PREVENCIJA CURENJA PODATAKA

PREVENTION OF DATA LEAKAGE

MSc Nataša Simić, MSc Nevena Miladinović, mr Zoran Živković

Towers Net d.o.o.

Abstrakt: *U doba modernih tehnologija sve više informacija se čuva u bazama podataka i u vidu elektronskih dokumenata. Ovaj pristup omogućuje brzo i lako deljenje informacija sa poslovnim partnerima i klijentima bez obzira na njihovu lokaciju. Sa druge strane, jedan od ključnih problema predstavlja curenje podataka. Hakerski napadi na veb aplikacije i baze podataka, ljudske greške, krađa ili gubljenje hardverskih medijuma su samo neke od situacija koje mogu dovesti do curenja podataka. U ovom radu je dat pregled uzroka i posledica curenja podataka kao i opis sistema koji se mogu koristiti u cilju prevencije ovog problema.*

Ključne reči: *curenje podataka, SQL injection, Cross-site scripting, IRM, WAF*

Abstract*: In the age of modern technologies more and more information is stored in databases and digital documents. This approach enables fast and simple sharing of information with business partners and clients regardless of their location. On the other hand, one of the main problems is data leakage. Hacker's attack on web applications and data bases, human errors, theft and hardware medium loses are some of situations that can cause data leakage. This paper will describe some of causes and consequences of data leakage. Also, it gives description of systems that can be used for prevention of this problem.*

Key words: *data leakage, SQL injection, Cross-site scripting, IRM, WAF*

1.UVOD

Otkrivanje osetljivih poslovnih podataka, može da ima ozbiljne posledice po poslovanje jedne kompanije, njenu reputaciju ili čak opstanak. U pitanju mogu da budu osetljive poslovne informacije ili intelektualna svojina čije otkrivanje narušava uspeh daljeg poslovanja kompanije, ili finansijski i lični podaci klijenata na čije čuvanje je kompanija obavezna.

Najveći rizik po poverljive poslovne informacije predstavlja pojam curenja podataka, tj neprimetno iznošenje podataka van granica sistema kojem pripadaju. Curenje podataka se definiše kao neautorizovana transmisija informacija (ili podataka) iz organizacije (kompanije, institucije) ka eksternoj adresi ili primaocu [1].

Za adekvatan pristup rešavanju ovog problema potrebno je shvatiti njegove uzroke, bilo da su oni tehnički ili pripadaju ljudskoj prirodi i ponašanju. Odgovor na tehničke izazove treba da prati razvoj rastućeg broja pretnji ali tako da bude u skladu sa svim aspektima organizacije poslovanja. Samo tako osetljive informacije mogu da budu sprečene da napuste granice sistema bez većeg opterećivanja poslovnih procesa.

2. UZROCI I POSLEDICE CURENJA PODATAKA

Sa aspekta intencije curenje podataka može da bude namerno ili slučajno.

Namerno curenje izazvano je od strane napadača koji ima korist od podataka koje preuzima. Sa tehničkog aspekta može da ima različite uzroke. Umetanje zlonamernog softvera poput *spyware*-a ili *backdoor*-a omogućava napadaču da neovlašćeno pristupi sistemu i preuzme osetljive podatke. Slično se može postići presretanjem kriptografski nezaštićenie komunikacije ili običnom fizičkom krađom hardverskog mediuma koji sadrži nezaštićene podatke (laptop, USB, prenosni hard diskovi).

Osim toga, curenje može biti posledica zlonamerne aktivnosti jednog od zaposlenih koji ima pristup sistemu sa određenim stepenom autorizacije. Najčešći uzroci ovakvog ponašanja su nezadovoljstvo na poslu, čak 92%, ali u pitanju mogu da budu i industrijska špijunaža i finansijska dobit. [2]

Slučajno curenje podataka je uglavnom uzrokovano nepažnjom, nemarom ili neinformisanošću zaposlenih koji nemaju za cilj nanošenje štete. Zapravo, istraživanja pokazuju da je ovo mnogo češći uzrok (99%) kada su unutrašnji rizici u pitanju. [2]

Dominantni problem je slanje osetljivih dokumenata putem elektronske pošte primaocu koji nema pravo uvida u primljene podatke ili gubitak prenosnog hardverskog medijuma sa osetljivim sadržajem. Zaposleni mogu biti nesvesni rizika pri nepromišljenom slanju dokumenata jer, na primer, nisu upoznati sa nivoom osetljivosti podataka koje dokumenta sadrže, rizicima koji postoje ako se ti podaci otkriju ili bezbednosnom politikom kojom je definisana njihova upotreba. Uz to, uvek postoji mogućnost slučajne greške pri slanju usled nepažnje ili zamora.

