Uloga IT revizije u sprečavanju APT napada

Rodoljub Kajganić,
Tehnički fakultet Mihajlo Pupin Zrenjanin
Banja Luka, Bosna i Hercegovina
rodoljub.kajganic@gmail.com

Biljana Radulović
Tehnički fakultet Mihajlo Pupin Zrenjanin
Zrenjanin, Srbija
biljana.radulovic66@gmail.com

Sažetak – ***U radu je opisan značaj IT revizije i doprinos u zaštiti sve više prisutnih IT prijetnji u obliku APT napada. IT revizija je funkcija koja je neophodna (često zahtjevana od samog regulatora) u svakoj kompaniji koja koristi informacione tehnologije. Kroz IT reviziju se vrši validacija kvaliteta internih kontrola i nivoa zaštite informacionih resursa. Zaštita informacionih resursa se uspostavlja radi očuvanja povjerljivosti, integriteta i dostupnosti, principa koji predstavljaju osnovna sigurnosna načela. IT prijetnje imaju za cilj da ugroze ova sigurnosna načela i omoguće ostvarivanje određenih koristi napadačima kojih ih iskorištavaju kroz specifične vrste napada od kojih je APT na globalnom nivou trenutno najdominantniji. Kroz rad su analizirane karakteristike APT napada, metodologije koje napadači koriste te uloga i značaj IT revizije kao jedne od funkcija koje značajno doprinose u sprečavanju IT prijetnji. Provodeći IT revizije testiraju se postojeće kontrole, otpornost na APT napade, daju se preporuke koje na osnovu autorovih praktičnih iskustava iz revizije i najboljih praksi predstavljaju trenutno jedini način zaštite.***

Ključne riječi-sigurnost; IT revizija; IT prijetnje; APT; osnovni sigurnosni principi;

I. UVOD

Nivo na kojem se trenutno nalaze informacione tehnologije je izuzetno visok i prisustvo informacionih tehnologija trenutno pronalazimo u većini poslovnih sfera kao i životu običnog čovjeka. Sam razvoj informacionih tehnologija je u zadnjih nekoliko godina dostigao značajne razmjere. Tokom ovako dinamičnog rasta i uticaja koji je sa sobom donio rastao je i rizik korištenja informacionih tehnologija. Složićemo se da opcija izbjegavanja korištenja informacionih tehnologija skoro da ni teoretski ne može da se razmatra a da se ne ugroze postojeći ciljevi u čiju svrhu se informacione tehnologije i koriste. Kao jedina mogućnost preostaje da postanemo u potpunosti svijesni rizika koji prate informacione tehnologije, da ih po mogućnosti izbjegnemo odnosno dovedemo na prihvatljiv nivo.

Koliki je velik obim rizika možemo utvrditi na primjeru narušavanja povjerljivosti 3,1 milijardi podataka u toku 2016. godine [1]. Čak i ovaj podatak treba uzeti sa rezervom jer se radi o javno poznatim slučajevima kompromitacije podataka, možemo pretpostaviti da je stvarni broj daleko veći. Narušavanje povjerljivosti podataka možemo posmatrati kroz više pojavnih oblika od kojih su najčešći krađa platnih kartica, preuzimanje identiteta, finansijski gubici, narušavanje državne sigurnosti, ugrožavanje privatnosti i slično. Svi navedeni rizici se pojavljuju pod djelovanjem IT prijetnji. Možemo konstatovati da smo ograničeni da djelujemo na mogućnost da određena IT prijetnja nastane i jedino što preostaje je uspostavljanje dovoljno kvalitetnih adekvatnih zaštitnih mjera koje će zaustaviti nastajanje rizika. Ovom cilju trebamo pristupiti sistematski i organizovano, trebamo sagledati sve resurse koje imamo na raspolaganju a možemo ih iskoristiti u borbi protiv IT prijetnji.

U samom početku moramo analizirati od kojih vrsta IT prijetnji treba da se zaštitimo. Analiza treba biti sveobuhvatna i mora imati kao rezultat identifikovane potencijalne oblike IT prijetnji i inventar resursa koji služe kao osnova za implementiranje zaštitnih mjera. Moramo skrenuti pažnju da se velika pažnja treba posvetiti na troškove jer određene zaštitne mjere (poput kupovine uređaja za detekciju internet napada) zahtijevaju značajna finansijska sredstva koja trebaju biti obezbjeđena. Da bi navedene aktivnosti bile pravilno izvedene, svoj objektivan i nezavisan sud daje IT revizija kroz kontrole koje provodi.

