

ULOGA UNIVERZITETA U PREVENCIJI ZLOUPOTREBA INFORMACIONIH TEHNOLOGIJA

Dr Stevica Krsmanović
Univerzitet Braća Karić, Fakultet za trgovinu i bankarstvo
stevica@amadeus.uni-bk.ac.yu

Velimir Dedić
Univerzitet Braća Karić, Fakultet za trgovinu i bankarstvo
vdd@ftb.uni-bk.ac.yu

Sažetak

Rad treba da pokaže koji su specifični bezbednosni rizici IT resursa na univerzitetima. Koristeći best practices i preporuke relevantnih međunarodnih tela, u radu će se dati predlog mera čija bi implementacija mogla dovesti do kvalitetnije prevencije kompjuterskog kriminala u visokoškolskim sredinama. Na kraju će se dati i predlog kako univerzitetska sredina može poslužiti kao model za implementaciju dobrih preventivnih rešenja. Ključne reči: IT security policy, IT crime

Abstract

This paper should state specific IT security risks found at universities. We will use best-practices and adopted standards method to propose the measures to be imposed and implemented in order to improve IT security risk awareness at universities.

Finally, we see universities as potentially good model for implementation of similar solutions within different organizations.

1. Uvod

Bezbednosni rizici ugrožavaju IT resurse organizacije. Racionalno orijentisana organizacija preduzeće korake koji će joj omogućiti da proceni moguće rizike, definiše postupke koji treba da smanje verovatnoću nastupanja rizika, predvidi akcije usmerene na minimizaciju efekata rizika koji su nastupili i odredi postupke realizacije pomenutih preventivnih i palijativnih metoda.

Možemo se složiti da su sledeći koraci logičan niz aktivnosti koje treba da organizuje i čije izvršenje treba da organizuje menadžment organizacije:

1. Analiza rizika
2. Definisanje bezbednosnih politika
3. Definisanje bezbednosnog plana
4. Izbor bezbednosne arhitekture
5. Implementacija

Ovaj rad tretiraće tačke 1, 2 i 3 iz prethodne liste.

2. Organizacione mere prevencije

Prevencija je stvar organizacije. Kultura organizacije, koju definiše menadžment, treba da je takva da je u stanju da definiše i što je još teže, sprovede politike koje su usmerene na prevenciju zloupotreba IT resursa.

2.1. Scenariji prevencije

Interpol [2] daje koncizno definisane moguće bezbednosne pretnje i metode njihove prevencije. Prvo su definisana polja u kojima se sreću bezbednosne pretnje. Razlikujemo:

1. pretnje nezavisne od arhitekture sistema
2. pretnje koje zavise od arhitekture sistema.

2.1.1. Pretnje nezavisne od arhitekture sistema

Kod pretnji nezavisnih od arhitekture sistema definišemo sledeće potencijalne ciljeve pretnji:

- Pojedinci iz organizacije, zaposleni, sa dodeljenim pravima i privilegijama
- Manipulacija medijima za čuvanje podataka
- Zlonamerni kod
- Korišćenje emisija elektromagnetnog zračenja

Razmotrimo detalje svakog od potencijalnih ciljeva. Definisaćemo potencijalni scenario, tok akcije u kojoj se izvodi neka zlonamerna radnja, kao i preventivni odgovor na odgovarajući scenario.

Scenario	Metod prevencije
Nelojalni zaposleni	Uvek se preporučuje definisanje i stroga primena proceduralnih, formalizovanih i proverljivih bezbednosnih metoda. Lična odgovornost treba da proizlazi iz položaja

	pojedince u organizaciji.
Korisnik sistema ostvaruje neautorizovan pristup	Treba da postoje pisane instrukcije koje nedvosmisleno definišu šta su dozvoljeni a šta nedozvoljeni postupci prilikom pristupa sistemu. Treba da se uvede «pravilo dva čoveka» kod pristupa osetljivim informacijama. Treba uvesti kulturu čuvanja lozinki i korisničkih imena.¹ Treba redovno proveravati systemske dnevnike (log files). Treba instalirati sisteme za otkrivanje neovlašćenog pristupa (intrusion detection systems).
Administrator sistema ostvaruje neautorizovan pristup	Treba koristiti fizički odvojene sisteme za proizvodnju i eksploataciju. Treba da se uvede «pravilo dva čoveka» kod pristupa osetljivim informacijama. Dodeljivanje administrativnih privilegija (root ili administrator nalozi) treba da bude restriktivno.
Privremeni korisnik ² sistema ostvaruje neautorizovan pristup	Vremenski ograničiti trajanje naloga za privremene korisnike. Ukinuti naloge posle isteka ugovora.

