrebe i lakoće implementacija promena.

Sve ove promene su ispraćene i tehničkim promenama programskih jezika te je pored ABAP (programski jezik za SAP) sada je za implemtaciju kastomizacije i promenu standardizovane verzije integracijom različitih aplikacija na modulima programerima na raspolaganju i SAP NetWeaver koji takođe može da se koristi i na drugim programskim jezicima C,C++ ili Java EE (Linkies and Karin, 2011).

### 2.1.1. SAP NetWeaver

SAP NetWeaver je platforma koja uz sve svoje komponente obezbeđuje upravljanje svim aplikacijama i onima koji su zasnovane na SAP-u i onima koje nisu kroz različita heterogena software-ska okruženja.

Aplikacija koja je razvijena od strane SAP-a pruža mogućnosti integracije poslovnih procesa i baza podataka koje imaju različite izvore uz istovremenu upotrebu vodeće tehnologije web servisa. Važan napredak koji je ostvaren stvaranjem NetWeaver aplikacije je u tome što je to prva aplikacija koja je interoperabilna kroz raličite aplikativne platforme i kompletno je zasnovana na web-u (Chaitanya, 2012). Ona kao takva u stanju je da se koristi ne samo za razvoj SAP aplikacija već i svih drugih koje se ne zasnivaju na SAP-u. NetWevaer u potpunosti omogućava programerima da u samu aplikaciju integrišu ne samo informacije, već i procese iz potpuno različitih geografsikih lokacija koristeći različite savremene informacione tehnologije kao što su Microsoft-ov .NET, IBM-ov WEBSphere, Sun-ovu Javu.

Prva verzija SAP NetWeaver-a lansirana je 2004. godine i tada je definisana kao sistem koji kombinuje različite osobine u cilju olakšavanja upravljanja različitim aplikacijama putem jedinstvenog sistema i po mnogo nižoj ceni. Kada je predstavljan, koncept niže cene objašnjen je u vidu jedinstvenog sistema koji će biti u mogućnosti da upravlja podacima iz različitih procesa i na taj način da smanji troškove. SAP NetWeaver pruža jedinstven sistem praćenja različitih procesa i to je ono što ga izdvaja na tržištu. Ovaj vid aplikacije predviđen je za sva preduzeća koja za cilj imaju da spoje svoje procese i upravljanja u jedan jedinstven sistem. Druga pogodnost ovog software-a je to što korisnicima pruža mogućnost kreiranja novih aplikacija, a da prilikom toga mogu vršiti potpunu migraciju podataka iz postojećih sistema. Sam program čini poslovanje kompanije pouzdanijim i efikasnijim što kao rezultat daje veći profit i vrednost same kompanije na tržištu (Magen-Goldstein, 2012).

SAP NetWeaver se sastoji od više različitih komponenti:

- SAP Business Information Warehouse (BIW)
- SAP Enterprise Portal
- SAP Business Intelligence
- SAP XI Exchanging Infrastructure
- SAP Knowledge Warehouse (KW)
- SAP Master Data Management (MDM)

SAP Business Information Warehouse predstavlja komponentu koja se odnosi na pružanje različitih informacija koje se odnose na način poslovanja samog preduzeća. Ovu komponentu možemo razložiti u nekoliko različitih slojeva. Tu podelu bi činili sloj za ekstrakciju, polazni sloj, sloj za transformaciju, sloj za utovar i sloj za izveštaj i analizu.

SAP Enterprise Portal je deo koji je zadužen da na jedinstven način izvrši skupljanje informacija i procesa iz različitih odeljenja i dopremi ih u jedan prostor.

SAP Business Intelligence možemo definisati tako da kada se sve prikupljene informacije skladište na jedno mesto, one zahtevaju dublju analizu radi daljeg upotrebe. SAP BI tu stupa na scenu tako što pojednostavljuje manipulisanje podacima i omogućava lakšu analitiku od strane korisnika.

SAP XI Exchanging Infrastructure komponenta je ona komponenta koja pruža mogućnost korisnicima da odaberu da li žele ili ne da koriste SAP-ove aplikacije, kao i da povežu sisteme različitih proizvođača.

SAP Knowledge Warehouse pruža podršku organizaciji kako bi uspostavila i rukovala sa specifičnim znanjima vezanim za industriju i poslovanje u ujedinenom sistemu. To je glavni element koji upravlja ključnim procesima kompanije.

SAP Master Data Management pruža jedinstveno software-sko rešenje koje je zaslužno za stvaranje, distribuciju i upravljanjem ključnim podacima na nivou preduzeća. Ova komponenta takođe pruža uvid u status poslovanja u realnom vremenu.

Prednost samog programa je u tome što korisniku pruža mogućnost da na jednom mestu mogu upravljati različitim aplikacijama koje su zasnovane na različitim programskim jezicima i različitim bazama podataka. Korisnik može putem ove aplikacije udrži sredstva koje poseduje bez potrebe da menja celu bazu podataka. (<http://www.simplilearn.com/sap-netweaver-and-its-components-rar112-article> , 2012).

### **3. Savremeni oblici ugrožavanja bezbednosti na internetu**

Tokom istorije čovečanstva, čovek je dolazio do značajnih otkrića koja su olakšala njegovu produktivnost, tako da sa slobodom možemo reći da računar predstavlja jedno od važnijih pronalaska. Brz razvoj računara uzrokovao je njegov brz ulazak u komercijalnu proizvodnju i tako je postajao sve više dostupniji širim narodnim masama. Takva ekspanzija bila je praćena time da se računar pojavio kao sredstvo za rad u svim segmentima društvenog života. Veliki broj računara iziskivao je da komunikacija između njih bude što brža i jednostavnija. Mogućnost da se tako nešto postigne je bilo stvaranje Interneta. Povezivanjem velikog broja uređaja na mreži, stvorio je plodno tlo za stvaranje novog oblika kriminala, a to je cyber kriminal.

Ubrzani razvoj informaciono-komunikacione tehnologije i nezaustavljiv rast primene u svim sferama ljudskog društva uvećava njihovu ranjivost i izloženost vrlo ozbiljnim opasnostima. Informaciono-komunikaciona tehnologija nosi u sebi ujedno i ono najbolje i ono najgore. Napredak se sastoji u komunikaciji skoro bez granica, a nevolja je u tome što taj „Titanik“ virtualne plovidbe nailazi na santu leda. Posle atomske bombe i uspostavljanja opšteg nuklearnog odvraćanja, modernom društvu je potrebna nova vrsta odvraćanja od najnovnije „informativne bombe“. (Virilio, 2000)

Bezbednosne pretnje informacionom društvu raznovrsne su i specifične po tome što se u velikoj meri prevashodno usmerene na zlonamerno destabilizovanje informativnih sistema. Onemogućavanje normalnog funkcionisanja informacionih sistema u društvu koje je od njih postalo zavisno može imati ozbiljne posledice na sve sfere društvenog života. Nove tehnologije nisu samo iznedrile nove pretnje već su i otežale sposobnost i identifikovanja aktera bezbednosnih pretnji. (Putnik i Bošković, 2013.)

Etimološki posmatrano, koreni pojma sajber bezbednosti sežu u šezdesete godine prošlog veka i vezuje se za prostoro SAD. U tom periodu tretirana komunikaciona bezbednost (Communication Security - COSMEC). Sa pojavom kompijutera, sedamdesetih godina prošlog veka, nastala je kompijuterska bezbednost (Computer Security – COMPUSEC). Već osamdesetih godina XX veka, usled incidenta kao što su bili Kukavičije jaje (Cuckoo's egg) i Morisov crv (Morris worm) uvidelo se da mreža sastavljena od velikog broja računara može biti iskorišćena za zlonamerne ciljeve. Tada dolazi do integracije komunikacione i kompijuterske bezbednosti. Te nastaje pojam informaciona bezbednost (Information Security - INFOSEC).

Informaciona bezbednost je integrisala ranije odvojene discipline, kao što su bezbednost personala, kompijuterska bezbednost, komunikaciona bezbednost i operativna bezbednost. (Sinkovski, 2005).

### **3.1.VRSTE CYBER NAPADA NA INFORMACIONE SISTEME**

Nakon velikog broja godina koje su prošle i počinjenih dela, još uvek niko ne može da da preciznu definiciju ko je „hacker“ i šta je njegov cilj. Dubljom analizom se dolazilo do odgovora da su to određeni pojedinci koji imaju veliko programersko iskustvo i koji zbog nekih svojih ličnih frustracija ili nezadovoljstva uništavaju određene informacione sisteme. Sa druge strane Hackere možemo definisati i kao osobe koje nelagalnim putem prikupljaju važne podatke koje kasnije prodaju radi ostvarivanja novčane dobiti. Prvi slučaj hackerisanja desio se još sedamdesetih godina XX veka kada je John T. Draper sasvim slučajno došao do saznanja da se duvanjem u običnu zviždaljku može reprodukovati tonove koji su u stanju da prevare telefonske centrale i da tako može vršiti besplatne pozive. Kasnije je John napravio uređaj pod nazivom BLUEBOX kako ne bi morao non-stop da duva u zviždaljku. Danas se

hackeri u mnogo većoj meri bave ozbiljnijim stvarima i često kao sredstvo koriste viruse koje postavljaju u kompjuterske sisteme koji su meta napada.

Postoji veliki broj definicija pojma virus. Međutim prva i najčešće prihvaćena je definicija Freda Kohena, ali pored njegove tu su i druge definicije sa kojima se možemo susreti poput:

- Profesor Fred Kohen sa univerziteta u Sinansitiju smatra se prvom osobom koja je 1983. godine uvela reč „virus“ u rečnik računarske terminologije. On je, u svojoj tezi, postavio opštu definiciju virusa, 1984. godine: „Definišemo kompjuterski „virus“ kao program koji „inficira“ ostale programe modifikujući ih da uključuju njegovu naprednu kopiju. Sa inficiranog područja, virus se može širiti kroz kompjuterski sistem i mrežu koristeći autorizaciju svakog korisnika, koristeći ih da inficira njihove programe. Svaki program koji se inficira se takođe ponaša kao virus i na taj način vrši „epidemiju“ i širi se među drugim datotekama“.
- Spafford je ovako definisao računarski virus: „Računarski virus je segment mašinskog koda, obično od 200-4000 bajta, koji će nakon aktivacije kopirati svoj kod na jedan ili više programa domaćina. Prilikom izvršavanja programa domaćina, „zaraženi“ kod će biti izvršen i virus ćena taj način nastaviti da se širi i reprodukuje kroz zaražen sistem“.
- Nacionalni kompjuterski bezbedonosni centar SAD u Rečniku računarsko-bezbedonosnih termina daje definiciju kompjuterskog virusa kao: „To je samošireći trojanski konj, komponovan od delova za određenu svrhu, okidačkog dela i samoširećeg dela. (Franc, 2010).

Kada smo definisali šta bi to virus mogao da bude onda treba da navedemo neke od njihovih vrsta i načina na koje oni deluju. Stoga ćemo u narednim glavama obraditi neke od najčešćih virusa koji se koriste u SAP napadima.

### 3.1.1. BACKDOOR

Backdoor je daljinski administracioni alat koji omogućava korisniku pristup i kontrolu računara putem mreže ili interneta. Backdoor je obično u stanju da preuzme kontrolu nad sistemom zato što se koristi nedokumentovanim procesima koji se nalaze u sistemskom kodu. Ove alatke mogu biti legitimne i mogu se koristiti iz opravdanih razloga od strane ovlašćenih administratora, ali se često koriste od strane napadača da bi se preuzela kontrola nad korisnikovim računarom

(<http://www.cisco.com/c/en/us/about/security-center/virus-differences.html> ,2016.). Tipičan backdoor se koristi od dve komponente, a to su klijent i njegov server. Napadač korisiti klijent aplikaciju da komunicira sa komponentama servera koje su instalirane na žrtvinom sistemu. Komponente servera mogu se dostaviti na žrtvin sistem na različite načine, kao deo deo crva ili trojanskog tereta, putem e-mail-a, file-ovi na peer-to-peer mreži. Jednom instaliran, serverske komponente će otvoriti mrežne portove i na taj način će omogućiti komunikaciju sa klijent aplikacijom. Napadač onda može nesmetano koristiti klijent aplikaciju kako bi zadao komande koje će se izvršavati na zaraženom sistemu.

U zavisnosti od toga koliko je klijent aplikacija kompleksna, može sadržati neke od sledećih komandi (<https://www.f-secure.com/v-descs/backdoor.shtml> 2016.):

- Slanje i primanje datoteke
- Pretraživanje hard diskova i mrežnih diskova
- Prikupljanje sistemskih informacija
- Pravljenje screenshot-ova

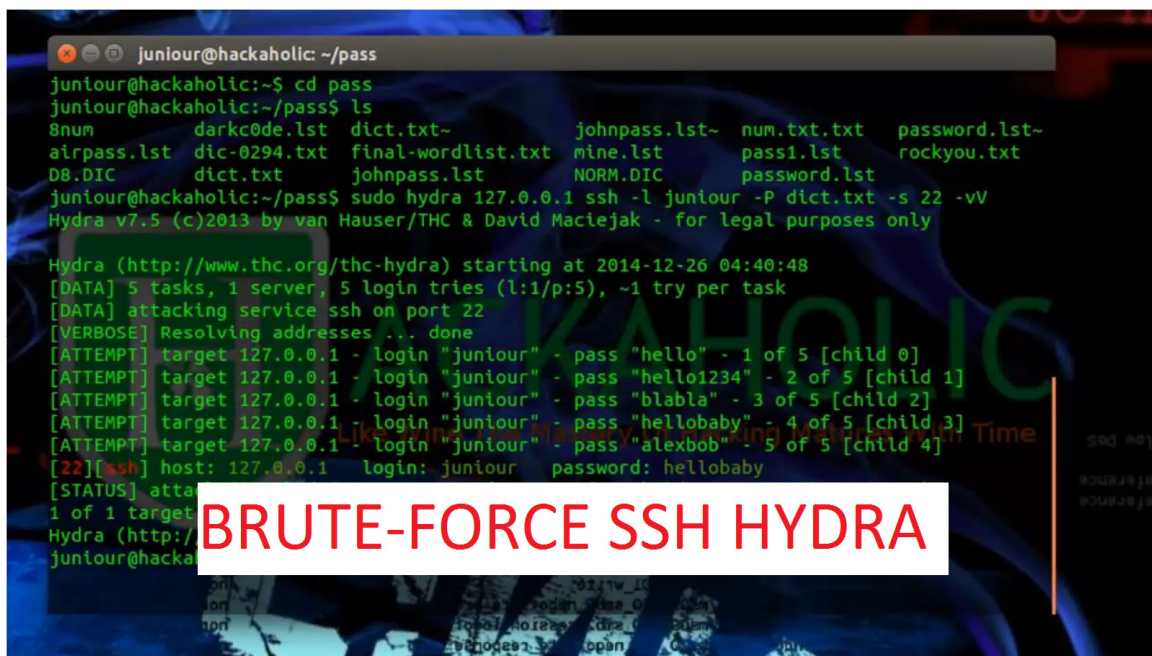
- Promena podešavanja, kao i vreme i datuma
- Izdavanja komandi poput otvaranje CD čitača itd.

### 3.1.2. BRUTE FORCE Napadi

Brute Force je pristup koji se koristi da se na različite načine pokuša i pogrešaka saznaju informacije poput korisničkih lozinki, identifikacionih brojeva, brojeva krednih kartica i drugih stvari. Da bi se izvršio Brute Force napad potrebno je kreirati program koji će na automatski način generisati veliki broj podataka i na taj način pokušavati da dođe do tačne kombinacije karaktera koji se poklapaju sa traženom informacijom.

Brute Force može se naći kako u primeni za zloupotrebu podataka, tako i u bezbednosne svrhe kada se pokušava testirati određena sigurnost nekog software-a. U današnje vreme još uvek postoji veliki broj sistema koje omogućavaju korisniku da kreira šifre sa malim brojem karaktera, na tim sistemima brute force ima izuzetno veliku uspešnost. Brute force napad može trajati od nekoliko minuta do nekoliko godina, u zavisnosti od količine resursa kojom raspolažu. U zavisnosti od cilja napada, resursi mogu biti izuzetno skupi pa je nekad i sam napad ne isplati.