U radu ćemo analizirati karakteristike trenutno najznačajnije vrste IT prijetnji a to je trajna prijetnja (engl. Advanced persistent threat – APT). Tek ako uradimo pravilno sagledavanje karakteristika i metodologiju APT napada možemo da formiramo i implementiramo adekvatne zaštitne mjere. Nakon uspostavljanja zaštitnih mjera neophodno je imati validaciju i kontrolu gdje dolazimo do neophodnosti korištenja IT revizije koja kroz svoju ulogu testira kvalitet internih kontrola i daje potrebne preporuke da bi sistem zaštite bio efikasan.

II. IT PRIJETNJE

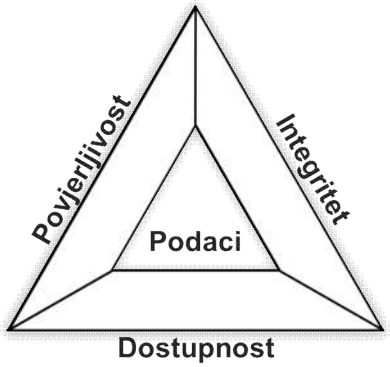
Analizirajući trenutnu situaciju na polju IT prijetnji možemo uvidjeti da nije dovoljno uspostaviti samo tehničke zaštitne mjere zato što aktuelne IT prijetnje zaobilaze ove sigurnosne mjere iskorištavajući ljudski faktor tehnikama socijalnog inženjeringa.

U zavisnosti od motiva napadača napadu su izloženi različite vrste podataka. Kategorije napadača koji ostvaruju najveći uticaj (u zavisnosti od njihovih motiva i sposobnosti) se kreću od organizovanih kriminalnih grupa (engl. cyber-criminals), grupa organizovanih od stranih obavještajnih agencija, političkih grupacija (engl. hactivists) do napadača motivisanih znatiželjom ili potrebom za dokazivanjem (engl. hackers).

Napadačima su na raspolaganju različiti alati i javno dostupni podaci. Uspjeh napada je direktno povezan vremenom trajanja napada. Opšte je poznata činjenica da ne postoji informacioni sistem koji nije ranjiv. Ranjivost svakako postoji, samo je pitanje vremena potrebnog da se ranjivost pronađe i iskoristi. Da bi se vrijeme analiziranja mete napada i realizovanje napada smanjilo traži se najslabija tačka odbrane.

Napadima se ugrožavaju osnovni sigurnosni principi podataka [2]:

- povjerljivost podataka – informacija je dostupna samo onima koji imaju ovlašteni pristup,
- integritet podataka – zaštita postojanja, tačnosti i kompletnosti kao i procesnih metoda,
- dostupnost podataka – osiguranje da ovlašteni korisnici imaju mogućnost pristupa informaciji kada im je ista potrebna.



Slika 1. Osnovni sigurnosni principi

Sistem putem koga se informacije prikupljaju, obrađuju, prenose i čuvaju predstavlja informacioni sistem. Njegove osnovne komponente su baze podataka, hardver (procesor, memorija, diskovi), softver (sistemski softver, aplikativni softver) i telekomunikacione tehnologije [2]. Sve navedene komponente mogu biti predmet napada.

Posebno rizični i značajni su napadi koje organizuju posebno organizovane grupe napadača najčešće sa finansijskim ili političkim motivima. Ovi napadi se nazivaju trajne prijetnje (engl. Advanced persistent threat – APT) i usmjereni su na precizno odabrane resurse. U daljem tekstu koristićemo termin – APT [3].

Napredna obilježja ovih vrsta napada se odnose na sofisticirano korištenje zlonamjernog softvera i socijalnog inženjeringa radi iskorištavanja ranjivosti informacionih sistema. APT napadi traju duži vremenski period kroz faze pripreme napada, izvođenja napada do održavanja osvojenog uporišta u informacionom sistemu.

APT po definiciji imaju naredne kriterijume: [4]

- ciljevi – krajnji cilj napadača,
- vremenski okvir – vrijeme provedeno u pripremi i izvođenju napada,
- resursi – nivo znanja i alati korišteni u napadu,
- tolerancija na rizik – do koje mjere će prijetnja ostati neotkrivena,
- vještine i metode – sredstva i tehnike korištene u napadu,
- akcije – preduzete aktivnosti napadača,
- polazne tačke napada – mjesto od koga počinje izvođenje napada,
- brojnost napada – broj informacionih sistema i resursa,
- prikupljanje informacija – kroz različite metode prikupljanja informacija.

