DOI 10.7251/ZRPIM2001365K

PRETHODNO SAOPŠTENJE – PRELIMINARY COMMUNICATION

ZAŠTITA OD CYBER NAPADA I PRIJETNJI

Alen Kamiš

Visoka škola za uslužni biznis Istočno Sarajevo - Sokolac, Cara Lazara bb 71350 Sokolac. Istočno Sarajevo, Bosna i Hercegovina, alen.kamis@mibo.ba

APSTRAKT

Ovaj rad obrađuje tehnologije koje su potrebne za zaštitu informacionog sistema. Cyber napadi su sve učestaliji i potrebno je posvetiti puno pažnje u zaštiti od istih. Kroz rad objasnit će se osnovne zaštite IT sistema i podataka.

U današnjem poslovanju konkurentnost na tržištu postiže se prvenstveno zahvaljujući kvalitetnim pozadinskim procesima i velikoj automatizaciji istih. Za automatizaciju pozadinskih procesa neophodan je informacioni sistem.

Ključne riječi: Informatička sigurnost, informacioni sistem, podatci, informatička oprema, računarska mreža.

UVOD

Živimo u doba velikih cyber napada, gdje napadači ne biraju institucije. Vidimo to u svakodnevnim napadima gdje se napadaju podaci državnih institucija, vojnih institucija, elektro kompanija, pa čak i bolnica. Cilj napadača često nije uništiti podatke vlasnika, već od vlasnika izvući neku korist ucjenom (Jon Erickson,2008). Najpoznatiji napadi tog tipa su napadi putem Ransomware virusa.

Da bi kompanija ostvarila konkurentnost na tržištu, potrebno je da ima kvalitetan sistem koji će omogućiti zaposlenima da kvalitetno izvršavaju svoje poslovne zadatke. Tržište zahtjeva veliki protok informacija i dobru saradnju svih zaposlenika. Kako bi ovo bilo ispunjeno potrebna je računarska mreža. Posebno treba obratiti pažnju na zaštitu podataka i cjelokupnog sistema.

Naredni tekst sadrži informacije potrebne za razumijevanje osnovnih pojmova o računarskim mrežama i sistemima.

Računarska mreža predstavlja skup hardverskih mrežnih uređaja (router, swich, firewall i slično) kao i ostalih uređaja (računari, laptopi, tableti) koji su povezani preko komunikacionih kanala (bakarni ili optički kablovi, radio talasi). Omogućava brzo i efikasno dijeljenje resursa i informacija između korisnika. Korisniku osigurava povezivanje svih lokacija i računara od interesa(Kevin Mitnick, et al, 2017).

IT sistem predstavlja upotrebu računarskih tehnologija sa svrhom upravljanja informacijama. U velikim kompanijama, odjeli zaduženi za upravljanjem IT sistema (IT odjeli) izvršavaju obaveze vezane za pohranjivanje, zaštitu, obradu i prenos podataka. Kvalitetna IT infrastruktura osigurava organizaciju internih dokumenata po odgovarajućim pravilima. Također, omogućava i primjenu odgovarajućih sigurnosnih postavki kao i kontrolu pojedinih zaposlenika.

Dizajn, implementacija i upotreba IT sistema omogućava lakše rješavanje različitih ljudskih i organizacijskih poslovnih problema. Na taj način povećava se efikasnost rada korisnika IT sistema. IT sistem se može podijeliti na nekoliko osnovnih funkcionalnih cjelina:

- Mrežni uređaji (router, firewall i switch uređaji), kablovi i razvodni paneli (patch paneli);
- Klijentski i serverski računari;
- Operativni sistemi i aplikacije.

NAPADI

Cyber napadi su napadi na informacione sisteme korisnika gdje je cilj napraviti krajnjem korisniku neki vid štete, npr. nedostupnost sistema, kriptovanje podatka, krađu podataka, i slično.