Brute Force pokušava sve moguće varijante bez obzira na njihovu nelogičnost, iz tog razloga ne treba brute force pomešati sa nekim od sličnih metoda koje ipak na neke različite načine redukuju količinu podataka sa kojom raspolažu u pokušaju dolaženja do dobitne kombinacije. Program koji možemo navesti kao primer koji se koristi u izvršavanju Brute Force napada je Hydra. Hydra poseduje sopstveni rečnik u koji je moguće upisivati reči koje se koriste od strane korisnika. Kada se pokrene napad program će pokušati da dođe do tačnog rezultata tako što će ispitivati različite kombinacije reči i karaktera. Uspešnost napada zavisi od količine baze podataka.



```

juniour@hackaholic: ~/pass
juniour@hackaholic:~$ cd pass
juniour@hackaholic:~/pass$ ls
8num      dark0de.lst  dict.txt-   johnpass.lst-  num.txt.txt  password.lst-
airpass.lst  dic-0294.txt  final-wordlist.txt  mine.lst      pass1.lst    rockyou.txt
DB.DIC      dict.txt     johnpass.lst  NORM.DIC      password.lst
juniour@hackaholic:~/pass$ sudo hydra 127.0.0.1 ssh -l juniour -P dict.txt -s 22 -vV
Hydra v7.5 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2014-12-26 04:40:48
[DATA] 5 tasks, 1 server, 5 login tries (l:1/p:5), ~1 try per task
[DATA] attacking service ssh on port 22
[VERBOSE] Resolving addresses ... done
[ATTEMPT] target 127.0.0.1 - login "juniour" - pass "hello" - 1 of 5 [child 0]
[ATTEMPT] target 127.0.0.1 - login "juniour" - pass "hello1234" - 2 of 5 [child 1]
[ATTEMPT] target 127.0.0.1 - login "juniour" - pass "blabla" - 3 of 5 [child 2]
[ATTEMPT] target 127.0.0.1 - login "juniour" - pass "helloworld" - 4 of 5 [child 3]
[ATTEMPT] target 127.0.0.1 - login "juniour" - pass "alexhob" - 5 of 5 [child 4]
[22][ssh] host: 127.0.0.1 login: juniour password: helloworld
[STATUS] atta
1 of 1 target
Hydra (http://
juniour@hacka

```

Image 6 - Napad Hydra programom

Brute Force možemo podeliti na dve vrste napada, a to su :

- Primarni
- Sekundarni

Primarni možemo definirati kao napada u kome se koristi jedno korisničko ime u kombinaciji sa velikom bazom podataka različitih šifri i na taj način se pokušava doći do tačnog para.

Sekundarni način bi bio onaj koji bi se koristio u velikim zatvorenim sistemima u kojima se polazi od pretpostavke da dva korisnika mogu imati istu korisničku šifru i tom slučaju se onda se koristi i velika baza korisničkih imena i velika baza šifri i kada se uspostavi jedan tačan par onda se sa tom šifrom pokušava pronaći još jedan korisnik.

Nedostaci Brute Force napada su u tome što dodavanjem samo jednog karaktera u šifru može povećati broj kombinacija koje bi bilo potrebno proveriti, a to se može manifestovati kroz vreme realizovanja napada koje se samo zbog tog jednog karaktera može povećati na nekoliko godina.

BruteForce je inače jedan od razloga zbog kojeg se korisnicima preporučuje da kreiraju svoje šifre koje će posedovati najmanje 6 - 8 karaktera sa velikim i malim slovom, brojem i znakom.

### 3.1.3. Keystroke Logging

Jedan od izuzetno pouzdanih načina dolaženja do autentifikacionih podataka predstavljaju keystroke logging ili skraćeno keylogging. Termin prvi put ulazi u upotrebu 1983. godine kada je napisan prvi keylogging program od strane Perry Kivolowitz-a. U osnovi naziv samog programa opisuje ono što on zapravo radi, a zamišljen je kao program koji će beležiti sve unose koje se manifestuju na tastaturi (Morgan et al., 2013). Nastajanje samog programa poteklo je od bezazlene namere i od toga da se program koristi u legalne svrhe. Sam program je razvijen u cilju da bi se u kompanijama imalo uvid u to šta korisnici radi i da ne zloupotrebljavaju kompanijske resurse, kao i da ne provode vreme na društvenim mrežama. Takođe još jedna od primena je bila administratorski uvid u to šta su zaposleni radili kako bi se na lakši i brži način pomoglo u rešavanju nekog problema (Sullivan i Lindgren, 2006).

Kao i sve drugo tako je i za KeyLogging pronađen način da se koristi u ilegalne svrhe i da se zloupotrebi. Određene granice su tanke, tako i ona koja se nalazi između kontrole i špijunaže (Gordon i Ford, 2006). Na taj način zloupotreba keyloggera se proširila od privatnih stvari kao što su špijunaža dece, ljubomora, do industrijske špijunaže i narušavanja bezbednosti jedne kompanije.

Za razliku od početnih verzija, današnje savremene verzija keyloggera imaju značajno veći broj funkcija sa kojima raspolažu. Tako jedan savremeni program za keylogging osim osnovne funkcije praćenja unosa na tastaturi može vršiti kreiranje screenshotova koje je u stanju da šalje na unapred predefinisano e-mail adresu, da vrši nadzor i rad određenih programa, nadgledanje internet saobraćaja, nadzor nad internet saobraćajem (Tuli and Sahu, 2013). Sve prikupljene podatke mogu slati napadaču u vidu e-mail adrese, slanjem na ftp server ili manuelnim preuzimanjem na usb memoriju.

Keyloggere možemo podeliti u dve grupe:

- Software-ske
- Hardware-ske

Nakon osnovne podele software-ske možemo da podelimo na sledeći način:

- Keylogger zasnovani na kernelu (Ovakav vid keylogger je težak za pravljenje jer rade na nivou kernela ali njihova prednost je u tome što se teško otkrivaju jer se mogu manifestovati kao driveri za tastaturu)

- Keyloggeri zasnovani na API-ju (Koriste API funkcije tastature i funkcionišu na taj način što OS daje obaveštenje keyloggeru o svakom unosu na tastaturi, njihova prednost je što se lako prave ali mana im je što se lako otkrivaju)
- Keylogger zasnovani na Form Grabbing ideju (Ovaj tip programa prikuplja sve podatke preko web formi pre nego što paket podataka prođe kroz HTTPS protokol)

Sa drastično manje funkcija ali podjednako pouzdani su i hardware-ski keyloggeri. Njihova prednost je u tome što ih nije moguće okriti ni jednim vrstom programa za zaštitu iz razloga što se hardware-ski postavljaju na računar (Ladakis et al.,2013). Njegova mana je baš u tome što je potrebno fizički pristupiti računaru da bi se uređaj instalirao. Nakon sve veće ekspanzije laptop računara kreirani su i hardware-ski keyloggeri za same laptop uređaje.

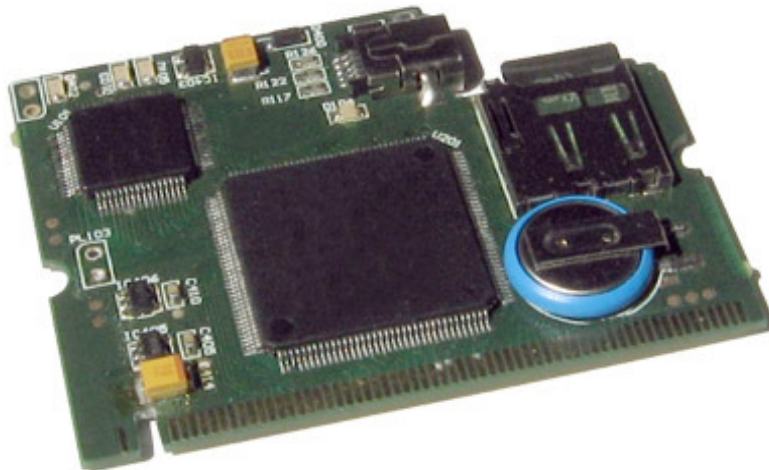


*Image 7 - Laptop Keylogger*

Zaštitu od keyloggera je moguće obaviti na različite načine u zavisnosti od vrste Keyloggera koja je u upotrebi. Što se tiče software-skih verzija keyloggera najsigurnija zaštita je redovno update-ovanje anti-virus baza iz razloga što anti-virus programi u svojim bazama imaju već definisanu grupu podataka koja detektuje keylogger programe kao maliciozne software. Još jedan od dobrih vidova zaštite od sotware-skih verzija je korišćenje kvalitetnog firewall-a koji će prepoznati svako neovlašćeno slanje informacije i o tome obavestiti korisnika. Kada govorimo o zaštiti od hardware-skih keyloggera ona bi se ogledala u edukaciji zaposlenih o mogućim rizicima i pretnjama.( <http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-01-106.pdf> , 2016. ) Stvaranjem određenih procedura u kojima računar ne bi smelo ostavljati bez nadzora kao i edukaciji da zaposlenog da njegov računar sme samo on da koristi i ne dozvoljava upotrebu istog drugim licima.

### **3.1.4 Phishing**

Phishing možemo definisati kao na pokušaj da se na različite načine ukrade nečije identitet u cyber prostoru. Phishing kao glavni alat koristi dovođenje u zabludu korisnika i na taj način dolazi do željenih podataka (Bergholz, A., Chang, J. H., Paass, G., Reichartz, F., & Strobel, S., 2008). Za tu primeni koriste se različite varijante e-mail-ova, lažne internet stranice koje izgledaju potpuno isto kao one prave. Sam naziv ove vrste napada potiče od engleske reči phishing koju možemo prevesti kao pecanje. Takozvanim, pecanjem pokušava se navesti meta napada tj korisnik da ostavi svoje podatke. Prvi napad usledio je još davne 1996. godine kada

je američka kompanija AOL zabranila otvaranje korisničkih naloga korišćenjem lažnih kreditnih brojeva (<http://www.phishing.org/history-of-phishing/>, 2015). Iz toga razloga dosetljivost određenog pojedinaca išla je do te mere da su kreirali lažne e-mail-ove u kojima su se predstavljali kao osoblje AOL koje je iz određenih razloga tražilo da se popuni formular sa potrebnim podacima. Tako kreiran mail slali su na veliki broj adresa i „pecali“ veliki broj korisnika koji bi odgovorio na mail sa potrebnim podacima. Ti prvi napada su bili veoma jednostavni, ali smisao napada je ostao isti tokom godina sa tim što su postali sve sofisticiraniji. Kod kreiranja lažnih internet stranica obično se koriste maske koje pružaju identičan izgled originalu i na čijem se početnom delu nalaze polja za unos korisničkog imena i šifre. U odnosu na original, na lažnim stranicama može se primeniti u URL same stranice koja se po određenim karakteristikama razlikuje od originalne. Kreirana stranica se putem e-mail-a šalje na veliki broj adresa.

Cilj napada uz pomoć phishing alata su najčešće bankovni sistemi, sistemi za online plaćanja, web based aplikacije poslovnih firmi, a u poslednje vreme i društvene mreže (Aaron i Rasmussen, 2015).

Kako bi se lakše uočio phishing napad postoje specijalizovane kompanije koje se bave samo proučavanjem ovog problema. Među njima možemo izdvojiti Anti-Phishing Working Group (APWG). Ona je komercijalna organizacija koja izdaje svoje izveštaje besplatno na mesečnom nivou, u kojima se može pronaći detaljna analiza svih novih phishing napada i načina na koji oni funkcionišu. Druga organizacija koju ćemo spomenuti je PhishTank neprofitabilna organizacija koja radi kao ogranak firme OpenDNS. Kao i prethodna tako i ova organizacija sve svoje informacije koje prikupi o phishing napadima pruža besplatno. Kako bi se što efikasnije zaštitili od phishing napada, poznate kompanije koje u svom posedu imaju web pregledače, razvijaju sopstvene anti-phishing alate. Na taj način Google u svom browser-u ima implementiran Google phishing filter, Microsoft sopstveni phishing filter za IE, itd. ([http://sigurnost.zemris.fer.hr/ns/2011\\_ruzman/ruzman-diplomski-final-09-2011.pdf](http://sigurnost.zemris.fer.hr/ns/2011_ruzman/ruzman-diplomski-final-09-2011.pdf) 2011.)

## 4. RANJIVOST SAP-a

Podučeni dosadašnjim iskustvima iz cyber prostora naučili smo jednu stvar, a to je da sa velikom slobodom možemo reći da je u moderno vreme sve što se nalazi na internetu podložno napadima. Sve što je zaštićeno, može se hakovati samo je pitanje vremena, upornosti, resursa kao i potrebe da se tako nešto učini. Multinacionalne i visokoprofitne kompanije ulažu mnogo resursa i novca u to da zaštite svoje proizvode i da poboljšaju njihovu bezbednost. Slična je situacija i sa SAP-om ali to ne znači da do sada nije bilo napada na taj sistem, pa čak i onih koji su se završavali sa pozitivnim ishodom.

Jedan od primera za to je napad koji se dogodio 2013. godine, a to je napad kineskih hacker-a na USIS (U.S. Investigation Services) koji je iskoristio propuste u SAP software-u da bi izvršio napad. Na osnovu informacija koje su dobijene nakon sprovedene istrage napadači su izvršili napad uz pomoć third-party aplikacije u SAP sistemu i na taj način omogućili sebi da pristupe poverljivim informacijama. Da bi lakše shvatili ozbiljnost ovog napada potrebno je objasniti da je USIS jedna od najvećih federalnih ustanova koja pruža pozadinske provere bezbedonosne informacije kako vladi tako i korporativnim preduzećima. Zapošljavaju više od 5700 ljudi i svoje usluge pružaju u svih 50 zemalja Sjedinjenih Američkih Država.

Ishod ovog napada je bio takav da je ugroženo više od 27000 sigurnosnih provera. Pored ovog napada koji je počinjen tada, sličnih posledica je bilo po Kancelariju za upravljanje kadrovima u čijem su posedu veliki broj sigurnosnih provera. Dolaženjem u posed ovakvim informacijama, hakeri su imali mogućnost da na više različitih načina utiču na život osoba koje su prošle vladine sigurnosne provere. Oni su na ovaj jednostavan način došli do JMBG brojeva, jedinstvenih identifikacionih brojeva i finansijskih podataka pojedinaca čime se

stvora prostor za krađu identita kao samo jedan od teških oblika napada na pojedince. Samo nekoliko sati nakon što se napad dogodio, proceurela je informacija da je problem nastao u propustu u okviru SAP sistema

(<https://erpscan.com/press-center/blog/chinease-attack-on-isis-using-sap-vulnerability-detailed-review-and-comments/>, 2015.).

Iz ovog propusta jasno se vidi da je meta napada bio SAP Enterprise sistem koji je zadužen za planiranje resursa. Stvar koja je ostala nerazjašnjena za vreme napada jeste da li je u vreme kada se propust dogodio postojala odgovarajuća zakrpa i da li zbog toga odgovornost treba pripisati SAP-u kao proizvođaču programa ili USIS-u koji bi bio odgovoran da sprovede krpljenje. Napadači su zahvaljujući svojim sposobnostima oktrili propust tj. samu anomaliju u sistemu koju su uspeali da eksplatišu i da se uz pomoć nje prikače na sistem. USIS je zvanično odbio da objavi ime software-ske aplikacije kojom je izvršen napad i da će u samo izveštaju istrage biti objavljene sve potrebne informacije.

Posledice koja je napravila third-party aplikacija za vreme istrage otkriveni su različitim logovima pod kojima se misli na logove firewall-a, logove bezbednosnih događaja, VPN logova, kao i logova koje prate SAP aplikacije. Napad koji je započet u 2013. godini i izložio sistem ranjivosti do 2014. godine ukazao je na još 20-30 novih kritičnih tačaka u okviru SAP ERP sistema (<http://www.nextgov.com/cybersecurity/2015/05/third-party-software-was-entry-point-background-check-system-hack/112354/>, 2015.).

Nekadašnji vojni obaveštajni analitičar, a danas jedan od stručnjaka za cyber napada u kompaniji ThreatConnect, Richard Barger ukazao je na to ranjivost koji su se manifestovale u okviru SAP sistema može hakerima pružiti mogućnosti za prikupljanje velikog broja poverljivih informacija.