Posledice gubitaka podataka mogu biti direktne ili indirektne. Direktne posledice se mogu sagledati na konkretan finansijski način. One nastaju nakon gubitka ličnih i finansijskih podataka klijenata. Kompanije kojima su podaci ukradeni primorane su da plaćaju visoke odštete i zakonom propisane kazne. Indirektne posledice je teže sagledati jer se javljaju tokom dužeg perioda i njihovu finansijsku težinu ne možemo uvek precizno da odredimo. Ove posledice nastaju nakon gubitka kritičnih poslovnih podataka i intelektualne svojine a uzorkuju narušavanje reputacije kompanije, okretanja klijenata ka konkurentim kompanijama i smanjivanje obima poslovanja.

3. PREVENCIJA CURENJA PODATAKA

Prevencija curenja podataka treba da bude usmerena ka najrizičnijim aspektima poslovne prakse. U ovom radu fokus je stavljen na dva zasebna rizika: baratanje osetljivom poslovnom dokumentacijom i očuvanje integriteta baza podataka.

3.1 ZAŠTITA ELEKTRONSKE DOKUMENTACIJE

Zaštita elektronskih dokumenata se može obaviti strogom kontrolom pristupa i dodelom dozvola odnosno pristupnih prava za svaki dokument. Tehnika dodele prava za pristup i manipulaciju dokumentima naziva se IRM (*Information Rights Management*). IRM predstavlja skup tehnologija za zaštitu osetljivih informacija od neovlašćenog pristupa. Sistemi koji su zasnovani na IRM tehnologijama rade na principu dodeljivanja prava pristupa korisnicima sistema. Administrator IRM sistema bi trebalo da ima mogućnost dodele prava odnosno dozvola za pristup dokumentu, modifikaciju, kopiranje, štampanje, *screenshot* i slično. Takođe, IRM sistemi bi trebalo da pružaju mogućnost klasifikacije dokumenata prema stepenu osetljivosti. Osim radnji koje korisnik može da sprovodi nad dokumentima IRM sistemi bi

trebalo da imaju i mogućnost definisanja dozvola za vremensko trajanje dokumenta i lokacija sa kojih se pristupa dokumentu. Administrator može postaviti rok trajanja dokumenta pri čemu se, nakon isteka tog roka, blokira pristup. Dozvole koje se odnose na lokaciju sa koje se pristupa dokumentu mogu biti definisane na osnovu serijskog broja uređaja ili IP adrese. Nakon dodele dozvola za pristup datoteci, IRM sistem vrši enkripciju te datoteke kako bi se sprečio neovlašćeni pristup.

Kod većine IRM sistema samo administrator može da dodeljuje, uklanja i modifikuje dozvole. Jednom dodeljene dozvole bi trebalo da ostanu trajno na zaštićenoj datoteci bez obzira na način deljenja i platforme sa koje se pristupa toj datoteci. Permanentnost pristupnih prava odnosno dozvola sprečava curenje poverljivih podataka u slučaju krađe ili gubitka prenosnih hardverskih medijuma. Naime, ukoliko dođe do gubitka ili krađe prenosnog medijuma (USB, hard disk) bilo koji korisnik koji pokuša da pristupi zaštićenim datotekama na tom medijumu neće biti u mogućnosti da to učini ukoliko nema definisana pristupna prava. Osim toga, sistem za zaštitu datoteka treba da ima mogućnost praćenja zaštićenih datoteka odnosno treba da pruži administratoru uvid u sve akcije izvršene nad dokumentom uključujući i pokušaje neovlašćenog pristupa. Ukoliko dođe do krađe ili gubitka zaštićenih datoteka administrator će imati informaciju o pokušajima neovlašćenog pristupa kao i o svim akcijama koje napadač ili sličajni pronalazač pokuša nad zaštićenim datotekama.

Radi autentifikacije korisnika i praćenja aktivnosti zaštićenih dokumenata poželjno je da IRM sistem ima mogućnost integracije sa LDAP sistemom kao što je *MS Microsoft Windows Active Directory*, *IBM Tivoli Directory Services* i slično. IRM sistemi bi trebali da imaju i mogućnost integracije sa softverskim paketima koji se koriste u poslovnom okruženju kao što su sistemi za prevenciju gubitaka podataka, poslovne komunikacije i upravljanje dokumentima.

Jedno od vodećih svetskih IRM rešenja je rešenje *Seclore FileSecure* kompanije *Seclore* iz Indije. Ovo rešenje je ima mogućnost integracije sa LDAP sistemima kao što je *MS Microsoft Windows Active Directory*. Fleksibilnost sistema se ogleda u činjenici da sva ugrađena pravila i klasifikacije mogu da se menjaju i prilagode bilo kom poslovnom okruženju.