III. IT REVIZIJA

IT reviziju možemo posmatrati u kontekstu interne ili eksterne revizija. Osnovna razlika je da li je funkcija organizaciono smještena unutar kompanije (interna revizija) ili je dio druge kompanije (eksterna revizija) koja pruža profesionalne usluge revizije. Za definisanje interne revizije koristićemo definiciju Instituta internih revizora (engl. The institute of internal auditors-IIA) prema kojoj je interna revizija nezavisna i objektivna aktivnost koja daje savjete i pruža uvjerenje sa ciljem da uveća vrijednost i unaprijedi djelatnost jedne organizacije. Rad IT revizije počiva na dva osnovna postulata revizije: nezavisnost i objektivnost. Pored toga revizija treba da zadovolji principe integriteta, objektivnosti, povjerljivosti i kompetentnosti. Svi navedeni principi su dio Etičkog kodeksa Instituta internih revizora.

IT revizija je proces prikupljanja i procjene dokaza kako bi se utvrdilo da li je informacioni sistem dizajniran da održava integritet podataka, štiti imovinu i omogući postizanje organizacijskih ciljeva uz efikasno i učinkovito korištenje resursa.

Za vrste IT revizija prema predmetu revizije koristićemo podjelu koju je dala Asocijacija za reviziju i kontrolu informacionih sistema (engl. Information Systems Audit and Control Association-ISACA) (Sl.2.):

- tehnička revizija IT – pokriva infrastrukturu, prenos podataka, komunikacione kanale kao i baze podataka,
- aplikaciona IT revizija – pokriva softver i podržavajuće programske alate,
- organizaciona IT revizija – pokriva upravljanje kontrola nad informacionim tehnologijama,
- razvojna i implementaciona IT revizija – pokriva specifikacije, zahtjeve, dizajn i razvoj, kao i implementaciju,
- zakonska IT revizija – pokriva nacionalne i međunarodne standarde.

Slika 2. Vrste IT revizije

IV. ANALIZA APT MODELA

Komandni i kontrolni centar je jedan od osnovnih karakteristika APT napada. Komandni i kontrolni centar se koristi radi izdavanja instrukcija i kontrola resursima nad kojim je preuzeto upravljanje kao i za pristup osjetljivim podacima. Izuzetno važan aspekt skrivanja malicioznih aktivnosti izvedenih pomoću APT napada je maskiranje komunikacije između komandnog i kontrolnog centra (engl.

Command and Control (C&C)) [5] i resursa na kome se izvršava napad.

APT ostaju neprimjećeni duži vremenski period jer često koriste kovertirane kanale. Kovertirani kanal (engl. Covert Channel) je bilo koji komunikacioni kanal koji može da prenese podatke na način koji nije predviđen dizajnom sistema, skriveno od vlasnika podataka i time ugrozi sigurnost podataka. Korištenje kovertiranih kanala se obično dešava u situacijama kada neovlaštena lica žele da ostvare pristup podacima bez saglasnosti vlasnika podataka.

Dizajn TCP/IP protokola omogućava navedene zloupotrebe za skriveni prenos podataka.
Specifikacija protokola definiše strukturu zaglavlja IP i TCP paketa. U navedenim zaglavljima postoji nekoliko polja koja su opciona ili se uopšte ne koriste. Ako ova polja popunimo kodiranim podacima dobićemo tipičan kovertirani kanal: dijagrami spolja izgledaju normalno, bez problema prolaze kroz paketske filtere u zaštitnim zidovima (Firewall), neupadljivi su za snifing u sistemima za detekciju upada (IDS) i potpuno su izvan detekcije svih sitema koji se baziraju na detekciji potpisa ili detekciji anomalija.
Ovako skrivene informacije se ne mogu primjetiti sistemom za pretragu ključnih riječi u porukama.