Kada govorimo o vrsti cyber/ hakerskim napadima možemo ih podijeliti na DDoS napade i viruse (Kevin Mitnick, 2011). Cyber napadi omogućavaju napadaču da ilegalno dobije pristup nekom uređaju, sistemu ili mreži žrtve, kako bi izvršio neku nedozvoljenu radnju. Postoji čitav spektar različitih vrsta napada koje napadač može pokrenuti. Napadi se biraju i zavise od toga šta je krajnji motiv napadača, kao i to koji napad može da bude efektivan u odnosu na otkrivenu "rupu" u sistemu žrtve (slika 1).

U daljem tekstu nabrojani su najčešći napadi i prijetnje.

• **Distributed Denial of Service (DDoS)** je napad na neki kompjuterski servis s ciljem da se korisnicima onemogući njegovo korištenje.

• **Botnet** je napad prilikom kojeg je više računara zaraženih nekim trojanskim konjem ili "crvom" koje je moguće kontrolisati i iskoristiti na način da svi računari istovremeno pošalju veliki broj zahteva na neku IP adresu s ciljem upada u računarski sistem ili zagušenja istog.

• **Backdoors (Backdoor)** napadi najčešće koriste dokumentovani (Exploit) žrtvinog računara. Kada haker uspije pristupiti žrtvinom računaru, isti instalira softver za backdoor koji mu omogućava stalnu vezu sa napadnutim računarom, kao i sposobnost manipulacije žrtvinog računara, među kojima su promjena podataka, pristup sistemu, kontrola audio i video ulaza (web kamera i mikrofon) i slično.

• **Direct-access Attack** zahtjeva da napadač ima fizički pristup računaru žrtve prilikom čega instalira keylogger, virus, ili trojanski konj preko USB-a ili putem Interneta te dobije potpunu kontrolu nad računarom.

• **Ransomware** je vrsta napada u kojoj haker napada mrežu, dobija pristup istoj i potom je zaključava (kriptuje podatke). Nakon kriptovanja podataka, haker stupa u kontakt s vlasnikom i traži otkup kako bi otključao (dekriptovao) server ili računar. U principu, Ransomware je sličan otmici, samo što su "taoci" serveri i baze, a ne ljudi.

• **Trojan Horses (Trojanski konj)** ili kraće trojanac je maliciozni računarski program koji se lažno predstavlja kao neki drugi program s korisnim ili poželjnim funkcijama. Većina trojanaca ima nazive vrlo slične uobičajenim korisničkim programima ili posebno primamljivim aplikacijama (Michael Sikorski et al, 2012).

Slika 1. Izgled code-a kad se vrši napad

ZAŠTITA INFORMACIONOG SISTEMA

Firewall

Firewall kao tehnologija je jedna od osnovnih zaštita, iako bismo mogli reći i glavna zaštita, informacionog sistema. Firewall uređaji mogu biti software-ski ili hardware-ski. Prije nekoliko godina prezentovani su novi tipovi firewall-a koji se nazivaju Next-Generation Firewall.

Next-Generation Firewall je treća generacija firewall uređaja koji je znatno povećao nivo zaštite informacionog sistema. U Next-Generation Firewall ubačeni su funkcionalnosti DPI (deep

packet inspection) koji podrazumjeva SSL inspekciju, inspekciju aplikacija, kontrola sadržaja, i IPS (intrusion prevention system). Zadnjih godina Next-Generation Firewall, osim na edge dijelu (dio sa izlazom prema Internetu), sve više se koristi i za lokalnu mrežu gdje se vrši filtriranje saobraćaja (port-ova i IP adresa).

Većina ovih novih firewall rješenja podržava i visokodostupnu opciju, gdje su dva ili više firewall uređaja povezana i čine jednu cjelinu (cluster). Next-Generation Firewall tehnologija može software-ski biti podijeljena na dva ili više firewall-a putem virtual domain tehnologije ili konteksta, ovisno od terminologije proizvođača opreme.

Core mreža

Jezgrene mreže (Core networks) su srž svakog mrežnog rješenja i kao takve osnova su za pružanje mrežnih i aplikativnih servisa. Core mreže omogućavaju brzo i efikasno usmjeravanje IP prometa do krajnjih uređaja i zbog toga predstavljaju jedinstveno rješenje za prijenos podataka, zvuka, slika, video i upravljačkih signala.