Portparol za odnose sa javnošću USIS, Ellen Davis potvrdila je da se napad dogodio i da si napadači uspeali da uz pomoć third-party aplikacije pristupe USIS mreži i da manipulišu podacima. Kako je SAP jedan od vodećih svetskih IT kompanija sa preko 50.000 korisnika širom sveta, interesatna je činjenica da u zvaničnom saopštenju u kojem se oglašio čovek SAP-a Mat Small, navodi u svom e-mail-u da - Budući da ne komentariše specifičnosti nijednog ugovora sa korisnicima ukoliko nemamo njihovu eksplicitnu saglasnost, SAP neće biti u mogućnosti da pruži kometenatar o nastaloj situaciji. Takođe nakon ove izjave dodao je još da nijedna druga kompanija kao SAP ne posvećuje toliko pažnje bezbednosti i sigurnosti podataka, i da SAP uvek je odgovarao i da će nastaviti da brzo, temeljno i energično odgovora kada kod se oktriju novi potencijalni bezbednosni propusti

(<http://www.nextgov.com/cybersecurity/2015/05/third-party-software-was-entry-point-background-check-system-hack/112354/>, 2015.) Iz izveštaja koje je sproveo Verzion prošle godine na prva tri mesta napada cyber špijunaže se nalaze kompanije koje pružaju usluge velikim organizacijama, proizvodnjama i vladi.

## 5. ZAŠTITA SAP ERP SISTEMA

Da bi lakše razumeli kompletnu oblast bezebednosti u okviru SAP ERP sistema potrebno je pre svega navesti da SAP ERP sistemi koriste sisteme autentifikacije kao i mehanizme upravljanja korisnicima koji se koriste u okviru SAP NetWeaver platforme i SAP NetWeaver aplikativnog servera (Linkies i Off, 2006). Iz tog razloga da bi se zaštita što bolje sprovele preporuka je da se prilikom sprovođenja zaštite izvrši provera paramatera i u okviru SAP NetWeavera.

Napadač može izvršiti neovlašćeni pristup sistemu uz pomoć poznatih korisničkih kredincijala. Jednom kad načini ovakav pristup može izvršavati sve akcije koje su dozvoljene tom korisniku. Na taj način ukoliko korisnik ima pristup poverljivim informacijama onda će i osoba koja ovim putem pristupa sistemu takođe imati pristup tim istim informacija (Mohay,

Anderson, Collie i DeVal, 2003). Iz ovog razloga veoma je bitno obezbediti sigurnu i kvalitetnu autentifikaciju kako bi se izvršila zaštita integriteta kompletnog sistema na svim mogućim nivoima. SAP podržava nekoliko mehanizama za autorizaciju korisnika i obezbeđuje Single Sign-On okruženje koje omogućava samo jedno logovanje prilikom korišćenja sistema.

## **5.1. Prijavljivanje i šifre kao zaštita u SAP sistemu**

Prijavljivanje na SAP sistem se vrši uz pomoć korisničkog naloga koji se sastoji od korisničkog imena i šifre. Radi podizanja bezbednosti na veći nivo sve šifre u okviru SAP-a su enkriptovane i čuvaju se i prenose isključivo samo u hash vrednosti. Kada je izvršena update SAP NetWeaver-a, u svakoj verziji posle 6.40 hash algoritam šifre je promenjen sa MD5 na SHA-1 (Fernandez i Pan, 2001). Ovakva promena je nastala da bi se zaštita podigla na viši nivo i da bi se mogućnost obrnutog inženjeringa kojim bi se možda ostvarila mogućnost za otkrivanje šifre svela na minimum. Nakon update-a sistem je počeo da proizvodi dve hash vrednosti iz razloga što stare hash vrednosti nisu bile kompatibilne sa novim sistemom. Sistem se može podesiti tako da generiše samo nove vrednosti hash-a. Prilikom prijave na sistem, sam sistem proverava hash vrednost unete šifre sa bazom podataka korisnika i upoređuje te dve vrednosti (Hirao, 2008). SAP sam generiše koji će deo hash vrednosti proveravati, ukoliko nastane podudaranje hash vrednosti pristup je odobren, ukoliko ne nastane prijava je odbijena. Ova novonastala promena nema nikakve posledice po način funkcionisanja sistema ili po performanse sistema. Jedina razlika koja je napravljena je ta da ukoliko postoji potreba za ovom vrstom hash vrednosti, neophodno je da postoje još dve komponente u sistemu (Fernandez, Mujica i Valenzuela, 2011). To su Communication Framework koji služi za transfer i skladištenje šifri i Central User Administration čija je uloga da raspoređuje hash vrednosti šifre.

Prilikom prijave na SAP sistem korisnik mora da unese korisničko ime i šifru. U trenutku pre nego što se korisniku odobri pristup na SAP sistem, sam sistem proverava sledeće parametre:

- Da li korisnik poseduje šifru i da li je moguće logovanje sa njom
- Da li je korisnički nalog zaključan i da li ima pravo pristupa ( Administrator ima pravo da korisniku zaključa nalog kao što i sam sistem može zaključati nalog ukoliko korisnik pokuša više puta da se neuspešno prijavi na sistem.)
- Da li su korisničko ime, šifra i klijent ispravni

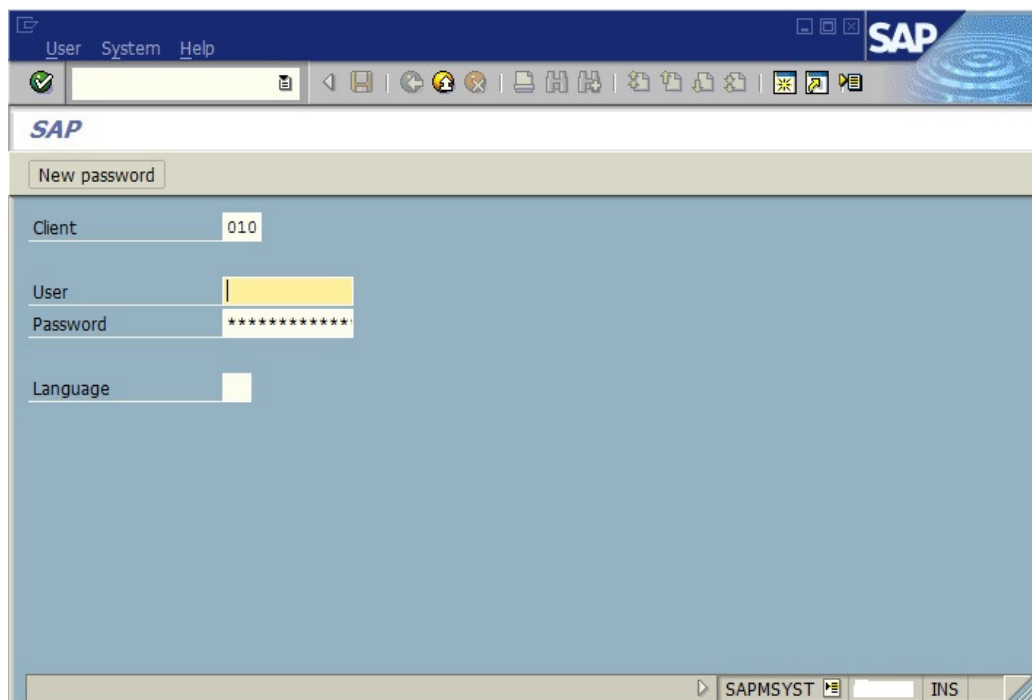


Image 8 -- Client SAP Log In screen

Kada se uspešno prijavi na sistem, sam sistem će ispisati datum korisničkog poslednjeg prijavljivanja na sistem. Uvid u te podatke moguće je ostvariti u delu System -> Status. Ova opcija omogućava korisniku da može da proveri da li je bilo nekog sumljivog pristupa na sistem. Podaci o pristupu na sistem ne mogu se menjati u okviru sistema, takođe i sam sistem ne vrši čuvanje vremena kada je neko izvršio odjavu sa sistema ([https://help.sap.com/saphelp\\_nw73/helpdata/en/48/3a0638902131c3e10000000a42189d/content.htm?frameset=/en/4a/c3f18f8c352470e10000000a42189c/frameset.htm&current\\_toc=/en/b9/24b7ba9cb0421e915b8414422804e8/plain.htm&node\\_id=5&show\\_children=false](https://help.sap.com/saphelp_nw73/helpdata/en/48/3a0638902131c3e10000000a42189d/content.htm?frameset=/en/4a/c3f18f8c352470e10000000a42189c/frameset.htm&current_toc=/en/b9/24b7ba9cb0421e915b8414422804e8/plain.htm&node_id=5&show_children=false), 2016).

### 5.1.1. Inicijalna šifra i pravila provere

Kada nastane zahtev za kreiranje novog korisnika u okviru sistema potrebno je prilikom pravljenja novog korisnika napraviti i inicijalnu šifru. Šifra mora da ispunjava određenje uslove koje su predefinisane u samom sistemu. Osnovni uslovi koji su potrebni da se ispune prilikom kreiranja šifre su sledeća ([https://help.sap.com/saphelp\\_nw73/helpdata/en/4a/c3f18f8c352470e10000000a42189c/content.htm](https://help.sap.com/saphelp_nw73/helpdata/en/4a/c3f18f8c352470e10000000a42189c/content.htm), 2016):

- Šifra mora da sadrži najmanje 3 karaktera
- Šifra ne može biti duža od 40 karaktera do verzije 6.40, nakon te verzije do 8 karaktera
- Do verzije 6.40 bila je mogućnost koristiti slova, brojeve i neke znakove i sistem nije razlikovala mala i velika slova
- Nakon verzije 6.40 moguće je koristiti bilo koji Unicode karakter i sistem razlikuje mala i velika slova
- SAP Web AS 6.10 i kasnije verzije podržavaju da administrator može definisati koji broj karaktera je potreban za šifru kao i koje vrste karaktera je pod obavezno koristiti
- Prva tri karaktera šifre ne smeju biti istim redom kao ona koja su u upotrebi za korisničko ime

- Prva tri karaktera ne smeju biti ista
- Ni jedno od prva tri karaktera ne sme biti razmak
- Šifra ne sme biti „PASS“ ili „SAP“
- Korisnik ne može postaviti novu šifru kao neku koja je bila ranije osim ukoliko mu administrator ne vrati šifru na neku od prethodnih. Istorija šifri je do 100 šifri po korisniku
- Šifru je moguće promeniti isključivo kada se stara šifra tačno unese (Do verzije SAP Web AS 6.10 šifru je moguće promeniti isključivo prilikom logovanja dok je nakon SAP Web AS 6.20 moguće promenu izvršiti u postavkama System -> User profile -> Own data ili uz pomoć transakcije SU03)
- Korisnik može sledeći put promeniti šifru tek nakon određenog vremenskog perioda, vremenski period je jedan dan. U periodu od ovog jednog dana jedino administrator može da promeni šifru i to na inicijalnu vrednost koju će korisnik morati da promeni odmah prilikom sledećeg prijavljivanja na sistem.
- Šifra mora sadržati bar po jedno malo i veliko slovo
- Nova šifra mora da se razlikuje najmanje po jednom karakteru u odnosu na prethodnu šifru

Svaki pristup sistemu pokreće niz akcija koje se vrše u cilju provere korisnikovih podataka. U postupku provere šifre postoji brojač neuspelih prijave koji se svaki put uvećava kada je porvera šifre neuspela. Takođe kada korisnik menja svoju šifru u obavezi je da unese prvo prethodnu šifru, sistem će prvo izvršiti proveru stare šifre i ukoliko je ona netačna, brojač neuspelih prijave će se uvećati. Onog trenutka kada brojač dostigne određenu vrednost, korisnički nalog će se po automatizmu zaključati. Postupak u kom će se korisnikom nalog zaključati biće evidenitiran u Security Audit Log-u u okviru Syslog-a. Brojač će se automatski resetovati prilikom uspešne porvere šifre tokom prijave na sistem ili nakon uspešne promene šifre ili nakon jednog dana, u slučaju kada je to potrebno administrator može i ranije otkloniti zabranu. Kada administrator izvrši zaključavanje korisnikovog naloga ta vrsta zaključavanja neće biti evidentirana u okviru Security Audit Log-a (Van der Aalst i de Medeiros, 2005).

Onog trenutka kada korisnik unese pogrešnu šifru prilikom prijave na sistem, sam sistem će mu omogućiti još dva pokušaja pre nego što dođe do zaključavanja naloga. Ukoliko korisnik nastavi da unosi pogrešnu šifru i sama konekcija sa SAP GUI-jem će biti prekinuta. Prekid po osnovnim podešavanjima bi trebalo da nastane nakon 3 pokušaja ali je moguće izmeniti ova podešavanja u okviru loginfails\_to\_user\_session\_end (Chuprunov, 2013).

### 5.1.2. Secure Network Communications i Single Sign-On

Osim tradicionalnog načina prijave na sistem uz pomoć korisničkog imena i lozinke, postoji mogućnost korišćenja Secure Network Communication-a (SNC). Ovaj način komunikacije koristi eksterne zaštite kako bi izvršio autorizaciju. Jedan od vidova kada se koristi SNC komunikacija je ostvarivanje komunikacije između SAP GUI za Windows i aplikativnog servera. Nivo zaštite koji će biti ostvaren ovom metodom zavisi od više uslova, kao na primer šta je cilj zaštite, tip infrastrukture i zaštitne mere koje ta eksterna zaštita pruža. Kada govorimo o ovom rešenju jedan od vidova zaštite predstavlja upotreba PKI (public-key infrastructure) ključeva kod koje se mora voditi računa o dve stvari, na koji način bi se generisali i distribuirali ključevi do korisnika, kao i na koji način bi korisnici čuvali ključeve ([http://help.sap.com/saphelp\\_nw73ehp1/helpdata/en/aa/38ff4fa187622fe10000000a44176d/content.htm](http://help.sap.com/saphelp_nw73ehp1/helpdata/en/aa/38ff4fa187622fe10000000a44176d/content.htm), 2016).

Postoje dva načina na koje je moguće izvršiti čuvanje ključeva:

- Hardware-sko čuvanje
- Software-sko čuvanje

Hardware-ski način čuvanja bi predstavljao oblik čuvanja u kome bi ključevi bili ubačeni smart kartice ili crypto kutije

([https://help.sap.com/saphelp\\_nw70/helpdata/en/4d/bf6f77a2c5446a86e0152f1b309db6/content.htm](https://help.sap.com/saphelp_nw70/helpdata/en/4d/bf6f77a2c5446a86e0152f1b309db6/content.htm), 2016). Na ovaj način čuvanja bi se svakom korisniku izdavala fizička kopija privatnog ključa. Ključ bi bio sačuvan na pametnoj kartici koja poseduje mehanizme za neoktrivanje ključa. Korisnik vrši pristup tako što uz pomoć biometrije se potvrđuje njegov indentitet koji je vezan za pametnu karticu, takođe pored biometrije kao što bi bio otisak prsta može se koristiti i PIN šifre. Uz pomoć pametnih kartica korisnici takođe mogu da izvrše i digitalno potpisivanje i kao kriptovanje podataka (Hirao, 2008). Problem koji nastaje kod hardware-ske zaštite je u tome što je na korisniku ostavljena ta odgovornost da čuva karticu od krađe i da pazi da je izgubi. Veoma je važno izvršiti edukaciju zaposlenih da čuvaju svoje kartice kao i to da svoju karticu ne dele sa drugim zaposlenima.

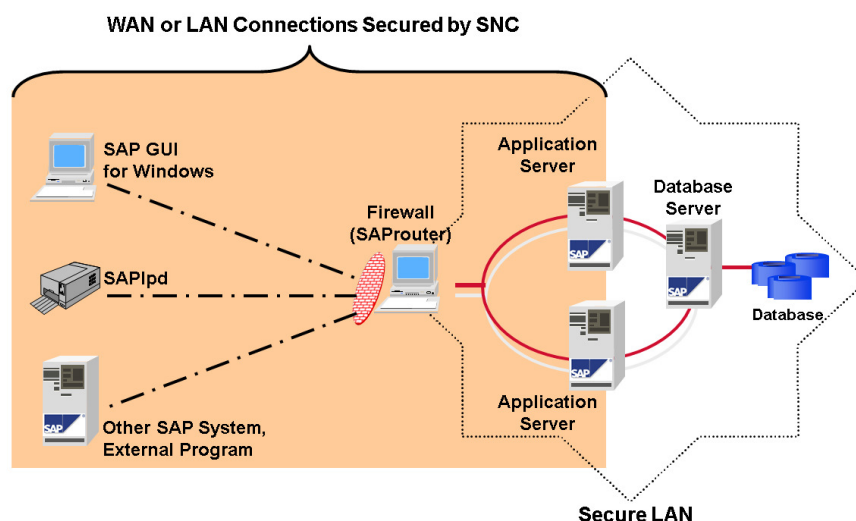


Image 9 - Secure Network Communications vizuelna prezentacija

Software-sko rešenje bi predstavljao drugi način na koji je moguće izvršiti čuvanje privatnog ključa. Ovaj način čuvanja ne predstavlja toliko siguran metod kao što je hardware-ski način ali zato daleko umanjuje troškove jer nije potrebno izvršiti fizičko izdavanje kartice svakom korisniku pojedinačno.