Seclore FileSecure pruža mogućnost dodele svih standardnih dozvola koje IRM sistem treba da podržava. Dozvole koje su definisane ovim sistemom ostaju na zaštićenoj datoteci sve dok ih administrator ne ukloni ili modifikuje i ne zavise od načina deljenja datoteke i platformi koje se koriste za pristup. Nakon dodele dozvola datoteka biva enkriptovana kako bi se sprečio neautorizovani pristup i može se podeliti sa drugim korisnicima. Čak i posle deljenja datoteke sa drugim korisnicima administrator može da modifikuje, ukine ili postavi novu dozvolu na datoteku bez potrebe za ponovnim deljenjem jer se sve promene rade na serveru samog sistema.

Za pristup datotekama zaštićenim *Seclore FileSecure* sistemom korisnik mora da se autentifikuje svojm korisničkim imenom i lozinkom. Zaštićenim datotekama se može pristupati preko *Seclore* aplikacije i tada se datoteka otvara u svojoj matičnoj aplikaciji (*word, excel, adobe*…). Drugi način pristupa datoteci je preko veb pregledača i na taj način datoteka može samo da se pregleda ali ne i da se modifikuje. Ukoliko se zaštićena datoteka šalje korisniku koji još uvek nije u sistemu njegov profil će automatski biti generisan i on će dobiti e-mail obaveštenje o prijemu zaštićene datoteke i načinu pristupa datoteci.

Administrator, preko upravljačke konzole, ima uvid u sve akcije sprovedene nad zaštićenom datotekom. U tabelarnom prikazu aktivnosti dat je pregled akcija preduzetih nad zaštićenom datotekom, vreme i datum kao i trenutno i

originalno ime datoteke i sve to je povezanom sa odgovarajućim korisnikom. Ukoliko korisnik pokuša da izvede akciju za koju nema dozvolu ili da neovlašćeno pristupi datoteci administrator će dobiti e-mail obaveštenje o tome a korisnik će na ekranu dobiti upozorenje.

Seclore FileSecure podržava rad sa brojnim tipovima datoteka kao što su *MS Office* (.doc, .docx, .xls, .ppt, .pptx), *Adobe*, *AutoCad*, tekstualni i formati slika. Osim toga, ovaj sistem ima mogućnost integracije sa sistemima za upravljanje dokumentima kao što su *FileNet, SharePoint, Newgen* i *Documentum*, sistemima za prevenciju gubitaka podataka kao što su *Symantec, McAfee, Websence, GTB technologies* i *MyDLP* i sistemima za poslovnu komunikaciju kao što su *SAP, Lotus Notes* i *Outlook*. [3]

Fleksibilnost kod dodele pristupnih prava, kompatibilnost sa velikim brojem tipova podataka i mogućnost integracije sa poslovnim softverskim rešenjima su osobine koje ovaj sistem čine vrlo dobrim rešenjem za zaštitu elektronskih dokumenata.

3.2 ZAŠTITA BAZA PODATAKA

Poverljive informacije se, osim u vidu elektronskih dokumenata, mogu čuvati i u bazama podataka. Baze podataka na sajtovima su česta meta napada. Napadi na veb aplikacije smatraju se jednim od najvećih problema organizacija poput institucija zdravstvene zaštite, finansijskih institucija i banaka kao i kompanija koje u svom poslovanju koriste veb aplikacije. Napadači koriste *Cross-site scripting* (XSS) i *SQL injection* napade kako bi došli do poverljivih informacija o korisnicima koji se čuvaju u bazama podataka veb aplikacija.

Cross-site scripting (XSS) predstavlja jedan od najvećih bezbednosnih problema kad je reč o veb aplikacijama a samim tim je i jedan od najčešćih tipova napada jer eksploatiše ranjivosti u veb aplikacijama, serverima i *plug in-ovima*. Ovaj tip napada pripada klasi napada koji koriste tehniku insertovanja koda. XSS napadi se izvode tako što napadač insertuje maliciozni skript u legitimni sajt. Ovaj skript će se automatski izvršiti kada korisnik u svom veb pregledaču otvori zaraženu stranu. Pri svom izvršenju maliciozni skript može da pristupi svim osetljivim informacijama koje se razmenjiju između veb pregledača i zaraženog sajta (*cookies, season tokens*). Ova vrsta napada se koristi rad zaobilaženja kontrole pristupa i/ili kako bi se došlo do osetljivih informacija o korisnicima. [4]

SQL injection, takođe, pripada klasi napada koji koriste tehniku insertovanja koda. Naime, napadač menja ključne reči ili operatore u već postojaćem SQL upitu kako bi došao do informacija koje se nalaze u bazi podataka. SQL ranjivosti opisane su kao jedna od najozbiljnijih pretnji po veb aplikacije i servere. Veb aplikacije i serveri koji su ranjivi na ovu vrstu napada otvaraju mogućnost napadaču da pristupi celokupnim bazama podataka koje se na njima nalaze. Ove baze podataka uglavnom sadrže osetljive informacije o klijentima i korisnicima pa posledice SQL injection napada mogu da budu krađa identiteta, gubitak poverljivih informacija ili finansijske prevare. [5]

Kako bi se zaštitile baze podataka na veb serverima i veb aplikacijama potrebno je, osim *firewall-a* i IPS sistema, postaviti i *Web Application Firewall* - WAF.