Switch je uređaj koji upravlja protokom podataka između dijelova lokalne mreže (LAN). Za srce mrežne komunikacije obično se uzimaju L3 (Layer 3) switch uređaji. Kod ovih switch uređaja visokih performansi, moguće je implementirati i visokodostupno opciju. Pojam "stack" znači da uređaj posjeduje tehnologiju spajanja više istih fizičkih uređaja u jednu logičku cjelinu koja dijeli jedan konfiguracioni file. Na L3 switch uređajima moguće je implementirati i core route-ranje cjelokupne mreže korisnika, koristeći i neke od naprednih routing protokola (OSPF, EIGRP). Na ovakvim switch uređajima, u svrhu zaštite, bile bi implementirane opcije zaštite segmentacije mreže, primjena kontrole prometa ka pojedinim mrežnim segmentima, te implementacija naprednih funkcionalnosti mrežne sigurnosti kao što je autentifikacija korisničkih računara, kontrola zagušenja, DHCP snooping, dinamička ARP inspekcija i slično. Preporuka je da se na Core i access switch uređajima implementira 802.11x autentifikacija, koja ne dozvoljava pristup lokalnoj mreži radnim i stanicama koji nisu autorizovane domenski (kerberos, certifikat, i slično).

Bežični internet pristup

Wi-Fi (Wireless-Fidelity ili IEEE 802.11) je bežična mreža gdje se podaci između dva ili više računara prenose pomoću radio frekvencija (RF) i odgovarajućih antena. Ovakva mreža se najčešće koristi za pristup unutar LAN mreže, ali se u posljednje vrijeme sve više nudi i bežični pristup WAN mreži, odnosno Internetu. Najveće prijetnje kod korištenja WI-FI mreže, su veoma česta pojava dokumentovanih BUG-ova na hardware-skim uređajima (WI-FI access point-i) i online tutorijali nudeći rješenje kako hackovati WI-FI autentifikaciju (najčešće WEP, WPA i WPA2). U svrhu zaštite lokalnih podataka od WI-FI upada, predlaže se uvođenje minimalno dvije odvojene WI-FI mreže. Prva je izričito namijenjena gostima. Mreža za goste može koristiti i slabiji vid autentifikacije (minimalno WPA2), ali mora biti izolovana u posebnom mrežnom subnet-u, koji ima isključivo pristup Internetu i naravno ograničen pristup Internetu brzinom, port-ovima i kontrolom sadržaja. Prilikom izrade dizajna za WI-FI namjenjenom uposlenicima, jedino prihvatljivo rješenje je 802.11x autentifikacija, koja ne dozvoljava pristup lokalnoj mreži uređajima i radnim stanicama koji nisu autorizovani na domeni (kerberos, certifikat, i slično). Osim pažnje usmjerene na WI-FI autentifikaciju, potrebno je i vršiti redovna ažuriranja software-a na WI-FI Access Point-ima i kontrolerima.

Server – storage infrastruktura

Server – Storage infrastruktura je oprema na kojoj su smješteni podatci. U zadnjih deset godina sve je manje fizičkih instalacija servera (bare metal). Većina instalacija servera u svijetu iskorišteno je za virtualizacijsku platformu. Dijeljeni diskovni prostor služi za pohranu podataka generiranih od strane jednog ili više servera ili korisnika. Dijeljeni diskovni prostor odlikuje se visokim performansama kao i visokom dostupnošću (svi uređaji su redundantni: napojne jedinice, kontroleri i slično). Idealan je za korištenje prilikom uspostave visoko dostupnog sistema. U kombinaciji sa dva servera i dijeljenim diskovnim prostorom čine jednu visoko dostupnu platformu (dva servera, dijeljeni diskovni prostor sa virtualizacijom = potpuno funkcionalni visokodostupni sistem, odnosno Cluster). Cyber napadi i prijetnje za ovakve sisteme obično se obavljaju primjenom dokumentovanih