Ovaj način prijave i Secure Network Communications se inače mogu nazvati Single Sign-On i predstavljaju deo tog rešenja (Boettcher, Daiberl, Fischer, i Liu, 2007). Za cilj Single Sign-On im baš to da korisnik nema potrebu da se više od jednom autorizije na sistem, čak i u uslovima kada radi na više sistema istovremeno. Svrha ovih načina prijave bilo ona hardware-ska ili softwar-ska je u tome da se prilikom prijave na sistem kreiraju kredencijali korisnika koji će predstavljati korisnika kroz celi sistem. Na ovaj način se podaci o korisniku kao što su šifra i korisničko ime ne šalju kroz sistem, već kroz sistem prolazi samo verifikacija koja postavlja upit da li je korisnik ostvario i da li ima autorizaciju. Postoji još jedan metod autorizacije koji je često u upotrebi kada je potrebno ostvariti prijavu koršćenjem Web aplikacije preko SAP WEB-a

(<http://searchsecurity.techtarget.com/tip/SAP-Security-Authentication-and-single-sign-on>, 2016). Tada se koristi X.509 client sertifikat da bi se izvršila autorizacija korisnika. Kada

korisnik vrši autorizaciju ovim putem tada se preko SSL protokola vrši provera njegove identiteta tako da slanje šifre nije obavezno u ovom slučaju. Prilikom korišćenja X.509 sertifikacije i SSL protokola jako je važno izabrati pouzdan digitalni sertifikat ili kreirati lični koji će biti distribuiran korisnicima kako bi mogli da se prijave na sistem. U slučaju korišćenja ovog načina prijave jedna stvar je obavezna, a to je upotreba Secure Network Communications-a iz razloga što se sama autorizacija obavlja na Web serveru, a ne u samom SAP sistemu. Prijava se sastoji od dva elementa, javnog ključa koji je čuvan u okviru X.509 i privatnog ključa koji poseduje korisnik. Prilikom prijave na sistem dolazi do poređenja ova dva ključa i ukoliko postoji pozitivna potvrda korisnik se pušta na server (Wood, Norton, Weschler, Ferris, & Wilson, 2005). Privatni ključ koji se nalazi kod korisnika je potrebno adekvatno obezbediti, u ovom slučaju to zavisi od zaštite koju koristi Web pregledač koji koristi korisnik.

## **6. SAP R/3 KONCEPT AUTORIZACIJE**

ERP sistemi su nastali sa idejom da se na jednom mestu integrišu sva poslovanja, polazeći od finansija, planiranja, proizvodnje, marketinga i prodaje. Što je jedno preduzeće veće, veći je i sam sistem. Kako sistem raste tako i administracija ovlašćenja i pristupa je sve više kompleksnija. Razlog obrade ove verzije je u tome što danas u svetu postoji veliki broj SAP ERP instalacija (veruje se da premašuje brojku od 100.00), iako postoje i novije verzije ovog software-a, baš ova je ta koja je najčešća od ukupnog broja instalacija. Autorizacija u SAP R/3 sistemu ima višestruku namenu koja se ogleda pre u svega zaštiti od slučajne ili namerne zloupotrebe podataka. Druga namena autorizacije je da sve podatke koji su raspoloživi u sistemu drži u tajnosti. SAP R/3 definiše ovlašćenja za svakog korisnika pojedinačno. U tim ovlašćenjima je definisano šta svaki od korisnika ima pravo da radi i kojim datotekama i podacima da pristupa. Sam koncept autorizacije mora u velikoj meri da bude adaptibilan i da pruža mogućnost preduzeću da kako se širi, vrši izmene u autorizaciji (Little and Best, 2003). Prema autorima Appelrath i Ritter (2013) autorizaciju možemo klasifikovati u tri nivoa:

- Prvi nivo se naziva Business process layer koji se odnosi na deo gde jedna kompanija odlučuje o propisima i ograničenjima koje će se primenjivati u okviru jednog poslovnog procesa u njenom sistemu. Kao primer osnovnog poslovnog procesa, možemo navesti proces kupovine. Određena preduzeća imaju uglavnom način rada u kojima se na određeni način ograničavaju različite akcije ili zabranjuju aktivnosti određene osobe. Ograničenje može biti na primer da osoba koja je napravila zahtev za plaćanje i kupac moraju biti dve različite osobe. Tako u SAP R/3 sistemu podnosiocu zahteva za plaćanje nije dozvoljen pristup kreiranju porudžbine u okviru sistema.
- Drugi nivo bi se odnosio na deo gde se vrše podešavanja autorizacije. U njima se tačno definiše da li je određenoj osobi dozvoljeno da izvrši određenu akciju ili nije. Autorizacije u okviru SAP R/3 dodeljuje se korisnicima u vidu uloga tj. profila.
- Treći nivo zadužen je za proveru autorizacije u samom sistemu. Provera autorizacije se dešava na nivou programskog koda koji su dostupni u okviru SAP R/3 sistema.

Prednost SAP R/3 sistema se ogleda u tome što je svaki od ova tri nivoa lako prilagodljiv zahtevima korisnika. SAP R/3 sistem u svom posedu ima više alataka koje se mogu koristiti (Missbach et al., 2013). Dve značajne koje se odnose na autorizaciju su Virsa Compliance Calibrator i Virsa Role Expert.

Virsa Compliance Calibrator je alat koji pruža mogućnost da se vrši interno nadgledavanje oko 200 rizika koje pokrivaju hiljade standardnih transakcija koje se odvijaju u okviru SAP-a. Virsa Compliance Calibrator na osnovu ovih parametara sprovodi testiranje dužnosti, skenira da li postoje povrede određenih dužnosti i na specifičan način pronalazi rešenja za njihovu sanaciju. Uz sve navede stvari, pomenuti alat se bavi i analizom rizika. Ukoliko dođe do otkrivanja nepoželjnih proboja tokom izvršavanja, alat će alarmirati odgovorno lice koje je unapred predefinisano. Jedna od prednosti još ovog alata je što sam vrši simulaciju napada i predlaže rešenja za bolju zaštitu ukoliko primeti određene ranjive tačke, na primer odvajanje dužnosti kod provere faktura (Proctor, Heiser i MacDonald, 2007).

Virsa Role Expert je alat koji se koristi da bi se napravili određeni profili i uloge i njima upravljalo. Virsa Role Expert ima ulogu i u proveravanju da li postoji podudaranje pravila dodeljena novom korisniku sa bazom pravila.

Osnovna komponenta u SAP R/3 sistemu za autorizaciju se naziva SAP Web Application Server koja je raniji prethodnih SAP NetWeaver. Ove dve komponente su u velikoj meri identične i funkcionišu na istom principu.

Da bi lakše razumeli autorizaciju osvrnućemo se na transakcije koje se sprovode u okvirima baza podataka. Transakcije u bazama podataka sastoje se od više manjih operacija koje moraju sve zajedno kao grupa proći odobrenje ili će u suprotnom biti neuspele. Transakcije se slično obavljaju i u SAP R/3 sistemu. Kada govorimo o zaštiti i autorizaciji u okviru ovog sistema, za svaki program postoji određen identifikacioni broj. Taj broj se drugačije naziva transakcioni kod. Prilikom svakog pozivanja programa, on prolazi kroz transakcionu proveru i kojoj se kod proverava. Ovo je definisano klasičnim „IF“ naredbama. Proces provere autorizacije počinje onog trenutka kada bilo koji od korisnika pokrene zahtev da pristupi određenoj transakciji. Prilikom pokretanja zahteva, prva stavka koja se obavlja je provera da li se korisnikovi kredencijali poklapaju sa podnetim zahtevom. U koliko dođe do poklapanja tada se korisniku koji je podneo zahtev omogućava pristup informacijama koje su bile zaštićene.

Proces autorizacije kao takav možemo podeliti u dva dela. Prvi deo bi se odnosio na proces u kome dolazi do provere da li postoje određene autorizacione informacije u okviru profila korisnika, dok drugi deo predstavlja poređenje tih autorizacionih informacija koje se nalaze u profilu sa bazom podataka u kojoj su pohranjene vrednosti autorizacije. Proces autorizacije je uspešan onda kada se oba dela procesa autorizacije završe sa pozitivnim ishodom (Fletcher, Brahm i Pargmann, 2003).

Čovek u svim domenima svog života teži ka što većem ostvarivanju nivoa bezbednosti i zaštite. Sam termin autorizacija nastaje u cilju da se spreči svaki nedozvoljen pristup. Autorizacija u okviru SAP R/3 sistema se odnosi na zaštitu svih transakcija i programa od neovlašćenog pristupa i korišćenja. Administrator je taj koji odlučuje ko od korisnika ima pravo da pristupi kojim programima i transakcijama. Prilikom svakog pozivanja transakcije ili programa vrši se provera autorizacije prilikom koje se proverava da li su korisniku dodeljena određena ovlašćenja kako bi mogao da izvrši željenu transakciju. Dve alata koja su značajna administratoru za sprovođenje kontrole pristupa su Profile Generator i Authorization Infosystem (Lamotte-Schubert i Weidenbach, 2009). Pored ove dve stavke u okviru SAP R/3 sistema postoji još niz procesa koji se odnosi na zaštitu i proveru bezbednost. Dalje u tekstu ćemo navesti neka najvažnija.

- **SAP R/3 autorizacija transakcija**

Kako smo već naveli ovaj proces služi da proveriti da li korisnički nalog raspolaže sa svim potrebnim ovlašćenjima koje su potrebne da se transakcija izvrši

- **Specifična autorizacija za transakcije**

Pored gore navede provere transakcija prilikom njenog pokretanja postoji i dodatna provera transakcija u SAP sistemu. Prilikom kreiranja transakcije od strane konsultanta koji vrši implementaciju SAP rešenja, moguće dodati dodatne provere za kreiranu transakciju.

- **Provera autorizacija na programskom nivou**

Kada govorimo o ovoj vrsti autorizacije ona predstavlja kompleksniju vrstu zaštite iz razloga što se vrši na nivou koda samog programa. Ovo je način koji je često u upotrebi od strane SAP programera kada je za određene stvari potreban visok stepen zaštite.

- **Izveštaji klasa i tabela autorizacionih grupa**

Kako bi podigli bezbednost i zaštitu na zavidan nivo takođe jedna od opcija koja nam je na raspolaganju je postavljanje zahteva za pravljenje izveštaja i tabela autorizacionih grupa.

## **6.1. Profile Generator**

Kako smo naveli u tekstu kada je pitanja autorizacija u okviru SAP R/3 sistema dve vodeće stvari su Profile Generator i Authorization Infosystem. Profile Generator je alatka u okviru SAP R/3 sistema koja omogućava administratoru sistema da automatizuje određene stvari koje se odnose na autorizaciju (Hernandez, 1999). Sama ideja generatora profila jeste da ne razmišlja u klasičnom tehničkom pravcu već da se konfigurišu aktivnosti, zadaci i uloge. Da bi se profile generator ispravno koristio neophodno je definisati potrebe kompanije i od jedne veće celine kao takve krenuti sa definisanjem sve manjih i manjih pojmova i na taj način doći do jednog korisnika i definisanja njegovog posla, grupe kojoj pripada kao i transakcija i programa koje su mu potrebne za uspešno izvršavanje posla i zadataka.

## Profile Generator: Steps

|                               |                                     |
|-------------------------------|-------------------------------------|
| Define Role Name              | <input checked="" type="checkbox"/> |
| Determine Activities          | <input type="checkbox"/>            |
| Design User Menus             | <input type="checkbox"/>            |
| Maintain Authorization Data   | <input type="checkbox"/>            |
| Generate Authorizaion Profile | <input type="checkbox"/>            |
| Assign Users                  | <input type="checkbox"/>            |
| Adjust User Master Records    | <input type="checkbox"/>            |

© SAP AG 1999

Image 10 - Generisanje profila SAP R/3

Upotrebom generatora profila značajno je olakšan način na koji se administracija autorizacija obavlja. Takođe on predstavlja jednu od novina koju je doneo SAP R/3 sistem i dostupna je počevši od verzije 3.1 (Manara i Cavalleri, 2012).

## 6.2. Authorization Infosystem

Authorization infosystem je u uskoj vezi sa alatom generator profila i njegova uloga u sistemu jeste da omogući uvid u autorizacije, profile, korisnike i autorizacione dodele. Pružajući ovakve informacije uz veoma jednostavnu proceduru, administratoru sistema je značajno olakšan posao. Authorization Infosystem pruža administratoru uvid kroz hijerarhijski prikaz tj. prikaz u obliku stabla (Appelrath i Ritter, 2013). Uz pomoć ove alatke moguće je zahtevati različite liste sa informacijama kao što su:

- Pregled korisnika sa autorizacijama
- Pregled specifičnog korisnika i njegove autorizacije
- Pregled svih autorizacija
- Poređenje profila
- Transakcije koje su na raspolaganju korisniku za izvršenje
- Promene u okviru autorizacija za specifičnog korisnika

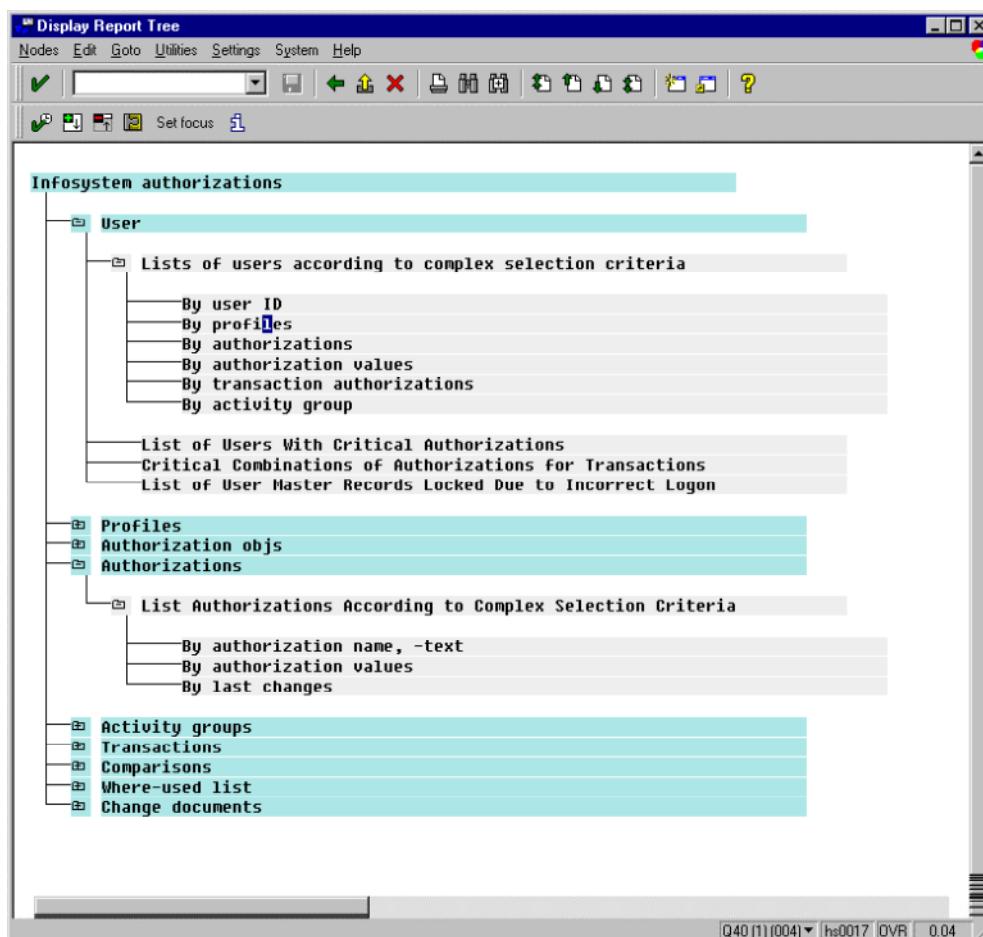


Image 11 - Authorization Infosystem prikaz

Na ovaj način moguće je veoma lako izvršiti uvid u sve potrebne informacije koje su izlistane na veoma pregledan način. Kao i generator profila tako Authorization Infosystem je novina koju donosi SAP R/3 sistem i dostupna je takođe od verzije 3.1.