Jednostavnom modifikacijom paketa - manipulisanjem adresnim informacijama može se postići reflektovanje paketima (odskakanje, eng. Bouncing). Ovim putem se pored sakrivanja informacija unutar paketa postiže i zametanje tragova o njihovom pravom porijeklu. To se radi tako što se upućivanje paketa sa polazne tačke prema odredištu radi tako što se paket šalje prema trećem nasumično odabranom sistemu od kojeg stiže odgovor (u kojem se skriva informacija) na adresu krajnjeg odredišta. Ovo se postiže tako što se u inicijalnom paketu u polje za izvornu adresu unosi adresa krajnjeg primaoca paketa. Korištenje TCP/IP protokola za skriveni prenos podataka se naziva i TCP/IP steganografija. Generalno, steganografija [6] je metod za sakrivanje podataka gdje se, umjesto polja u datagramu mrežnog protokola, za smještaj podataka koriste prazna mjesta u strukturi nekog binarnog fajla. Najčešće je to nekompromitovani grafički format, na primjer, u bitmapiranu sliku se ubace kodirani podaci tako da se izgled i veličina slike uopšte ne promijene.

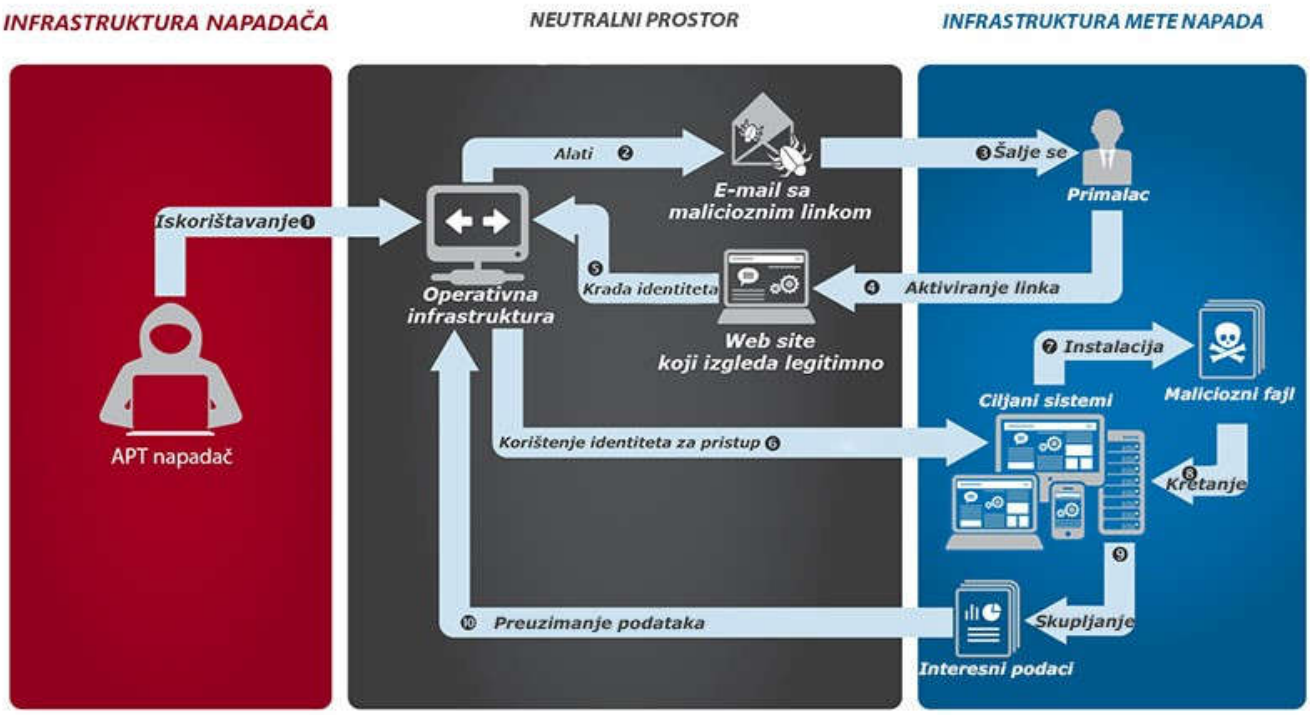
U nastavku ćemo predstaviti model i način izvođenja APT napada, provjere koje treba da izvrši IT revizija kao i adekvatne preporuke u vidu zaštitnih mjera.

Grupe koje izvode ovu vrstu APT napada koriste napredne alate i infrastrukturu kombinovanu sa socijalnim inženjeringom da kompromituju i iskoriste informacione sisteme koje preuzmu pod kontrolu. Njihove aktivnosti uključuju posebno ciljane krađe identiteta (engl. Spearphishing) koje se kombinovano usmjeravaju na državne institucije, industrijski sektor, privredne kompanije, političke organizacije ili obrazovne institucije. Često se ovi napadi izvode koristeći resurse trećih strana radi maskiranja identiteta stvarnog napadača.