BUG-ova na hardware-skim uređajima. Također prijetnje na ovim sistema mogu se naći i na pokušajima upada putem neautorizovane autentifikacije na serversku – storage platformu ili virtualizaciju (Keyloggeri ili Brute-Force pokušaji). Passwordi na ovim sistemima moraju biti vrlo kompleksni (dužina password-a treba biti minimalno 12 karaktera, a isti treba sadržati veliko i malo slovo, broj i specijalni karakter). Preporuka je da je server -storage infrastruktura redovno održavana, odnosno da su redovno izvršena ažuriranja Firmware-a i primjena patch-eva za hardware-sku platformu. Po pitanju software-ske platforme, preporuka je da su virtualna platforma, operativni sistem i aplikacije redovno održavani na zadnjoj preporučenoj verziji (preporuka je i korištenje WSUS servera). Pored preporuka za korištenje zadnje dostupne verzije operetivnog sistema, na podržanim serverima i radnim stanicama obavezno je instalirati i neko od endpoint security rješenje.

EndPoint Security rješenja

EndPoint Security software (antivirusni softver ili antivirus) je kompjuterski software koji služi za zaštitu, identifikaciju i uklanjanje računarskih virusa, kao i svog ostalog software-a koji može da nanese štetu računarskom software-u. U zadnje vrijeme antivirusna rješenja sadržavaju i module kao što su Device kontrola, Application kontrola, Web kontrola, Firewall MDM kontrola, te su upravoiz tog razloga ova rješenja nazvana EndPoint Security rješenja. Preporuka je da se iskoriste sve dostupne mogućnosti EndPoint Security rješenja koje bi mogle pomoći u zaštiti od cyber napada i prijetnje. Neka EndPoint Security rješenja posjeduju i integraciju sa firewall rješenjima, gdje je integrirana zaštita u jednu upravljačku konzolu pa tako imaju još bolju zaštitu i upravljanje. Pored integracije sa firewall-om neka rješenja također posjeduju integraciju sa još naprednijim endpoint rješenjima koja se većinom nalaze u cloud-u a lokalne instalacije antivirusnog software su iskorištene kao senzori za detekciju. Jedan od novijih modela naprednog EndPoint Security rješenja je Endpoint detection and response (EDR) rješenje.

Antispam rješenja

Preko pola svih svjetskih virusnih zaraza dogodi se putem otvaranja nepoznate e-mail poruke. Preporuka je da se e-mail poruke od nepoznatog pošiljaoca i sumnjivog sadržaja ne otvaraju, već da se odmah obrišu ili obavijesti osoblje iz IT odjela (Hadnagy, C, 2010). Da krajnji korisnici ne bi primali ili bar primali manje neželjenih e-mail poruka, preporuka je implemenacija antispam rješenja. Antispam rješenja su software-i koji presretnu problematičnu email poruku, na uređaju sa instaliranim antispam rješenjem je izvršeno skeniranje poruke, i samo ako je poruka označena kao sigurna ista je proslijeđena krajnjem korisniku. Ako je e-mail poruka označena kao sumnjiva ili zaražena, istaje automatski obrisana ili ostavljena u karantenu. Antispam rješenja osim skeniranja na viruse posjeduju i druge nivoe zaštite i testiranja kao što su testiranje reputation domain, sender policy framework (SPF), Domain Keys Identified Mail (DKIM), i Domain-based Message Authentication, Reporting & Conformance (DMARC). Implementacijom ovih dodatnih opcija znatno je smanjen broj primljenih neželjenih poruka (spam poruka).