Tabela 1: Analiza scenarija za cilj: pojedinci iz organizacije, zaposleni, sa dodeljenim pravima i privilegijama

Scenario	Metod prevencije
Krađa fizičkog medija	Mediji treba da budu pod ključem, sa definisanim metodima izdavanja, manipulacije i čuvanja ključeva.
Neautorizovano kopiranje podataka	Treba kriptozastiti osetljive podatke. Osoblje koje fizički manipuliše medijima ne treba da ima ključeve šifara. Treba primeniti «pravilo dva čoveka» za kreiranje rezervnih kopija (backup). Treba primeniti «pravilo dva čoveka» za pristup rezervnim kopijama (backup).

¹ Korisničko ime (user name) i lozinka (password) tretiraju se kao i fizički ključevi. Kultura organizacije mora biti takva da je radnja nemarnog odnosa prema lozinkama i korisničkim imenima jednako neprihvatljiva kao i radnja nemarnog odnosa prema ključevima od sefa.

² Privremeni korisnik definiše se kao pojedinac koji nije zaposlen u organizaciji, a prava pristupa sistemu dobio je po osnovu konsultantskog ugovora sa organizacijom ili na drugi regularan način.

Neautorizovano iznošenje medija iz prostorija organizacije	Ne treba slati uređaje sa medijima na servisiranje ili posudbu. Uvek treba da se šalje uređaj bez diska ili drugog medija.
--	--

Tabela 2: Analiza scenarija za cilj: manipulacija medijima za čuvanje podataka

Scenario	Metod prevencije
Napad virusima	Koristiti antivirusni sistem.
Programi koji omogućavaju neautorizovan pristup sisemu	Uvesti stroge procedure instalacije softvera. Korisnicima svih nivoa i funkcija dati minimalne instalacije. Ne ohrabrivati individualne instalacije softvera.

Tabela 3: Analiza scenarija za cilj: zlonamerni kod

Scenario	Metod prevencije
Prisluškivanje	Premda je oklapanje kablova i korišćenje Faradayevog kaveza za smeštanje osetljive opreme jedino rešenje koje onemogućuje prisluškivanje elektromagnetske emisije, ovo rešenje je skupo i stoga uglavnom u praksi neprimenljivo. Zato treba koristiti oklapanje vodova koliko je moguće, kontrolisati fizičke puteve prostiranja kablova i obavezno kriptoštititi komunikacije. Na taj način, ukoliko i dođe do uspešnog presretanja signala, informacija će jedno vreme ostati neupotrebljiva.

Tabela 4: Analiza scenarija za cilj: korišćenje emisije elektromagnetnog zračenja

Prethodno navedeni scenariji zajednički su za sve sisteme, nezavisno od konkretne arhitekture. Može se reći da su navedeni scenariji jednako verovatni u svakom tipu organizacije.

2.1.2. Pretnje zavisne od arhitekture sistema

Prema [2] analiziraćemo sada neke arhitekturno zavisne grupe scenarija, a to su:

1. Scenariji specifični za mikrokompjutere (standalone PC)
2. Scenariji specifični za LAN/WAN arhitekture i sisteme sa pristupom internetu
3. Scenariji specifični za mainframe arhitekture

Nalazimo razumnim da se koncentrišemo na drugu grupu scenarija, onu koja tretira LAN/WAN arhitekture i sisteme sa pristupom internetu, jer smatramo da je ova arhitekturna komponenta na savremenim univerzitetima najzastupljenija.

Pogledajmo sada scenarije koji su specifični za pomenutu arhitekturu.

Scenario	Metod prevencije
Gubitak podataka ili izmena podataka	
Namerno i neautorizovano uništenje podataka	Treba imati ažurne rezervne kopije (backup) Treba koristiti sistemske dnevnike (log files)
Neautorizovano priključenje radnih stanica u mrežu	Treba postaviti i koristiti pravila i politike mreže. Administrator ne sme odstupati od pravila.
Administrator neovlašćeno pristupa korisničkim podacima	Treba koristiti fizički odvojene sisteme za proizvodnju i eksploataciju. Treba da se uvede «pravilo dva čoveka» kod pristupa osetljivim informacijama. Dodeljivanje administrativnih privilegija (root ili administrator nalozi) treba da bude restriktivno.
Neautorizovan pristup mreži	Uvesti i sprovesti pravila modemskeg ili drugačijeg pristupa mreži. Koristiti firewall. Koristiti sisteme za otkrivanje neovlašćenog pristupa (intrusion detection systems)
Hacking	Definisati i sprovoditi sve navedene politike i pravila.