Prema metama napada se šalju web linkovi sa malicioznim sadržajem. Kada se ovi linkovi pokrenu od neoprezne žrtve dolazi do skrivenog instaliranja alata za udaljeni pristup (engl. Remote access tools – RAT).
RAT izbjegava detekciju postojećih odbrambenih sistema različitim tehnikama.

Maliziozni linkovi se isporučuju i putem kanala elektronske pošte. Na isti način, poput već opisanog korištenja web linkova, se dolazi do kontrole napadnutog resursa te analiziranja i preuzimanja osjetljivih podataka (Sl. 3.).

Slika 3. Proces APT napada



Za izvođenje APT napada organizovane grupe prethodno uspostave odgovarajuću operativnu infrastrukturu radi maskiranja izvora napada, hostovanje malicioznog sadržaja i uspostavljanja komunikacije sa komandnim i kontrolnim centrom (C&C).

Ako detaljnije analiziramo navedene dvije vrste APT napada (putem web linkova odnosno elektronske pošte) možemo konstatovati da nakon ostvarivanja pristupa napadnutom sistemu napadači uspostavljaju trajnost pristupa, eskaliraju privilegije, pristupaju osjetljivim podacima i omogućavaju zaštićeno (kriptovano) preuzimanje podataka.

Karakteristično za uspješne APT napada je upotreba takozvanih „zero-day ranjivosti“, gdje se koriste slabosti informacionih sistema koje nisu poznate proizvođačima softvera. Baš zbog ovoga ne postoji odbrana koja je efikasna nego se samo može osloniti na višeslojni sistem zaštite koji treba zaustaviti napada na nekom od uspostavljenih linija odbrane.

V. RANJIVOSTI KOJE APT ISKORIŠTAVAJU

Analizirajući koje ranjivosti APT iskorištavaju došli smo do narednih rezultata. S obzirom da je napadaču izuzetno važno da iskorištavajući ranjivosti informacionih sistema i baza podataka pristupi do osjetljivih podataka kombinuju se varijacije tehnika.

Posebnu pažnju ćemo posvetiti Injection flaws napadima. Injection flaws su napadi na web aplikacije kada se kroz slanje komandi bazi podataka ili browser-u preuzima kontrola na napadnutom informacionom resursu. Prema OWASP (engl. Open Web Application Security Project) istraživanju [7] ova vrsta napada je najčešća i uključuje SQL injection, OS injection i LDAP (engl. Lightweight Directory Access Protocol) injection. SQL injection tehnika je jedna od najčešćih i najefikasnijih napada. Ovaj oblik napada iskorištava ranjivost na sloju baze podataka a dešava se zbog loših provjera ulaznih podataka koji se koriste pri preuzimanju podataka iz baze. Ova ranjivost se može iskoristiti za sve web stranice koje koriste baze podataka za svoj rad. Nažalost, SQL injection napade je relativno jednostavno izvesti i dovoljno je osnovno znanje o upitima za rad sa bazom podataka [8]. Ovi napadi utiču na povjerljivost, autentikaciju, autorizaciju i integritet podataka baze podataka. Brojne web stranice su postala meta ovog oblika napada, a najčešći cilj napada je bila krađa korisničkih podataka zapisanih u bazi podataka, poput podataka o kreditnim karticama ili adresama elektronske pošte.

SQL injection iskorištava loše provjere podataka koje korisnik unosi u web aplikaciju [9]. Jednostavan primjer ovog oblika napada je zaobilaženje legitimne prijave na sistem. Prilikom prijave obično se od korisnika zahtjeva upisivanje korisničkog imena i lozinke u predviđena polja za unos podataka. Nakon unosa ovih podataka web aplikacija ih preuzima i smiješta kao dvije varijable, na primjer “user” i “pass”. Dobijene podatke web aplikacija koristi za pokretanje SQL upita kako bi se u bazi podataka provjerilo da li postoji korisnik sa podacima koji odgovaraju podacima unesenim prilikom prijave na sistem. Navedeni proces se iskorištava kada napadač koristi polja za unos podataka kako bi umetnuo posebno oblikovani SQL kod:

```
' OR '1'='1'
```

Posle korištenja navedenog koda napadač je postigao da baza podataka ne upoređuje podatke u tabeli sa korisničkim imenom koje je korisnik unio već provjerava istinitost tvrdnje '1'='1'. Pošto je ova tvrdnja uvijek tačna napadač se može uspješno prijaviti kao legitimni korisnik. Neke od varijacija zlonamjernog SQL koda mogu biti:

```
' or 1=1--
' or 1=1#
' or 1=1/*
') or '1'='1--
') or ('1'='1--
```

Napadi sa umetanjem SQL koda nižu nekoliko SQL naredbi pomoću znaka tačka-zarez odnosno koriste znak dvostrukih crtica koje označavaju komentar u SQL kodu.