## 7. Zaštita mreže

Kada govorimo o bezbednosti veoma je važno kada krenemo u njenu implementaciju da razmotrimo sve moguće vidove i oblike pretnji koji mogu da nas ugroze. Uzimajući takve stvari u obzir važno je da razumemo koliko je mreža bitna za zaštitu jednog sistema. Iz tih razloga potrebno je sagledati mrežnu infrastrukturu sa svih aspekata. Svaka kompanija ima određene potrebe i zahteve kada su mreže i komunikacije u pitanju i te potrebe i zahtevi moraju biti u skladu sa tim da se obezbedi da ne dođe do neovlašćenog pristupa mreži. Sa druge strane potrebno je obezbediti onaj nivo zaštite koji je potreban, a nikako ići korak dalje u procedurama i nivoima zaštite jer to koliko može da pomogne sa druge strane može da usporu produktivnost jedne kompanije ukoliko postoje suvišne procedure (Sorsa, 2007). Dve komponente su zadužene za bezbednost u okviru SAP sistema, jednu koji smo već spominjali, a to je Secure Network Communications (SNC) i druga SAProuter. SAProuter možemo definisati kao oblik proxy-ja na aplikativnom nivou koji se može koristiti u uskoj vezi sa klasičnom firewall zaštitom kako bi se obezbedila zaštita od neovlašćenog ulaska na sistem (Sel i Van Der Auwera, 2010). Cilj svake firewall zaštite je da se odvrte napadi koji su usmereni na neovlašćeni pristup mreži koja se štiti. Problem je u delu gde je potrebno otvoriti firewall zaštitu kako bi omogućili pristup željenim komunikacijama. U ovom delu na scenu

stupa SAProuter koji je moguće koristiti kao vid zaštite koji će obavljati funkciju kontrole pristupa. SAP router je u mogućnosti da vrši dozvolu ili zabranu pristupa određenih korisnika ili računara. U uskoj korelaciji sa firewall zaštitom SAProuter predstavlja veoma uspešnu zaštitu SAP sistema u okviru LAN mreže (Hague, 2014). SAProuter se može koristiti u sledećoj primeni:

- Kontrolisanje konekcija na SAP sistem i pravljenje logova svih pristupa
- Zaštita komunikacija od neovlašćenih pristupa
- Povećavanje performansi samog SAP sistema
- Omogućava postavljanje indirektnih veza između dva programa kada imaju problem u komunikaciji zbog različitih postavki mreže

Secure Network Communications kako smo ranije spomenuli ima ulogu da obezbedi mogućnost upotrebe drugim sistemima zaštite kao što su: Single Sign-On, Pametne kartice, itd. Kod ovih stvari je važno napomenuti da one nisu uključene od strane SAP software-a i da ih je potrebno nabaviti od drugih proizvođača koji su sertifikovani od strane SAP-a. Još jedna važna funkcija Secure Network Communications je zaštita na aplikativnom nivou. Ovo podrazumeva da će Secure Network Communications obezbediti zaštitu u komunikaciji između dva različita programa SAP-a. Secure Network Communications je u stanju da obezbedi sigurnu vezu između svih SAP R/3 aplikativnih servera, svih klijenata i SAProuter-a. Nedostatak SNC je u tome što nije u mogućnosti da obezbedi sigurnu vezu između aplikativnih servera i baze podataka i iz tog razloga je potrebno obezbediti dobru i sigurnu LAN mrežu (Cohrs i Kirschenmann, 2015).

## 8. SSF mehanizmi i digitalni potpisi

Nastavljajući svoj razvoj na sistemima zaštite SAP je u okviru svojih software-a uveo mogućnost Secure Store & Forward (SSF) mehanizama i digitalnih potpisa. Sa razvojem na software-u i dolazećom verzijom 4.0 SAP R/3 sistema ove funkcije su bile omogućene kao dodatni mehanizmi zaštite. Bezbednost koju pružaju ovi mehanizmi ogleda se u tome da podaci ostaju zaštićeni i u trenutku kada se više ne nalaze u okviru SAP R/3 sistema. Kada je SAP sistem dostigao verziju 4.5 u sebi je imao uključen SAPSECLIB (SAP Security Library) koja je bila zadužena za ostvarivanje SSF funkcije. SSF u cilju zaštite dokumenata koristi digitalne potpise i digitalne kovertke. Prednost samih digitalnih potpisa ogleda se u tome što su oni po svojoj prirodi jedinstveni, ne mogu se zaboraviti i njihovo kopiranje je teško ostvarljivo

([https://help.sap.com/saphelp\\_nw70ehp2/helpdata/en/b8/821ff4dadd11d2a60a0000e835363f/content.htm](https://help.sap.com/saphelp_nw70ehp2/helpdata/en/b8/821ff4dadd11d2a60a0000e835363f/content.htm), 2016). Upotreba digitalne kovertke funkcioniše na taj način da korisnik koji pravi digitalnu kovertku poseduje dva ključa koja imaju sledeća obeležja:

- Ključevi su usko povezani i moraju biti par
- Jedan ključ se ne može napraviti na osnovu drugog
- Jedan ključ je javan i onaj koji prima poruku mora da bude svestan njegovog postojanja kako bi mogao da izvrši dešifrovanje poruke pre nego što poruku bude u mogućnosti da pročita

Takođe, digitalni potpisi se mogu kreirati uz pomoć privatnih ključeva

([https://help.sap.com/saphelp\\_nw70ehp2/helpdata/en/40/8a0b37e44d7c2fe10000009b38f889/content.htm?frameset=/en/d9/440b37dd3e9e15e10000009b38f936/frameset.htm&current\\_toc=/en/58/251a355d0c4d78e10000009b38f83b/plain.htm&node\\_id=28&show\\_children=false](https://help.sap.com/saphelp_nw70ehp2/helpdata/en/40/8a0b37e44d7c2fe10000009b38f889/content.htm?frameset=/en/d9/440b37dd3e9e15e10000009b38f936/frameset.htm&current_toc=/en/58/251a355d0c4d78e10000009b38f83b/plain.htm&node_id=28&show_children=false), 2016). Lice koje poseduje privatni ključ u obavezi da je privatni ključ drži obezbeđen i na sigurnom kako niko ne bi mogao da izvrši neautorizovan pristup ključu. Dokle god je ključ bezbedan, mogu se kreirati potpisi koje nije moguće verodostojno kopirati. Da bi se potpis izvršio kada je to potrebno, ono što je prvo potrebno uraditi je dozvoliti pristup sistemu vašem privatnom ključu. Privatni ključevi mogu biti čuvani na tokenima, pametnim karticama ili nekim drugim uređajima i prilikom njihovog korišćenja prvo je potrebno uneti PIN kod ili šifru kako bi sistem mogao da izvrši digitalni potpis. Samo kada je javni ključ prepoznat i kada dođe do pozitivnog poklapanja između javnog i privatnog ključa može doći do uspešnog potpisivanja. Da bi se potvrdila autentičnost digitalnog potpisa i integritet podataka izvršiće se procedura u kojoj će se jedna hash vrednost primeniti poruku i dobijeni rezultat će biti upoređen sa kratkim prikazom poruke. Ukoliko se dva prikaza u potpunosti poklapaju onda je digitalni potpis potvrđen i verifikovan. Pored osnovne verifikacije postoji i dodatni sistem zaštite koji funkcioniše na taj način da ukoliko se uoče bilo kakve promene na digitalnom ključu ili dokumentu nakon verifikacije digitalnog potpisa, verifikacija će onda postati neuspešna

([https://help.sap.com/saphelp\\_nw70ehp2/helpdata/en/b8/821feedadd11d2a60a0000e835363f/content.htm?frameset=/en/8d/517619da7d11d1a5ab0000e835363f/frameset.htm&current\\_toc=/en/58/251a355d0c4d78e10000009b38f83b/plain.htm&node\\_id=35](https://help.sap.com/saphelp_nw70ehp2/helpdata/en/b8/821feedadd11d2a60a0000e835363f/content.htm?frameset=/en/8d/517619da7d11d1a5ab0000e835363f/frameset.htm&current_toc=/en/58/251a355d0c4d78e10000009b38f83b/plain.htm&node_id=35), 2016).

Svrha digitalnih koverti je u tome da samo određeni primalac ima pravo da pročita sadržaj poruke. Postupak kreiranja digitalne koverta je takav da se korisiti poseban tajni ključ kako bi se kompletan sadržaj poruke enkriptovao i na taj način se stvorio digitalno zaštićen dokument. Primalac poruke mora da bude svestan i upoznat sa tim da poruku koju prima je enkriptovana i da pored toga ima dovoljno znanja i iskustva da bi mogao da izvrši njeno dekriptovanje kako bi mogao da pročita poruku. Tajni kod koji se koristi prilikom enkriptovanja poruke je ništa drugo nego javni ključ koji je dodeljen primaocu i koji se šalje zajedno sa porukom, a primalac koristi svoj privatni kod kako bi izvršio dekriptovanje poruke.

## 8.1. Infrastruktura javnih ključeva

Kako bi upotreba digitalnih potpisa i digitalnih koverti uopšte bila moguća neophodno je obezbediti infrastrukturu javnih ključeva (Vacca, 2004). Glavna svrha infrastrukture javnih ključeva je da obezbedi generisanje i distribuciju ključeva koji se nalaze u paru. Postoje nekoliko načina da se uspostavi ova infrastruktura, kao i nekoliko uslova. Iz razloga što još uvek u svetu ne postoji globalni servis koji bi generisao ključeve postoje dve opcije. Prva opcija bi bila uspostavljanje svog ličnog sistema tj. infrastrukture za generisanje ključeva. Ovaj metod može da se susretne sa određenim ograničenjima u vidu broja ključeva koje je moguće generisati kao i kompatibilnosti sa eksternim sistemima zaštite koji su u upotrebi. Još jedan od problema sa kojima se susreće lična infrastruktura za generisanje ključeva je ta da i kada se uspostavi nastaje problem njenog povezivanja između korisnika i biznis partnera koji je

koriste

([https://help.sap.com/saphelp\\_nw70ehp2/helpdata/en/8d/51761cda7d11d1a5ab0000e835363f/content.htm](https://help.sap.com/saphelp_nw70ehp2/helpdata/en/8d/51761cda7d11d1a5ab0000e835363f/content.htm), 2016). Druga opcija za uspostavljanje infrastrukture je angažovanje treće kompanije koja se bavi ovim poslom i koju su zvanični provajder ovakvih usluga. Ovaj oblik uspostavljanja infrastrukture u značajno meri smanjuje broj problema koji mogu da nastanu. Funkcionalnost koje pružaju SSF usluge mogu se koristiti u više svrha u cilju čuvanja dokumenata i podataka. Digitalni potpisi imaju širok diapazon primene pogotovo u situacijama gde je potrebno potpisivanje dokumenata koji se ne koriste u papirnom obliku kao što su zahtevi za plaćanje, ugovori, porudžbine (Faltin, Glöckner, Viebeg, Berger, Giehl,

Hühnlein, i Surkau,2013). Kako bi lakše razumeli svrhu, navešćemo neke od klasičnih primera upotrebe ove tehnologije u sklopu SAP R/3 sistema

([https://help.sap.com/saphelp\\_nw70ehp2/helpdata/en/d9/440b37dd3e9e15e10000009b38f936/content.htm?frameset=/en/25/4e0b37cf3e3273e10000009b38f936/frameset.htm&current\\_toc=/en/58/251a355d0c4d78e10000009b38f83b/plain.htm&node\\_id=3](https://help.sap.com/saphelp_nw70ehp2/helpdata/en/d9/440b37dd3e9e15e10000009b38f936/content.htm?frameset=/en/25/4e0b37cf3e3273e10000009b38f936/frameset.htm&current_toc=/en/58/251a355d0c4d78e10000009b38f83b/plain.htm&node_id=3), 2016):

- SSF se koristi od strane određenih aplikacija da izvrše konvertovanje celokupnog teksta iz SAPGUI okruženja u zaštićeni format i kao takav se čuvan u SAP R/3 bazi. Kasnije kada nastane opet potreba za tim podacima, aplikacije iz baze čitaju informaciju, vrše njihovo dekriptovanje uz pomoć SSF tehnologije. Ukoliko su dokumenta koja su enkriptovana potpisana digitalni potpisom, aplikacija može izvršiti proveru i potvrdu digitalnog potpisa.
- Prilikom eksternog transporta ili skladištenja aplikacije će takođe vršiti čitanje podataka iz SAP R/3 baze. Nakon što izvrši očitavanje iz baze i pre nego što izvrši eksterne slanje, aplikacije će obraditi podatke na taj način da će podatke prvo konvertovati u potreban format za eksternu upotrebu, a nakon toga će obezbediti podatke u skladu sa SSF procedurom. Jednom kada sve potrebne informacije za slanje budu obezbeđene sistem će dozvoliti njihovo čuvanje na transportni medij poput USB memorije, CD, memorijske kartice ili slanje preko neosiguranje linije poput Interneta. Prijem se može vršiti na drugom SAP R/3 sistemu ili na bilo kom drugom sistemu koji podržava format obezbeđenog paketa.
- Prilikom prijema digitalno potpisanog i obezbeđenog paketa podataka nekim eksternim putem, aplikacije će izvršiti njegovo čuvanje u okviru SAP R/3 sistema. Ukoliko su podaci obezbeđeni uz pomoć SSF funkcija, aplikacije će biti u mogućnosti da izvrše dekriptovanje podataka ili potrebnu verifikaciju potpisa. Podaci koji pristižu u SAP R/3 sistema ne moraju biti enkriptovani od strane drugog SAP R/3 sistema, ali je potrebno da ta procedura bude izvršena od strane programa koji će enkriptovanje podataka uraditi u nekom od formata koji je podržan od strane SSF-a.

Kada je reč o eksternoj zaštiti podataka SSF podržava PKCS#7 standarde, kao i X.509 sertifikate koje se odnose na zaštitu podataka, njihovo potpisivanje i enkriptovanje. SSF mehanizmi u okviru SAP-a su dostupni od R/3 v.4 sistema, kao i SAPSECULIB koji je dostupan od v.4.5

([https://help.sap.com/saphelp\\_nw70ehp2/helpdata/en/25/4e0b37cf3e3273e10000009b38f936/content.htm](https://help.sap.com/saphelp_nw70ehp2/helpdata/en/25/4e0b37cf3e3273e10000009b38f936/content.htm), 2016).

## 9. Zaštita SAP R/3 Internet aplikacija

SAP R/3 sistem kreira određen broj komponenti koji predstavljaju internet aplikacije uz pomoć kojih korisnik ima mogućnost da vrše biznis operacije u SAP R/3 sistemu tako što će koristiti World Wide Web umesto klasičnog SAPGUI okruženja. SAP kako sistem je predstavljen da bude u službi korisnika, pa ista stvar se odnosi i na internet komponente. Svaku internet komponentu je moguće kastomatizovati da odgovara zahtevima korisnika (Österle, Fleisch & Alt, 2012. Business networking: Shaping enterprise relationships on the Internet. Springer Science & Business Media). Ukoliko ne postoji odgovarajuća internet komponenta takođe je moguće izvršiti razvoj potrebnih komponenti kako bi se odgovorilo na potrebe klijenta. Da bi omogućili rad internet komponenti neophodno je da postoji Internet

transakcioni server čija je uloga da vrši komunikaciju između SAP R/3 sistema i Web-a (Woods & Mattern, 2006).