Tabela 5: Analiza scenarija za cilj: LAN sistemi sa pristupom internetu

2.2. Politike prevencije

Prema [1] nalazimo da se politike korišćenja IT resursa na akreditovanim američkim univerzitetima mogu kategorizovati kao eksplicitna regulativa :

1. Individualnih privilegija
2. Institucionalnih privilegija
3. Individualnih odgovornosti
4. Institucionalnih odgovornosti
5. Čuvanje arhiviranih podataka
6. Bezbednosti sistema i podataka
7. Tajnosti podataka
8. Zloupotreba sistema
9. Performansi sistema
10. Mrežnih resursa

11. Restitucije izgubljenih podataka
12. Ostalih aspekata upotrebe IT resursa

Interesantno je pogledati i detalje navedenih kategorija

Kategorija	Tretirani aspekti
Individualne privilegije	Privatnost, sloboda izražavanja
Institucionalne privilegije	Pravo upravljanja resursima
Individualne odgovornosti	Pravila pristojnosti, pravila korespondencije, definicija uznemiravanja, poštovanje copyrighta
Institucionalne odgovornosti	Prijava krivičnog dela, poštovanje privatnosti
Čuvanje arhiviranih podataka	Čuvanje u skladu sa propisima
Bezbednost sistema i podataka	Fizička bezbednost, bezbednost korisničkih imena i lozinki, bezbednost datoteka, bezbednost sistema, pristupa sistemu, bezbednost administrativnih podataka, bezbednost diskova, bezbednost mreže i servera, bezbednost radnih stanica i identifikacionih kartica.
Tajnost podataka	Tajnost administrativnih podataka
Zloupotreba sistema	Zloupotreba štampe, zloupotreba javnih resursa, zloupotreba sistema, administrativnih podataka, radnih stanica, mreže
Performanse sistema	Pravila kolegijalnog ponašanja
Mrežni resursi	Opšte zloupotrebe mrežnih resursa, neovlašćeno objavljivanje podataka, korišćenje diskusionih grupa i kreiranje web lokacija za vanfakultetske svrhe
Restitucija izgubljenih podataka	Pravila za sistemsko osoblje
Ostali aspekti upotrebe IT resursa	Pravila korišćenja administrativnih podataka, pravila korišćenja elektronske pošte

3. Zaključak

Zapitajmo se: kolika je korist od primene navedenih politika i pravila? Da bismo odgovorili na to pitanje, možda je bolje da idemo korak unatrag i da se potsetimo elementarnih činjenica: univerzitet je sredina iz koje diplomirani studenti odlaze u profesionalnu praksu; a ta se praksa dešava u strukturiranim organizacijama-firmama. Potsetimo se da je ceo ciklus preventivnih aktivnosti, već pomenut u ovom radu i definisan kao niz:

- Analiza rizika
- Definisanje bezbednosnih politika
- Definisanje bezbednosnog plana
- Izbor bezbednosne arhitekture
- Implementacija

Smatramo da je za univerzitetsku sredinu veoma važna implementacija politika na način definisan u ovom radu, a to znači: bazirano na best practices pristupu i usvojenim standardima, formalizovano i organizovano, ugrađeno u organizaciju i prihvaćeno kao korisno u organizaciji.

Međutim, po našem mišljenju još je važnija obrazovna uloga univerziteta u ovom smislu: jednom viđena i prihvaćena praksa implementirana na univerzitetu biće model i matrica diplomiranim studentima u njihovim organizacijama.

Možemo zaključiti da:

Univerzitetska sredina predstavlja dobar izbor za implementaciju bezbednosnih politika definisanih i tretiranih u ovom radu;

iskustva pokazuju da je metod prikazan u ovom radu superioran u odnosu na nesistematske metode prevencije rizika i metode fokusirane na ulogu pojedinca [4];

razumno je pretpostaviti da će diplomirani studenti u većem delu hteti da prenesu dobra iskustva sa univerziteta u svoje organizacije.

Literatura:

1. Oribello, Anne(ed.): *A Survey of Selected Computer Policies from Institutions of Higher Education*, Brown University, 1996.
2. <http://www.interpol.int/Public/TechnologyCrime/CrimePrev/ITSecurity.asp#5>
3. Caruso, Judith B: *Information Technology Security: Governance, Strategy and Practice in Higher Education*, ECAR 2003
4. <http://www.interpol.int/Public/TechnologyCrime/CrimePrev/companyChecklist.asp>