Kao preporuku za zaštitu od ove vrste napada IT revizija zahtijeva da se na poseban način obrade svi podaci koji: sadrže sumnjive znakove poput znaka tačke-zarez, dvostruke crtice ili navodnike, SQL ključne riječi, ne odgovaraju očekivanom tipu podataka ili sadrže preveliki broj znakova. Također, preporučuje se zaštita baze podataka i servera tako da se mogućnost izmjene podataka omogućuje samo maloj grupi korisnika sa administratorskim ovlaštenjima.

Još jedan način borbe protiv SQL injection napada je korištenje neuobičajenih imena za tabele i atribute u bazi podataka te minimalan obim informacija koje su dostupne u porukama greške. Time se napadaču otežava prikupljanje informacija o bazi podataka što je prvi korak u izvođenju napada. Ako napadač ne zna strukturu baze podatka te imena tabela i atributa ne može izvesti napad.

Preporučuje se i da se koriste sistemi koji omogućavaju provjeru sigurnosti web stranica. Ovi sistemi izvode automatizirane napade umetanjem SQL koda kako bi otkrili ranjivosti web aplikacija. Nakon uspješno izvedenog napada, pružaju povratnu informaciju koju administratori mogu iskoristiti kako bi povećali sigurnost svoje web stranice. Neki od poznatiji alata za testiranja web aplikacija su w3af, Burp Suite, Nikto, sqlmap.

APT napadači izuzetno često koriste Cross-site scripting (XSS) ranjivosti. Kao i prethodno navedeni SQL injection i ovdje se ubacuje i pokreće maliciozni kod (na primjer JavaScript) u web aplikaciju. Cilj napadača je da preuzme kontrolu nad web aplikacijom i dođe u posjed osjetljivih podataka. Primjer malicioznog koda:

```
<script>
window.location='http://attacker/?cookie='+document.c
ookie
</script>
```

Pokretanjen navedenog koda korisnik se navodi na određenu web stanicu koja putem HTTP zahtjeva preuzima korisnikov cookie [10] u kome može pronaći ID sesija i preuzeti korisnikov identitet.

Kao preventivne mjere protiv ove vrste napada treba koristiti validaciju podataka koje korisnik unosi u web aplikaciju (kako na klijent strani tako i na server strani) i HTML encoding [11].

Za mjere koje je potrebno preduzeti u cilju identifikovanja prisustva APT napada preporučujemo da mrežni administratori nadgledaju mrežni saobraćaj i koriste YARA alat [12]. Ovaj alat radi na bazi upoređivanja potpisa i otkrivanja malicioznog dijelovanja. U nastavku primjer potpisa malicioznog fajla.

```
Yara Signature
rule PAS_TOOL_PHP_WEB_KIT
{
meta:
description = "PAS TOOL PHP WEB KIT FOUND"
strings:
$php = "<?php"
$base64decode = /\='base'\.\(\d+\*\d+\)\.'_de'\.'code'/
$strreplace = "(str_replace("
$md5 = ".substr(md5(strrev("
$gzinflate = "gzinflate"
$cookie = "_COOKIE"
$isset = "isset"
condition:
(filesize > 20KB and filesize < 22KB) and
#cookie == 2 and
#isset == 3 and
all of them
}
```

Potpisi koji ukazuju na maliciozni sadržaj se mogu pronaći na više adresa (Github, MISP, ThreatConnect) [12].

VI. ZAŠTITNE MJERE

U cilju zaštite i prevencije malicioznih napada u vidu APT djelovanja potrebno je uspostaviti niz mjera. Najveći dio ovih mjera se odnosi na preventivne mjere odnosno generičke mjere, mjere opšteg karaktera koje se generalno odnose na IT zaštitu. Ne ulazeći dublje u analizu ovih generalnih kategorija mjera zaštite, ako ih posmatramo iz ugla poslovnih subjekata, onda ih možemo vidjeti kao ciljeve kompanije [13]:

- principi, procedure i okviri,
- procesi,
- organizaciona struktura,
- organizaciona kultura, etika,
- informacije,
- servisi, infrastruktura i aplikacije,
- zaposleni, vještine i kompentencije.