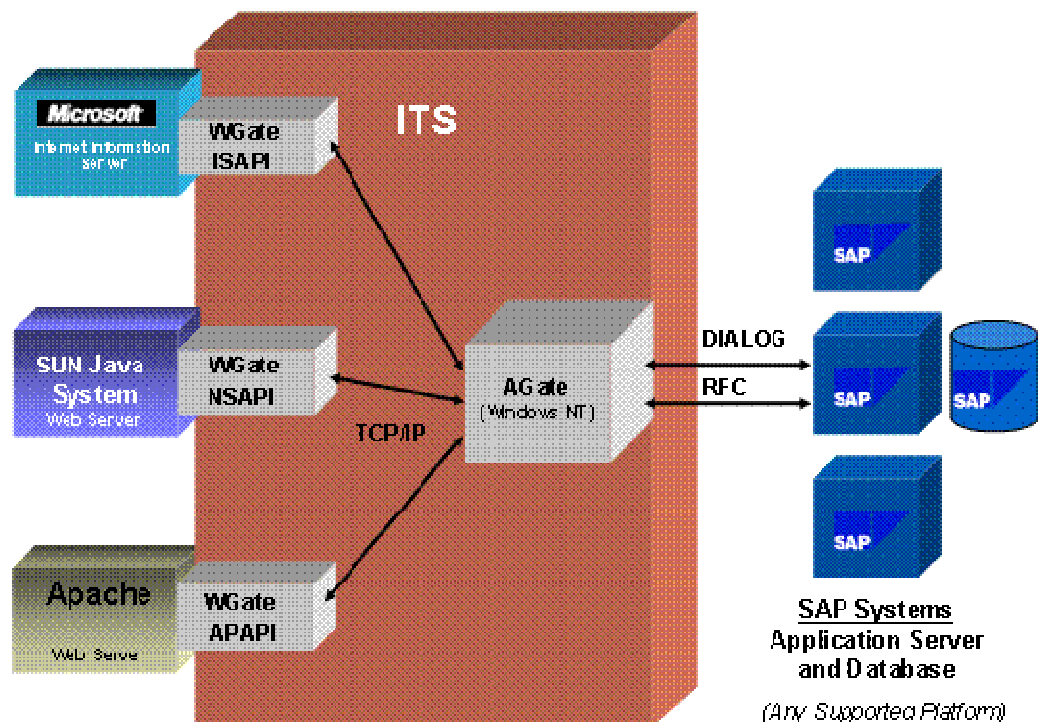


Image 12 - Internet transakcioni server šematski prikaz

Internet transakcioni server omogućava da se SAP R/3 aplikacije pokreću u sigurnom okruženju. Uloga ovog servera je da kontroliše protok podataka i da omogući pristup internet aplikacija SAP sistemu. Arhitektura Internet transakcionog servera se sastoji od dve komponente Wgate-a i Agate-a. Wgate se nalazi na internet serveru i njegova uloga je da ostvaruje konekciju web servera i Internet transakcionog servera. Za razliku od Wgate, Agate se najčešće postavlja u sklopu nekog odvojenog servera i njegova uloga je u ostvarivanju komunikacije između Internet transakcionog servera i SAP R/3 sistema. Agate vrši uspostavu konekcije, generiše HTML dokumenta i vrši kontrolu sesija i pristupa. Kako bi se nivo bezbednosti zadržao na određenom nivou, SAP R/3 internet arhitektura raspolaže sa nekoliko različitih mehanizama zaštite. Jedan od njih je mogućnost da se Wgate i Agate pokreću u okviru različitih hostova (Lam, 2007). Pored ove mogućnost za bezbedan rad u okviru interneta u ponudi je uoptreba različitih firewall-ova, filtera, SAProutera. Upotreba navedenih komponenti koje doprinese poboljšanju bezbednosti su čak i preporuka od samog SAP-a. Iz razloga što se svi podaci kroz internet šalju u vidu običnog teksta prepruka je da se između pošiljaoca i primaoca koristi neki vid enkripcije. Iz tog razloga vrste enkripcije koje je moguće koristiti u okviru Internet transakcionog servera su sledeće:

- Između Web pregledača i Web servera moguće je koristiti SSL vid zaštite
- Između Wgate i Agate moguće je koristiti ITS 1.0 i 1.1 statički ključ i ITS 2.0 uz SNC
- Između Agate i SAP R/3 sistema moguće je koristiti SNC od verzije 4.5. SAP sistema

Internet transakcioni server je dostupan od SAP R/3 verzije 3.1.

## 10. SAP S/4 HANA

SAP-ova poslednja verzija ERP sistema koja nosi naziv S4 HANA, zamišljena je kao ceo sistem koji će raditi u pokretu (on-the-fly), s' toga to je bio veoma hrabar potez da se promeni celokupno funkcionisanje sistema. U februaru SAP-ov koosnivač Hasso Plattner je na njujorškoj berzi opisao kako bi SAP HANA eliminisala čak više od 40% nagomilanih podataka koji nastaju prilikom razmene podataka između sistema, kao npr. ERP i CRM.

Nakon niza godina sam SAP sistem je postajao sve složeniji na taj način što su mu dodavane nove komponente, tako je jedna ideja o SAP S4 HANA da se smanji složenost a da pritome i dalje ispuni obećanje u isporuci jedinstvenog integrisanog sistema. Kako je Plattner istakao ovo uključuje detaljno smanjivanje kompleksnosti podataka, a samo smanjivanje od 1:10 će biti moguće ostvariti redukcijom agregata. (Agregat – je materijalizovani pogled na podatak u InfoCube-u, omogućava brz pristup podacima i sličan je indeksima baze podataka.). (Murphy, 2015).

SAP HANA platforma je bazirana na skladištenju velike baze podataka na unutrašnjoj RAM memoriji gde je sam performans i brzina dostavljanja podataka izuzetno brza, precizna i dinamična, što je upravo i razlog zašto se kompanije odlučuju da investiraju u implementaciju ovog sistema. Statistika pokazuje da za jednostavne upite SAP HANA može da ponudi rešenje za nekoliko stotinki dok za kompleksne upite nudi kompletno rešenje za sve 4 sekunde

([http://www.isaca.org/Groups/Professional-English/sap-applications/GroupDocuments/Security\\_In\\_SAP\\_HANA.pdf](http://www.isaca.org/Groups/Professional-English/sap-applications/GroupDocuments/Security_In_SAP_HANA.pdf), 2013).

Kada govorimo o njenoj brzini, fascinantno je podatak kojom je SAP Simple Financial Application analizirala podatke za zadnjih osam tromesečija sa ukupno 245 miliona unosa koje uključuju i dobitke u gubitke u samo jednoj sekundi. Prednost koju je HANA donela takođe odnosi i na korisničko okruženje. SAP je ranije porpilično bio kritikovan zbog svog korisničkog okruženja, te je zbog toga razvio Fiori koji dolazi uz SAP S4 HANA-u. SAP je produžio podršku za dosadašnju verziju SAP ECC 6.0 do 2025. godine i obećao da će svim korisnicima jednostavan prelazak na SAP S4 HANA-u.

SAP pruža veliku podršku svojim korisnicima i iz to razlog razvili su alat pod nazivom SAP Rapid Deployment čija osnovna svrha jeste da omogući brzu migraciju na SAP HANA platformu kao i na SAP Simple Finance.

Od 2010 godine kada je SAP HANA postala dostupna korisnicima, ovo rešenje je implementirano u preko 2000 kompanija i na taj način je postalo najbrže rastući proizvod SAP-a, i samim tim je poraslo interesovanje i mogućnosti za hakerskim i malicioznim napadima. Sama činjenica da su u različitim kompanijama koje su implementirale SAP HANA-u ovi napadi uspešno izvedeni i poverljivi podaci javno objavljeni je podiglo nivo zabrinutnosti oko kvaliteta bezbednosti sistema (Bonderud, 2015). Wiegensteinova studija (2016) je pokazala da je veliki deo propusta upravo napravljen u autorizaciji tokom kastomizacije SAP HANA-e gde nije posvećeno dovoljno pažnje bezbednosnim rizicima (Blume, 2015).

U cilju poboljšanja bezbednosti SAP HANA sistema, kompanija Onapsis se ciljano bavi pitanjem bezbednosti u SAP-u i do sada je detektovala preko 20 krucijalnih propusta, i ono što posebno naglašavaju kao opasnost jeste da se propustima može pristupiti udaljeno (Kirk, 2015). Bonderud (2015) tvrdi da je deo problema vezanih za propuste u SAP HANA u činjenici da se cyber-bezbednost najčešće fokusira na zaštitu procesa, ljudi i infrastrukture dok je sam SAP sistem prilično zapostavljen. Često se dešava da zbog svoje kompleksnosti i umreženosti sa osnovnom infteastrukturom kompanije odgovorni za bezbednost ne prepoznaju napade koji se dešavaju u SAP-u sve dok nije kasno i propust se već desio.

Na razvoju SAP HANA-e se kontinuirano radi u skladu sa problemima koji se javljaju i sa ciljem da se korisnicima pruži najkvalitetniji i istovremeno najbezbedniji mogući proizvod. U skladu sa tim poslednji update koji je napravljen adresira pitanja poboljšanja kvaliteta brzine

procesiranja podataka, bezbednosti autorizacije vezano za kastomizovane transakcije kao i pojačan pristup podacima u slučaju prekida (disaster recovery) (<https://hana.sap.com/capabilities/sps-releases/sps11.html>, 2016). Istraživanje iz 2011 godine koje je Onapsis sproveo pokazuje da deo napada najjednostavnije može da se izvede koristeći takozvani „backdoor“ ulaz kreiranjem novog usera sa izuzetno visokim ovlašćenima – koji se neće odmah pokazati u sistemu i može da načini znatnu štetu (Nunez, 2015). Sa druge strane postoji i niz predostrožnosti poput redovnih revizija i interne kontrole, koji donekle mogu da spreče bazične i relativno niske sigurnosne propuste.

## 11. SAP S/4 HANA zaštita mreže i komunikacija

SAP S/4 HANA je poslednje software-sko rešenje koje je SAP kompanija proizvela. Kada je prvi put prestravljena celokupna zamisao ove verzije software-a bila je da se kompletan program bazira na cloud rešenju. Na taj način došlo je do znatno većeg pomaka u performansama samog sistema i period koji je potreban za obradu informacija se značajno smanjio. Kako je cela ideja bazira na cloud-u, ono što predstavlja moguću pretnju po ovakav sistem jeste baš bezbednost samih mreža. U cilju što pouzdanijeg rada i podizanja bezbednosti kako bi sačuvao integritet svojih klijenata, SAP je ponudio nekoliko bezbednosnih rešenja. SAP HANA podržava enkriptovanu komunikaciju i kanale. Kada je reč o bezbednosnim kanalima u okviru SAP S/4 HANA možemo ih podeliti u dve grupe, u kanale koje se odnose na komunikaciju između klijenata baze podataka koji ostvaruju komunikaciju sa SAP S/4 HANA-om i kanale koji su zaduženi za unutrašnju komunikaciju između baza podataka. SAP je preporučuje da se enkriptovana komunikacija koristi gde god je to moguće jer na taj način se postiže ostvarivanje sistema sa što manje slabih tačaka ([http://help.sap.com/hana/SAP\\_HANA\\_Security\\_Guide\\_en.pdf](http://help.sap.com/hana/SAP_HANA_Security_Guide_en.pdf), 2016). Kako bi postigli što optimizovaniji rad SAP je ponudio nekoliko rešenja i postavki kanala u okviru SAP S/4 HANA sistema. Ti scenariji komunikacije su sledeći (Ritter i Rinderle-Ma, 2015):

- Kanali za upostavljanje eksternog pristupa sistemu SAP S/4 HANA od strane krajnjih korisnika, takođe prilikom administracije klijentnih naloga, pristupanje od strane aplikativnih servera i razmena podataka kroz SQL i HTTP
- Kanali koji su u upotrebi prilikom ostvarivanja interne komunikacija između SAP S/4 HANA sistema i baza podataka, ostvarivanje komunikacije između hostova kao i multi-host sistema i u komunikacijama između sistema kada se vrši kopiranje celokupnih sistema.

Kada je reč o prvoj grupi kanala, komunikacije u ovoj grupi možemo još detaljnije podeliti u sledeće kategorije:

- Konekcije koje ostvaruju radi vršenja poslova administracije sistema
- Konekcije koje služe da klijenti baze podataka mogu da pristupe SQL/MDX interfejsu na SAP S/4 HANA bazi podataka
- Konekcije koje se osvaruju od strane HTTP/S klijenata
- Kanale za ostvarivanje odlazećih konekcija.

Da bi uspešno izvršili implementaciju SAP S/4 HANA sistem veoma je važno da njeno okruženje kreiramo u sigurnim uslovima. Kako bi ostvarili takve zahteve na raspolaganju nam je da se uspostavi mreža u kojoj će se odvijati autorizovan saobraćaj. Osnovni parametri koje treba postaviti da bi kreirali ovakve uslove su sledeći:

- Obavezno je definisati da svi klijenti imaju isključivo pristup preko pristupnih portova
- Da se pristupanje SAP HANA okruženju putem HTTP od strane klijenata isključivo odvija posredno SAP HANA Extended Application Services-om (SAP HANA XS)
- Definirati da se sve administrativni poslovi i funkcije obavljaju preko administrativnih portova
- Uspostaviti upotrebu URL filtera u korelaciji sa SAP XS.

U okviru SAP S/4 HANA sistema svaka baza podataka poseduje svoj jedinstven port, SQL port i HTTP/S port. Ova grupa parametara se dodaje se svim bazama prilikom njihovog kreiranja. SAP Web Dispatcher ima ulogu da vrši preusmeravanje svih dolazećih HTTP zahteva od strane klijenata na određen XS server. SAP Web Dispatcher funkcioniše na taj način što radi kao zaseban servis na sistemskoj bazi podataka (Kristen, Mack i Schröer, 2016). Kada je reč o internim komunikacijama koje se odvijaju u okviru SAP S/4 HANA sistema, možemo ih detaljnije razvrstati na sledeći način:

- Komunikacije koje su ostvarene ka bazama podataka
- Komunikacije koje je potrebno postići da bi se ostvarila veza između hostova u procesu distribucije
- Komunikaciju koju je potrebno ostvariti između više različitih sajtova kada se vrši proces backup-ovanje sistema

### 11.1. SSL protokol kao sistem zaštite

Transport Layer Security (TLS) kako i Secure Socket Layer (SSL) predstavljaju protokole koje najčešću primenu imaju u zaštiti računarskih mreža. SSL protokol možemo upotrebiti kao način na koji bi osigurali internu mrežnu komunikaciju u SAP S/4 HANA sistemu koja se odvija između primarnih i sekundarnih sajtova. Ovaj vid zaštite je veoma značajan u proceduri kada se vrši backup-ovanje sistema. Backup-ovanje sistema je proces koji je veoma značajan za očuvanje sistema kao što je SAP S/4 HANA

([https://help.sap.com/saphelp\\_nw73/helpdata/en/77/6fb4308dbe40d6b6ac5903e95c2521/frame.htm](https://help.sap.com/saphelp_nw73/helpdata/en/77/6fb4308dbe40d6b6ac5903e95c2521/frame.htm), 2016). Cilj ove procedure je taj da se na svaki mogući način izbegne havarija koja bi dovela do prestanka rada sistema. Na ovaj način sistem vrši konstatno kopiranje podataka između primarnog i sekundarnog sistema. Ovaj vid podrške sistema omogućava da sistem bude u što kraćem vremenskom periodu neaktivan i da pređe na sekundarni sistem ili da primarni sistem preuzme deo koji je neispravan od sekundarnog sistema. Komunikaciji kanala između ove dve vrste sistema mogu biti osigurani tako što će u upotrebi biti metadata kanal koji vrši prenos meta podataka između sistema, kao i sam kanal za podatke koji će vršiti transfer samih podataka. Dodatna bezbednost koja se ostvaruje za ovu proceduru je ta je infrastruktura javnih ključeva (PKI) u upotrebi za zaštitu ovih komunikacija od onog trenutka od kad se celokupni sistem napravi. Ova vrsta zaštite je predefinisana u radu sistema ali takođe je moguće kreirati i sopstveni PKI infrastrukturu (Hirao, 2008).

U cilju kako bi se obezbedilo ispravno funkcionisanje SSL protokola potrebno je definisati komunikaciju između sistema na taj način što će se svim IP adresama odrediti da li imaju pristup portovima koji su potrebni za kopiranje samog sistema.