Firewall vrši nadzor i analizu saobraćaja na osnovu definisanih pravila, a IPS sistem odbija maliciozne pakete ali nijedan od ovih sistema nema mogućnost razumevanja logike veb protokola. Upravo iz tog razloga često napadači uspevaju da zaobiđu ove barijere i uspeju da dođu do podataka iz baza na veb serverima. WAF je dizajniran upravo da štiti veb aplikacije i servere od napada tako što analizira pakete na aplikativnom sloju odnosno vrši dubinsku analizu sadržaja odlaznih i dolaznih paketa.

WAF treba da bude ima mogućnost detekcije *SQL injection* i XSS napada ali i novih i nepoznatih napada odnosno *Zero day attacks*.

Napade nultog dana WAF detektuje uočavanjem neočekivanih ili neobičnih dešavanja nakon čega treba da bude u mogućnosti da blokira napad i pošalje upozorenje administratoru.

Sistem pogodan za zaštitu baza podataka na veb serverima je *Towers Net Defender* – TND. TND je sistem za detekciju i prevenciju upada sa integrisanim WAF-om. U ovom sistemu su objedinjene funkcionalnost IPS-a odnosno nadgledanje saobraćaja i blokiranje malicioznih paketa sa funkcionalnostima WAF-a odnosno analiza paketa na aplikativnom nivou. Shodno tome, TND štiti sistem od DoS i DDoS napada, *SQL injection*, XSS, *Brute-force* napada, *SYN floods*, *Zero day* napada i *rootkits-a*. Osim zaštite, TND ima i funkciju automatizovanog i prilagođenog izveštavanja o aktivnostima na mreži. Ovaj sistem pruža efikasnu zaštitu bazama podataka na veb serverima a ne usporava saobraćaj jer zahteva vrlo malo resursa (memorija, procesorsko vreme…). [6]

4. ZAKLJUČAK

Curenje podataka je jedan od najvećih problema današnjice. Kompanijama i institucijama koje rukuju osetljivim informacijama je u interesu da te informacije čuvaju na promišljen način jer posedice otkrivanja takvih informacija mogu da budu nesagledive. Krađa identiteta, finansijske prevare i krađa intelektualne svojine su samo neke od potencijalnih posledica curenja podataka. Osim ovih direktnih postoje i indirektne posledice kao što su kazne predviđene zakonom zbog nepropisnog čuvanja poverljivih podataka, gubitak intelektualnog vlasništva, narušavanje reputacije i slično. Sa aspekta kiber bezbednosti, najveće pretnje po osetljive podatke su loše baratanje poslovnom dokumentacijom, krađa/gubitak hardverskih prenosnih medijuma i kiber napadi kao što su *SQL injection* i *Cross-site scripting*. Ovi napadi ali i slučajne greške zaposlenih mogu se u znatnoj meri sprečiti primenom odgovarajućih sistema zaštite. Za kvalitetnu prevenciju curenja podataka neophodno je shvatiti sve faktore rizika i pravovremeno primeniti odgovarajući nivo zaštite u skladu sa svim aspektima poslovanja.

.

REFERENCE

[1] C. Eckstein, R. Carbone, *Preventing data leakage: A risk based approach for controlled use of the use of administrative and access privileges*, SANS Institute, 2015

[2] P. Gordon, D. Adrizanto Hindarto, *Data Leakage – Threats and Mitigation*, SANS Institute, 2007.

[3] Seclore FileSecure brošura, http://www.towersnet.rs/wp-content/uploads/2015/07/Seclore-flyer.pdf

[4] A.Vernotte, F. Dadeau, F. Lebeau , B. Legeard, F. Peureux, F. Piat, *Efficient Detection of Multi-step Cross-Site Scripting Vulnerabilities, 10th International Conference on Information Security Systems* (ICISS 2014), Indija, decembar 2014.

[5] W.Halfond, J.Viegas, A.Orso, *A Classification of SQL Injection Attacks and Countermeasures, IEEE International Symposium on Secure Software Engineering (ISSSE 2006)*, 2006.

[6] Towers Net Defender brošura, http://www.towersnet.rs/wp-content/uploads/2015/06/TND-flajer.pdf