Tokom IT revizije pokreće se niz provjera radi utvrđivanja nivoa informacione sigurnosti. Cilj provjera je utvrđivanje postojanja adekvatnih sigurnosnih mjera koje imaju ulogu prevencije, zaštite i onemogućavanja APT napada.

Prema našim analizama, iskustvima u sprečavanju APT napada i najboljim praksama, na raspolaganju je niz zaštitnih mjera. Tokom IT revizije provjerava se:

1. Da li se redovno prave rezervne kopije podataka (engl. backup)? Da li je posvećena posebna pažnja kritičnim podacima? Smještaju li se rezervne kopije van mreže (engl. offline)? Testiraju li se redovno procesi oporavka podataka radi utvrđivanja sposobnosti za reagovanje u slučaju incidenta?
2. Da li se vrši redovno skeniranje ranjivosti informacionih sistema (engl. vulnerability scanning) i mreža radi utvrđivanja rizika i postupka eliminisanja uočenih ranjivosti (engl. patching)? Upravo su informacioni sistemi i aplikacije najčešće meta napada zbog identifikovanih ranjivosti. IT revizijom se preporučuje implementiranje kontinuiranog ažuriranja sa objavljenim sigurnosnim softverskim ispravkama [14]. Kontrolom statusa implementacije zadnjih objavljenih softverskih ispravki (engl. patch) značajno se sužava prostor koje napadač ima dok istražuje ranjivosti.
   Naravno, obavezno je utvrditi da li postoji proces testiranja softverskih ispravki prije instalacije u produkciono okruženje [14].
3. Jesu li uspostavljene kontrole pokretanja dozvoljenih aplikacija (engl. application whitelisting), odnosno uspostavljeno blokiranje pokretanja aplikacija koje nisu dozvoljene?
4. Postoji li plan reagovanja na incidente i da li se isti koristi? Da li su određeni ključni indikatori pomoću kojih se prati vrijeme detekcije, analize, izvještavanja i otklanjanja incidenta? Postoji li tim zadužen za reagovanje na incidente, da li je isti adekvatno obučen i opremljen [15] ?
5. Jesu li ograničene privilegije administratora jer se rizik u slučaju preuzimanja administratorskih ovlaštenja drastično povećava u odnosu na druge korisničke grupe? Napadači su posebno fokusirani na administrativna ovlaštenja (u procesu eskalacije privilegija) jer im oni pružaju najveći nivo ovlaštenja uključujući često i brisanje logova čime se otežava oporavak posle napada i forenzika. Logovi trebaju biti posebno osigurani od modifikacija, centralizovano smješteni na udaljenu lokaciju.
6. Niz je dodatnih kontrola koje treba provesti a tiču se upravljanja sa korisničkim ovlaštenjima. Među značajnije spadaju: brisanje i onemogućavanje korištenja naloga koji se ne upotrebljavaju, onemogućavanje naloga gosta (engl. guest), preimenovanje administratorskih naloga, onemogućavanje anonimnog prijavljivanja (engl. anonymous logon) [16]. Značajno je provjeriti da li se koristi snažnija autentifikacija – korištenje više faktora autentifikacije (poput pametnih kartica, posebno generisanih kodova poslanih na pametni telefon, biometrijskih metoda).Također je važno provjeriti kompleksnost lozinki, frekvenciju zahtjevanih promjena lozinki i korištenje hash vrijednosti za čuvanje lozinki.
7. Da li je pripremljen plan kontinuiteta poslovanja (engl. business continuity plan) i da li se isti ažurira i redovno testira? Koliko dugo se može izdržati bez pristupa određenim informacionim sistemima i resursima?
8. Provode li se probojna testiranja (engl. penetration testing) web aplikacija, informacionih sistema zbog utvrđivanja stepena otpornosti na napade?

Posebnu pažnju je potrebno posvetiti zloupotrebi slabosti koje se odnose na ljudski faktor. Već smo spominjali socijalni inženjering kao jedan od vektora napada. Predvidljivost ljudskih reakcija, lakovjernost i neznanje mogu

biti iskorištene od napadača kada se koristi lažno predstavljanje, manipulacije i korištenje lažnih informacija.