## 12. Tipovi korisnika i kreiranje korisnika u okviru SAP S/4 HANA

Prilikom definisanja korisnika u okviru sistema SAP S/4 HANA treba nampomenuti da je tip korisnika veoma sličan onom koji možemo pronaći u SAP R/3 sistemu, s' tim što je razlika u komunikaciji na relaciji korisnik i baza podataka. Svaki korisnik u okviru HANA sistema koji želi da radi direktno sa bazom podataka, mora da ima kreiran korisnički nalog sa određenim dodeljenim privilegijama na tom nalogu. Postoje u okviru SAP S/4 HANA podela korisničkih naloga na dva osnovna tipa, a to su tehnički korisnici baze podataka i korisnički nalozi koji pripadaju pravim osobama. Kada se govori o različitim vrstama korisničkih naloga isto tako možemo definisati različite alatke za svaki korisnički nalog u zavisnosti od toga za koju vrstu posla je namenjen taj nalog

(<https://help.hana.ondemand.com/help/frameset.htm?e6b196abbb5710148c8ec6a698441b1e.html>, 2016). Tehnički posmatrano ove dve vrste naloga su iste i razlika je samo u konceptu primene. Korisnički nalozi baza podataka koji pripadaju realnim osobama su nalozi koji se kreiraju za svaku osobu kojoj je potrebno omogućiti rad u okviru SAP S/4 HANA sistema. Ova vrsta korisničkih naloga se gasi, kad god osoba kojoj nalog pripada ode iz organizacije. Sa gašenjem naloga takođe se ukidaju i sve privilegije koje su dodate tom nalogu. U okviru ovog tipa korisničkih naloga postoje još dve vrste naloga koje se mogu kreirati a to su standardni nalozi i nalozi sa ograničenjima. Standardni nalozi se kreiraju sa funkcijom „CREATE USER“ i ovim nalozi je omogućeno da kreiraju svoje sopstvene objekte i da vrše čitanje podataka u okviru sistema. Nalozi sa ograničenjima se kreiraju uz pomoć funkcije „CREATE RESTRICTED USER“ i ovaj tip naloga se kreiraj za potrebe korisnika koji pristupaju sistemu uz pomoć klijent aplikacije. Prilikom ovog načina pristupanja SAP S/4 HANA sistemu potrebno je omogućiti pristup korisniku ali da ne može da ostvari potpuni pristup SQL-u putem SQL konzole (Hourani, 2014). Kada bi izvršili poređenje ova dva tipa korisničkih naloga razlika naloga sa ograničenjima u odnosu na standardne naloge bi bila u tome što:

- Ovaj tip naloga nema mogućnost da ni na jedan način kreira objekte u okviru baze podataka
- Nemaju mogućnost da vrše očitavanja ni jedne vrste podataka iz baze podataka
- Jedinu mogućnost koju imaju je ta da mogu da izvrše konekciju prema bazi podataka uz pomoć HTTP/S konekcija

Kada spomenemo tehničke korisnike baze podataka uglavnom se ne odnose na pravo osoblje i ovaj tip korisničkih naloga se ne gasi prilikom nečijeg odlaska iz preduzeća. Ovaj tip naloga se uglavnom kreira za potrebe određenih aplikacija kojima je potrebno omogućiti pristup bazi podataka kako bi mogla da izvrši određeno upisivanje ili očitavanje. Objektivno posmatrano oni su isti kao standardni korisnički nalozi i takođe se kreiraju uz pomoć funkcije „CREATE USER“.

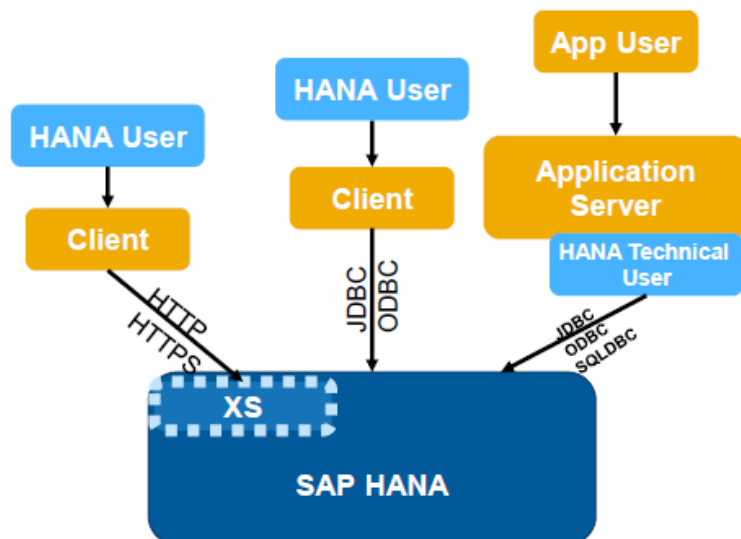


Image 13 - SAP HANA User access

Prilikom kreiranja korisničkih naloga svaki nalog je namenjen određenom zaposlenom koji ima specifičan opis posla, zbog toga se u okviru svakog korisničkog naloga mogu se omogućiti različiti korisnički alati. Korisnički alati koji se mogu pridodati korisničkim nalogima radi ostvarivanja administrativnih funkcija su alati za kreiranje i definisanje uloga, alati za kreiranja naloga, alati za dodavanje uloga određenim nalogima. Takođe drugi zadaci koji obuhvataju administrativni alati su alati za brisanje korisničkih naloga kada osoba napusti preduzeće, alati za ponovno aktiviranje naloga kada korisnik pokuša više puta da se bezuspešno uloguje na sistem, alati za deaktiviranje korisničkog naloga ako je ugrožena bezbednost sistema i alati za resetovanje korisničke šifre.

Pored dva navedena tipa naloga takođe postoji i treći tip, a to je sistemski nalog koji se koristi da se kreiraju nalozi sa nižim privilegijama. Ovaj tip naloga nije predviđen da se koristi u okviru sistema koji treba da bude u produkciji niti da se koristi kao svakodnevni nalog, zato se savetuje da se prilikom kreiranja svih potrebnih stvari ovaj nalog deaktivira. Jednom deaktiviran nalog ne može se ponovo konektovati na SAP S/4 HANA bazu podataka ([http://help.sap.com/saphelp\\_hanaplatform/helpdata/en/de/a55d23bb571014bf25f6ed0d3b2b17/content.htm](http://help.sap.com/saphelp_hanaplatform/helpdata/en/de/a55d23bb571014bf25f6ed0d3b2b17/content.htm), 2016).

Kod SAP S/4 sistema koji objedinjuju više baza podataka, svaka baza podataka sa sobom donosi i određeni broj korisnika kao i sistemski nalog svake baze podataka. Na koji način će šifra za sistemski nalog biti kreirana zavisi od toga da li je nalog nastao u sistemu sa više baza ili u sistemu sa jednom bazom koja je konvertovana u višebazni sistem. Ukoliko se prilikom same postavke sistema uspostavi sistem sa više baza podataka onda se još prilikom same instalacije vrši kreiranje sistemskog naloga i njegove šifre. Nakon instalacije svaki sistem koji je objedinjen instalacijom će imati zaseban korisnički nalog i šifru koja će biti navedena za vreme instalacije za svaku bazu podataka ponaosob

([http://help.sap.com/saphelp\\_hanaplatform/helpdata/en/dd/a2ae94bb571014a48fc3b22f8e919e/content.htm](http://help.sap.com/saphelp_hanaplatform/helpdata/en/dd/a2ae94bb571014a48fc3b22f8e919e/content.htm), 2016). Ukoliko sistem nastaje tako što se vrši konverzija sistem u višebazni sistem, onda će prilikom konverzije svaka baza podataka koja se napravi naslediti korisnički nalog i šifru od baze podataka od koje je nastala. Tokom ovog procesa jako je bitno navesti tačni korisničku šifru. Što se tiče prijave na sam sistem SAP S/4 HANA je u većoj meri zadržala principe i način rada osnovnog SAP R/3 sistema. Pored osnovnih stvari tu su takođe dalje SingleSign-On kao način prijave na sistem, SNC, SSL protokoli, Profile Generator i X.509 sertifikat.

## 13. Zaključak

U dosadašnjem radu upoznali smo se sa principima i načinom rada jednog sistem kao što SAP i sa time šta sve taj sistem podrazumeva. Pored osnovnih stvari koje su predstavljene u ovom radu, napravljen je osvrt i na neke od osnovnih načina putem kojih se ilegalno može doći u posed poverljivim informacija. Glavni akcenat je stavljen na samu bezbednost i na to koliko je ovaj sistem ranjiv i koliko je zapravo javnost upoznata sa tim, kao i koliko je moguće doći do takvih informacija. Kada je reč o bezbednosti SAP sistema, treba napomenuti interesantne činjenice, kao što je to da je zapravo broj ranjivih mesta u SAP sistemu mnogo veći od onog što se misli i što je dostupno javnosti. Približni broj koji je poznat je oko 3000 ranjivih mesta SAP sistema, što čini oko 5% svih ranjivosti objavljenih na internetu (<https://erpscan.com/wp-content/uploads/publications/3000-SAP-notes-Analysis-by-ERPScan.pdf>, 2014). Ta činjenica podstakla je povećanje u zainteresovanosti za SAP bezbednost što je dovelo do masovne izrade broja zakrpa SAP sistema na mesečnom nivou koje ranije iznosilo 10%, a sada je poraslo na oko 60-70%. (Polyakov i Tyurin, 2013).

Kada govorimo o popularnosti nekog software-a, ona može da se posmatra i kroz broj hakerskih napada na sistem. Što je veći broj napada to je popularnost tog software-a veća iz razloga što se program upražnjava na brojnim mestima i da se u njemu može pronaći veliki broj poverljivih informacija. Broj korisnika koji je počeo da primećuje propuste u okviru SAP sistema se u odnosu na 2014. godinu udvostručio.

SAP kao sistem je izuzetno kompleksan i ogroman u kojem tradicionalni sistemi bezbednosti ne igraju preterano važnu ulogu. Zbog svoje specifičnosti i samog SAP NetWeaver programa, u okviru kojeg može postojati na više od hiljadu web servisa gde se svaki manifestuje kao mala web stranica i koja može biti meta napada, značajne bezbednosne mere se oslanjaju na pouzdan rad administratora sistema. U tako kompleksnom sistemu razumljivo je da postoje problemi koji mogu narušavati bezbednost i suviše je napomenuti da je kompleksnost obrnuto srazmerna bezbednosti. Jedan od problema u dolaženju do informacija i razoktrivanju propusta u okviru jednog ovakvog sistema takođe proizilazi iz želje obe strane, i SAP-a i korisnika SAP usluga, da sve moguće informacije o bezbednosnim propustima zadrže za sebe i ne dozvole da informacije o propustima procure na tržište. Ovo ima za primarni cilj da se ne podiže panika zbog curenja poverljivih informacija ali je u pitanju i održavanje reputacije kompanije i dobrog javnog imidža.

Sa ciljem da spreči i smanji broj ranjivosti SAP kompanija je razvila nešto što se zove SAP Security Notes koje objavljuje svakog drugog utorka koji se naziva SAP Critical Patch Day ([www.sap.com](http://www.sap.com), 2016). U okviru SAP Security Notes mogu se pronaći sve potrebe informacije o novim pronađenim ranjivostima u okviru SAP sistema. Prvi SAP Security Notes objavljen je 2001. godine, dok je 2007. doživeo svoj eksponencijalni rast koji je svoj vrhunac dostigao 2010. godine. Od te godine stagnira ali i dalje doprinosi značajne informacije koje pomažu u poboljšavanju bezbednosti. Na ovaj način SAP aktivno pokazuje da spremno radi i posvećuje pažnju sigurnosti i zaštiti podataka svojih klijenata uz kontinuirani razvoj samog sistema.

Sve u svemu, kada se sagleda SAP kao proizvod i mogućnosti koje nudi klijentima možemo da zaključimo da je u pitanju proizvod koji je izuzetnog kvaliteta ali da će se i nastaviti sa daljim razvojem u skladu sa potrebama poslovanja. Unapređenja i usavršavanja programa su neophodni kako zbog održavanja tržišne konkurentnosti ali takođe i sa ciljem zaštite zvog kontinuiranog napredovanja hakerskih i bezbednosnih napada sa malaicioznim ciljevima.

## Spisak referenci

1. Aaron, G. & Rasmussen, R., „**Global Phishing Survey 2H2014: Trends and Domain Name Use**“, An APWG Industry Advisory. (2015).
2. Analysis of 3000 SAP vulnerabilities in SAP, <https://erpscan.com/wp-content/uploads/publications/3000-SAP-notes-Analysis-by-ERPScan.pdf> (pristup 24.04.2016).
3. An Introduction to SAP, <http://www.erpgreat.com/sap-introduction.htm> (pristup 16.03.2016.)
4. Anderson, G.V., Nilson, C.D. & Rhodes, T., „**SAP implementation unleashed : a business and technical roadmap to deploying SAP**“. Indianapolis, Ind. : Sams (2009).
5. Appelrath, H. J., & Ritter, J., „**SAP R/3 implementation: methods and tools**“. Springer Science & Business Media. (2013).
6. Berry, M., Defining ERP: Enterprise Resource Planning Software Guide, <http://www.itmanagerdaily.com/erp/> (pristup 16.03.2016.)
7. Bergholz, A., Chang, J. H., Paass, G., Reichartz, F., & Strobel, S., „**Improved Phishing Detection using Model-Based Features**“. In CEAS. (2008)
8. Blume, J., The “Cost of Cyber Crime” Study in the Context of SAP Security, <https://www.virtualforge.com/en/blog/post/the-cost-of-cyber-crime-study-in-the-context-of-sap-security.html> (pristup 08.02.2016)
9. Bonderud, D., „**SAP Vulnerabilities Shaking HANA’s Tree, Could Lead to Data Breach**“, <https://securityintelligence.com/news/sap-vulnerabilities-shaking-hanas-tree-could-lead-to-data-breach/> (pristup 14.04.2016)
10. Bonderud, D., „**New SAP Vulnerabilities Create Sticky Situation for IT Security**“, <https://securityintelligence.com/news/new-sap-vulnerabilities-create-sticky-situation-for-it-security/> (pristup 15.04.2016).
11. Boeder, J. & Groene, B., „**The Architecture of SAP ERP: Understand how successful software works**“. Tredition (2014).
12. Chaitanya, M., „**The Complete Guide to SAP NetWeaver Portal**“. SAP Press (2012).
13. Chetan, S.S., „**Implementation Strategies for SAP R/3 in a Multinational Organization: Lessons from a Real-World Case Study**“. Cybertech Publishing (2006).
14. Chinese attack on USIS using SAP vulnerability – Detailed review and comments, <https://erpscan.com/press-center/blog/chinese-attack-on-usis-using-sap-vulnerability-detailed-review-and-comments/> (pristup 25.04.2016).
15. Fletcher, A.N., Brahm, M. i Pargmann, H. , „**Workflow Management with SAP® WebFlow®: A Practical Manual**“. Springer Science and business media (2003).
16. Franc, I., „**Virusi - pojam i vrste**“, <http://www.singipedia.singidunum.ac.rs/entries/10-Virusi-pojam-i-vrste> (pristup, 13.03.2016)
17. Gordon, S. i Ford, R., „**On the definition and classification of cybercrime**“, J Comput Virol (2006) 2:13–20.
18. Hernandez, J., A., „**SAP R/3 Handbook**“. New York: McGraw-Hill (2000).
19. History of Phishing, <http://www.phishing.org/history-of-phishing/> (pristu 27.03.2016)
20. ow SAP works?, <http://www.technofunc.com/index.php/erp/145-how-sap-works> (pristup 16.03.2016)