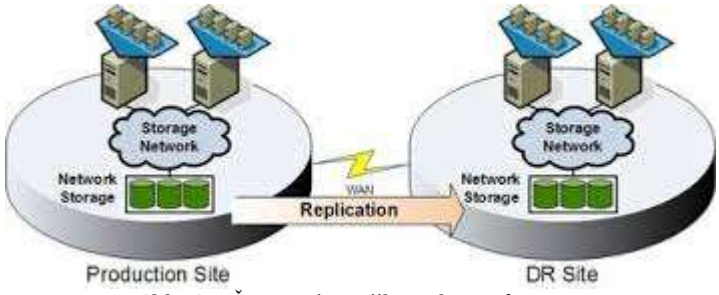
Backup software

Backup software predstavlja zadnji vid zaštite informacionog sistema i njegova namjena je da, u slučaju napada i pristupa hakera lokalnoj mreži, omogući korisniku povrat podataka iz posljednje generisane sigurnosne kopije. Naprednija backup software rješenja mogu i vršiti povrat fizičkih i virtualnih servera pomoću instant restore opcije (u kom slučaju server je dostupan u periodu cca 2 minute iz sigurnosnih kopija). Pored toga, ova rješenja omogućavaju i granularni povrat podataka, odnosno povrat pojedinačnih datoteka, mail poruka, mailbox-ova, korisnika unutar AD-a, baze podataka ili tabele iz baze podataka. Preporuka je da se zbog bolje zaštite prilikom konfiguracije backup software koristi pravilo 3-2-1 (slika 2). Pravilo 3-2-1 je da je uvijek sačuvano 3 kopije vaših podataka, na 2 različita medija i na 1 off-site mediju.

Slika 2. Šematski prikaz pravila 3-2-1

Replikacijski software

Kontinuirana zaštita podataka i dostupnost se povećava replikacijski software-om. Isti služi za replikaciju produkcionih servera na resurse drugog data centar site-a (DR site). Replikacijski software prvenstveno prestavlja vid zaštite, podatka kompanije kada je primarni data centar nedostupan uslijed hardware-skih greški, požara, poplava, hakerskih napada i slično (slika 3).



Slika 3 - Šema rada replikacijskog software-a

ZAKLJUČAK

Sadržaj ovog rada iznosi rezultat dugogodišnje edukacije i iskustva autora. U istom su opisani osnovni koncepti cyber napada i prijetnji, te kako se zaštititi od istih.

U eri "cloud" rješenja, uznapredovale IT tehnologije, svaka kompanija bi trebala pratiti trendove i najbolje svjetske prakse po pitanju dizajna sigurnosti IT sistema. IT sistem mora biti redovito održavan i obnovljen da bi ispravno funkcionisao. Redovnim održavanjem IT infrastrukture poboljšava se sigurnost i dostupnost IT sistema, a time i produktivnost i fleksibilnost radnika. Kao zaključak može se reći da je potrebna kontinuirana edukacija zaposlenika u vezi informacione sigurnosti, da bi rizik od neželjenih upada u informacioni sistem bio maksimalno umanjen. Pored edukacije korisnika veoma je bitno da kompanije nabavkom odgovarajuće opreme i održavanjem iste, ulažu u informacionu sigurnost.

LITERATURA

Hadnagy, C. (2010). *Social engineering: The art of human hacking*. John Wiley & Sons.

Gibson, D. (2011). CompTIA Security+: Get Certified Get Ahead: SY0-201 Study Guide. *North Charleston, SC: CreateSpace*.

Erickson, J. (2008). *Hacking: the art of exploitation*. No starch press.

Mitnick, K. (2017). *The art of invisibility: The world's most famous hacker teaches you how to be safe in the age of big brother and big data*. Little, Brown.

Mitnick, K. (2011). *Ghost in the wires: My adventures as the world's most wanted hacker*. Hachette UK.

Sikorski, M., & Honig, A. (2012). *Practical malware analysis: the hands-on guide to dissecting malicious software*. no starch press.

Singh, S. (2003). The code book. The science of secrecy from ancient Egypt to quantum cryptography. *Swiat Ksiazki*, 19-21.

CYBER ATTACK AND THREAT PROTECTION

Alen Kamiš

The College of Service Business, Cara Lazara bb, 71350 Sokolac, Istočno Sarajevo, Bosna i Hercegovina, alen.kamis@mibo.ba

ABSTRACT

This paper covers technologies needed for protection of an IT System. Cyber attacks are more frequent then ever and lots of attention should be given to protection from these attacks. This paper covers basis of protecting an IT system and data.

In today's business a competitiveness is maintained mainly by high quality back-office processes and large automatization of those processes. For automatization of business processes an IT system is mandatory.

Keywords: Information safety, information system, data, information equipment, computer network