21. Kirk, J. „**Dangerous bugs leave open doors to SAP HANA systems**“ , <http://www.csoonline.com/article/3003083/application-security/dangerous-bugs-leave-open-doors-to-sap-hana-systems.html> (pristup 15.04.2016).
22. Ladakis, E., Koromilas, L., Vasiliadis, G., Polychronakis, M. I Ioannidis. S., „**You**
23. **Can Type, but You Can't Hide: A Stealthy GPU-based Keylogger**“. In EuroSec'13,(2013)
24. Little, A. G. & Best, P. J., **A Framework For Separation Of Duties In An SAP R/3 Environment**. Managerial Auditing Journal XVIII(5): pp. 419-430. (2003)
25. Linkies, M. & Karin, H., „**SAP Security and Risk Management**“. Rheinwerk Publisher (2011).
26. Magal, S. and Word, J. „**Integrated Business Processes with ERP Systems**“. John Wiley & Sons. Hoboken, NJ., (2012).
27. Magen-Goldstein, T., „**SAP NetWeaver at a Glance**“, <http://scn.sap.com/docs/DOC-8287> (pristup 02.03.2016.)
28. Martinez, M. & McKibbin, S., „**SAP Training Tutorials : SAP Introduction and Basic Skills Handbook**“. Equity Press (2009).
29. Missbach, M., Stelzel, J., Gardiner, C., Anderson, G., & Tempes, M., „**From R/3 to HANA. In SAP on the Cloud**“. Springer Berlin Heidelberg (2013).
30. Morgan, J. H., Cheng, C. Y., Pike, C., & Ritter, F. E. „**A design, tests and considerations for improving keystroke and mouse loggers**“. Interacting with Computers, iws014. (2013).
31. Murphy, M. „**SAP offers S/4HANA for free**“, <http://www.computerworlduk.com/it-management/s4-hana-what-does-saps-next-generation-erp-mean-for-customers-3596790/> (prsitup 31.03.2016).
32. Nunez, M., „**Onapsis Discovers and Helps Mitigate New Critical Cyber Security Vulnerabilities Affecting All SAP HANA-based Applications, Including SAP S/4HANA and SAP Cloud Solutions**“, <https://www.onapsis.com/onapsis-discovers-and-helps-mitigate-new-critical-cyber-security-vulnerabilities-affecting-all-sap> (pristup 15.04.2016).
33. Olson, D. L., & Kesharwani, S. „**Enterprise information systems: contemporary trends and issues**“. World Scientific. (2010).
34. Okungbowa, A. , „**SAP ERP Financial Accounting and Controlling Configuration and Use Management**“. Apress, (2015).
35. Proctor, P. E., Heiser, J., & MacDonald, N., „**MarketScope for Segregation of Duties Controls Within ERP**“. Gartner Research G, (2007).
36. Phishing napadi, <http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-01-106.pdf> (pristup 16.03.2016).
37. Putnik N. I Bošković, M., „**Savremeni bezbednosni izazovi – haktivizam kao novi oblik društvenog konflikta, (Contemporary Security Challenges–hactivism as a new form of social conflict)**“ , Faculty of Security, Belgrade, (2013).
38. Ricalda,A., SAP Bests Oracle, Other Rivals in Shift to Cloud Computing, <http://www.bloomberg.com/news/articles/2015-10-13/sap-third-quarter-sales-operating-profit-beat-analyst-estimates> (pristup 14.03.2016.)
39. Sinkovski S., „**Informaciona bezbednost – komponenta nacionalne bezbednosti**“. Vojno delo, str. 31-81 (2/2005).
40. SAP HANA platform: Introducing SPS 11, <https://hana.sap.com/capabilities/sps-releases/sps11.html> (pristup 16.04.2016)
41. SAP NetWeaver and its Components, <http://www.simplilearn.com/sap-netweaver-and-its-components-rar112-article> (pristup 02.03.2016.)

42. SAP: A 44-year history of success,  
<http://go.sap.com/corporate/en/company/history.html> (pristup 18.02.2016)
43. SAP definition, <http://searchsap.techtarget.com/definition/SAP> (pristup 15.03.2016)
44. Von Aspen, J., „**Getting started in SAP: How to transform your career and become a highly paid SAP expert**“. CreateSpace Independent Publishing Platform (2014).
45. Security in SAP HANA: The Challenges of In-Memory Computing,  
[http://www.isaca.org/Groups/Professional-English/sap-applications/GroupDocuments/Security\\_In\\_SAP\\_HANA.pdf](http://www.isaca.org/Groups/Professional-English/sap-applications/GroupDocuments/Security_In_SAP_HANA.pdf) (pristup 31.03.2016).
46. Sullivan, K.P.H. i Lindgren, E., „**Computer keystroke logging and writing: methods and applications**“. Oxford: Elsevier. (2006).
47. Third-party software was entry point for background-check system hack,  
<http://www.nextgov.com/cybersecurity/2015/05/third-party-software-was-entry-point-background-check-system-hack/112354/> (pristup 24.04.2016)
48. Threat Description Backdoor, <https://www.f-secure.com/v-descs/backdoor.shtml> (pristup 12.03.2016)
49. Tuli, P. i Sahu, P., „**System Monitoring and Security Using Keylogger**“, IJCSMC, Vol. 2, Issue. 3, pp.106 – 111 (2013).
50. Virilio, P., „**Informatička bomba**“ Novi Sad: Svetovi. (2000).
51. What is ERP?, <http://www.netsuite.com/portal/resource/articles/erp/what-is-erp.shtml> (pristup 15.03.2016)
52. What is SAP Hana?, <http://scn.sap.com/docs/DOC-60338> (pristup 03.02.2016.)
53. What Is the Difference: Viruses, Worms, Trojans, and Bots?,  
<http://www.cisco.com/c/en/us/about/security-center/virus-differences.html> (pristup 13.03.2016)
54. Polyakov, A. i Tyurin, A., „**12 years of sap security in figures: A global survey 2001–2013**“, <https://erpscan.com/wp-content/uploads/2013/11/SAP-Security-in-Figures-A-Global-Survey-2013.pdf> (pristup 24.04.2016)
55. Appelrath, H. J., & Ritter, J. (2013). **SAP R/3 implementation: methods and tools**. Springer Science & Business Media.
56. Boettcher, T., Daiberl, J., Fischer, A. i Liu, L., (2007). **Unleash the Power of Single Sign-On with Microsoft and SAP**. Collaboration Technology Support Center – Microsoft – Collaboration Brief, White Paper.
57. Chuprunov, M. (2013). **IT General Controls in SAP ERP**. In **Auditing and GRC Automation in SAP** (pp. 131-163). Springer Berlin Heidelberg.
58. Cohrs, C. i Kirschenmann, M. (2015). **Simple and Secure User Authentication with SAP Single Sign-On 2.0 - How the Latest Features Enhance the User Experience, Strengthen Security, and Streamline Administration**. SAPinsider, Volume 16, Issue 3
59. **Identity and Access Management**,  
<https://help.hana.ondemand.com/help/frameset.htm?e6b196abbb5710148c8ec6a698441b1e.html>, pristup 12.07.2016.
60. Faltin, U., Glöckner, P., Viebeg, U., Berger, A., Giehl, H., Hühnlein, D., & Surkau, T. (2013). **On the development of a security toolkit for open**. Verlässliche IT-Systeme: Zwischen Key Escrow und elektronischem Geld, 113.
61. Fernandez, E. B., & Pan, R. (2001,). **A pattern language for security models**. In Proc. of PLoP (Vol. 1).
62. Fernandez, E. B., Mujica, S., & Valenzuela, F. (2011,). **Two security patterns: least privilege and security logger and auditor**. In Proceedings of the 2nd Asian Conference on Pattern Languages of Programs, ACM.

63. Hague, D. (2014). **Universal Worklist with SAP NetWeaver Portal**. Espresso Tutorials GmbH.
64. Hernandez, J. A. (1999). **Sap R/3 Administrator's Handbook**. McGraw-Hill Professional.
65. Hirao, J. (2008). **SAP security configuration and deployment: The IT administrator's guide to best practices**. Syngress.
66. Hourani, M. (2014). **Understanding SAP HANA Security Concepts and Mitigating Risks**.
67. Kristen, A., Mack, H i Scholer, T. (2016). **SAP HANA Security Whitepaper**. SAP HANA SPS11
68. Linkies, M. i Off, F. (2006)., **SAP Security and Authorizations**, SAP Press/ Galileo Press
69. Lamotte-Schubert, M., & Weidenbach, C. (2009). **Analysis of Authorizations in SAP R/3**. First-order Theorem Proving FTP, 90.
70. Lam, W. (Ed.). (2007). **Enterprise Architecture and Integration: Methods, Implementation and Technologies: Methods, Implementation and Technologies**. IGI Global.
71. Manara, M., & Cavalleri, A. (2012). **100 Things You Should Know about Authorizations in SAP**. SAP PRESS.
72. Mohay, M., Anderson, A., Collie, B. i de Vel, O., (2003). **Computer and Intrusion Forensics (Artech House Computer Security Series)**, ISBN 1-58053-369-8
73. **Network and Transport Layer Security**,  
[https://help.sap.com/saphelp\\_nw73/helpdata/en/77/6fb4308dbe40d6b6ac5903e95c2521/frameset.htm](https://help.sap.com/saphelp_nw73/helpdata/en/77/6fb4308dbe40d6b6ac5903e95c2521/frameset.htm), pristup 15.07.2016.
74. Österle, H., Fleisch, E., & Alt, R. (2012). **Business networking: Shaping enterprise relationships on the Internet**. Springer Science & Business Media.
75. **Personal Security Environment**,  
[https://help.sap.com/saphelp\\_nw70ehp2/helpdata/en/b8/821feedadd11d2a60a0000e835363f/content.htm?frameset=/en/8d/517619da7d11d1a5ab0000e835363f/frameset.htm&current\\_toc=/en/58/251a355d0c4d78e10000009b38f83b/plain.htm&node\\_id=35](https://help.sap.com/saphelp_nw70ehp2/helpdata/en/b8/821feedadd11d2a60a0000e835363f/content.htm?frameset=/en/8d/517619da7d11d1a5ab0000e835363f/frameset.htm&current_toc=/en/58/251a355d0c4d78e10000009b38f83b/plain.htm&node_id=35), pristup 12.06.2016
76. **Public and private Keys**,  
[https://help.sap.com/saphelp\\_nw70ehp2/helpdata/en/40/8a0b37e44d7c2fe10000009b38f889/content.htm?frameset=/en/d9/440b37dd3e9e15e10000009b38f936/frameset.htm&current\\_toc=/en/58/251a355d0c4d78e10000009b38f83b/plain.htm&node\\_id=28&show\\_children=false](https://help.sap.com/saphelp_nw70ehp2/helpdata/en/40/8a0b37e44d7c2fe10000009b38f889/content.htm?frameset=/en/d9/440b37dd3e9e15e10000009b38f936/frameset.htm&current_toc=/en/58/251a355d0c4d78e10000009b38f83b/plain.htm&node_id=28&show_children=false), pristup 12.06.2016.
77. **Public Keys Certificate**,  
[https://help.sap.com/saphelp\\_nw70ehp2/helpdata/en/8d/51761cda7d11d1a5ab0000e835363f/content.htm](https://help.sap.com/saphelp_nw70ehp2/helpdata/en/8d/51761cda7d11d1a5ab0000e835363f/content.htm), pristup 12.06.2016
78. Ritter, D., & Rinderle-Ma, S. (2015). **Toward A Collection of Cloud Integration Patterns**. arXiv preprint arXiv:1511.09250.
79. **The SAP Security Library (SAPSECULIB)**,  
[https://help.sap.com/saphelp\\_nw70ehp2/helpdata/en/b8/821ff4dadd11d2a60a0000e835363f/content.htm](https://help.sap.com/saphelp_nw70ehp2/helpdata/en/b8/821ff4dadd11d2a60a0000e835363f/content.htm), pristup 18.07.2016.
80. **The SSF Initialization File**,  
[https://help.sap.com/saphelp\\_nw70ehp2/helpdata/en/25/4e0b37cf3e3273e10000009b38f936/content.htm](https://help.sap.com/saphelp_nw70ehp2/helpdata/en/25/4e0b37cf3e3273e10000009b38f936/content.htm), pristup 15.07.2016.
81. Sel, M., & Van Der Auwera, K. (2010). **Demystifying SAP security**. In ISSE 2009 Securing Electronic Business Processes (pp. 27-36). Vieweg+ Teubner.

82. **SAP, Profile Parameters for Logon and Password (Login Parameters),**  
[https://help.sap.com/saphelp\\_nw73/helpdata/en/4a/c3f18f8c352470e10000000a42189c/content.htm](https://help.sap.com/saphelp_nw73/helpdata/en/4a/c3f18f8c352470e10000000a42189c/content.htm), pristup 19.07.2016.
83. **SAP HANA User Management,**  
[http://help.sap.com/saphelp\\_hanaplatform/helpdata/en/de/a55d23bb571014bf25f6ed0d3b2b17/content.htm](http://help.sap.com/saphelp_hanaplatform/helpdata/en/de/a55d23bb571014bf25f6ed0d3b2b17/content.htm), pristup 23.07.2016.
84. **SAP, System Logon,**  
[https://help.sap.com/saphelp\\_nw73/helpdata/en/48/3a0638902131c3e10000000a42189d/content.htm?frameset=/en/4a/c3f18f8c352470e10000000a42189c/frameset.htm&current\\_toc=/en/b9/24b7ba9cb0421e915b8414422804e8/plain.htm&node\\_id=5&show\\_children=false](https://help.sap.com/saphelp_nw73/helpdata/en/48/3a0638902131c3e10000000a42189d/content.htm?frameset=/en/4a/c3f18f8c352470e10000000a42189c/frameset.htm&current_toc=/en/b9/24b7ba9cb0421e915b8414422804e8/plain.htm&node_id=5&show_children=false), pristup 17.07.2016
85. **SAP Security: Authentication and single sign-on,**
  - a. <http://searchsecurity.techtarget.com/tip/SAP-Security-Authentication-and-single-sign-on>, pristup 24.07.2016.
86. **SAP HANA Security Guide,**  
[http://help.sap.com/hana/SAP\\_HANA\\_Security\\_Guide\\_en.pdf](http://help.sap.com/hana/SAP_HANA_Security_Guide_en.pdf), pristup 25.07.2016
87. **Secure Network Communications (SNC),**  
[http://help.sap.com/saphelp\\_nw73ehp1/helpdata/en/aa/38ff4fa187622fe10000000a44176d/content.htm](http://help.sap.com/saphelp_nw73ehp1/helpdata/en/aa/38ff4fa187622fe10000000a44176d/content.htm), pristup 20.07.2016.
88. **Securing Data Connection,**  
[http://help.sap.com/saphelp\\_hanaplatform/helpdata/en/dd/a2ae94bb571014a48fc3b22f8e919e/content.htm](http://help.sap.com/saphelp_hanaplatform/helpdata/en/dd/a2ae94bb571014a48fc3b22f8e919e/content.htm), pristup 12.07.2016.
89. **SNC-Protected Communication Paths in SAP Systems,**  
[http://help.sap.com/saphelp\\_nw73ehp1/helpdata/en/ad/38ff4fa187622fe10000000a44176d/content.htm](http://help.sap.com/saphelp_nw73ehp1/helpdata/en/ad/38ff4fa187622fe10000000a44176d/content.htm), pristup 22.07.2016
90. **Secure Store and Forward Mechanism (SSF),**  
[https://help.sap.com/saphelp\\_nw70/helpdata/en/4d/bf6f77a2c5446a86e0152f1b309db6/content.htm](https://help.sap.com/saphelp_nw70/helpdata/en/4d/bf6f77a2c5446a86e0152f1b309db6/content.htm), pristup 15.07.2016.
91. **System Infrastructure for Using SSF Functions,**  
[https://help.sap.com/saphelp\\_nw70ehp2/helpdata/en/d9/440b37dd3e9e15e10000009b38f936/content.htm?frameset=/en/25/4e0b37cf3e3273e10000009b38f936/frameset.htm&current\\_toc=/en/58/251a355d0c4d78e10000009b38f83b/plain.htm&node\\_id=3](https://help.sap.com/saphelp_nw70ehp2/helpdata/en/d9/440b37dd3e9e15e10000009b38f936/content.htm?frameset=/en/25/4e0b37cf3e3273e10000009b38f936/frameset.htm&current_toc=/en/58/251a355d0c4d78e10000009b38f83b/plain.htm&node_id=3), pristup 12.07.2016
92. Sorsa, P. (2010). **Overview of authorizations in an SAP enterprise portal environment.**
93. Vacca, J. R. (2004). **Public key infrastructure: building trusted applications and Web services.** CRC Press.
94. Van der Aalst, W. M., & de Medeiros, A. K. A. (2005). **Process mining and security: Detecting anomalous process executions and checking process conformance.** Electronic Notes in Theoretical Computer Science, 121, 3-21.
95. Wood, D.L., Norton, D., Weschler, P., Ferris, C. i Wilson, Y., (2005). **Single sign-on framework with trust-level mapping to authentication requirements.** Sun Microsystems, Inc., U.S. Patent 6,892,307.
96. Woods, D., & Mattern, T. (2006). **Enterprise SOA: designing IT for business innovation.** " O'Reilly Media, Inc."