Posebnu kategoriju unutar socijalnog inženjeringa predstavlja krađa identiteta. Ovo može biti čest vektor napada a pogađa ili veći broj korisnika (engl. phishing) ili se fokusira na tačno određenu ciljanu grupu (engl. spear phishing). Phishing uobičajeno započinje slanjem elektronske poruke koja izgleda kao da je izvorno poslata sa poznate adrese (na primjer banka, internet trgovina) i u sebi sadrži link koji upućuje na lokaciju putem koje se kradu lični podaci žrtve napada. Spear phishing ne šalje poruke prema većem broju korisnika već na već opisani način cilja tačno odabrane pojedince. Spear phising je teže otkriti i sam po sebi ostvaruje bolje rezultate napada.

U cilju zaštite od napada korištenjem socijalnog inženjeringa IT revizija treba provjeriti da li se:

- koriste i koliko su efikasne anti-phishing tehnike u internet preglednicima i programima elektronske pošte.
- se organizuju treninzi i edukacije korisnika na temu informacione sigurnosti. Na ovim edukacijama trebaju biti obrađene teme i dati primjeri lažnog predstavljanja, otkrivanja i korištenja povjerljivih podataka, prepoznavanje indikatora napada, reagovanja kod pojavljivanja incidenta, korištenja linkova dobijenih u elektronskim porukama ili nepouzdanim internet stranicama.
- koristi SPF standard (engl. sender policy framework) koji provjerava originalni server sa koga se upućuje elektronska poruka – provjera „return-path vrijednosti. Ovaj sistem pomaže u otkrivanju pravog identiteta pošiljaoca poruke.

VII. ZAKLJUČAK

Kroz praktična iskustva autora u funkciji IT revizora potvrđena je efikasnost prikazanih zaštitnih mjera protiv APT napada. Nepobitna je činjenica korištenja ove vrste napada na globalnom nivou te se nameće kao nužno obaveza implementiranja navedenih zaštitnih mjera i sprečavanje eskalacije rizika. Možemo zaključiti da kroz IT reviziju radimo validaciju i procjenjujemo koliko smo uspješno implementirali zaštitne mjere protiv APT napada.

Jedna grupa zaštitnih mjera se odnosi na sistemske procese poput pravljenja rezervnih kopija podataka, skeniranja ranjivosti, plana reagovanja na incidente i slično. Drugu grupu zaštitnih mjera predstavljaju tehničke kontrole koje se često pominju kao efikasan vid odbrane (kontrole perimetra poput zaštitnog zida, IPS/IDS sistema, antivirusa i anti-malware aplikacija). Tokom IT revizije cilj je da se ne fokusiramo samo na sistemske procese i tehničke kontrole Ove tehničke kontrole su zaista efikasne u odbrani protiv tradicionalnih napada ali se ne pokazuju uspješne protiv APT napada koji koriste zero-day ranjivosti i socijalni inženjering.

Zbog navedenog, pored tehničkih kontrola kao mjere zaštite od visoko profilisanih APT napada, neophodno je razviti i implementirati e-mail sigurnost kao i edukaciju u oblasti informacione sigurnosti. Sve navedene zaštitne mjere su rezultat praktičnih iskustava i predstavljaju osnovu za kvalitetno implementiranu odbranu informacionih resursa. Prikazane preporuke koje IT revizija treba pružiti do sada nisu nigdje na ovakav način sveobuhvatno prikazane i predstavljaju snažnu pretpostavku za efikasno postavljen sistem zaštite informacionih resursa.

LITERATURA

[1] IT Governance, „List of data breaches and cyber attacks in 2016“ https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2016-1-6-billion-records-leaked/

[2] Dragan Pleskonjić, Nemanja Maček, Borislav Đorđević, Marko Carić, “Sigurnost računarskih sistema i mreža”, Mikro knjiga, 2007

[3] Tyler Wrightson, Advanced persistent threats, McGraw-Hill Education, 2015

[4] Sean Bodmer, Dr. Max Kilger, Gregory Carpenter, Jones Jade, “Reverse deception: organized cyber threat counter-exploitation”, McGraw-Hill Osborne media, 2012

[5] SANS, „The Importance of Command and Control Analysis for Incident Response“, https://digital-forensics.sans.org/blog/2014/03/31/the-importance-of-command-and-control-analysis-for-incident-response

[6] InfoSysSec, „Introduction to Steganography“, http://www.infosyssec.com/infosyssec/Steganography/menu.htm

[7] OWASP “Top 10-2013 The ten most critical web application security risks” https://www.owasp.org/images/f/f8/OWASP_Top_10_-_2013.pdf

[8] CIS “Napadi umetanjem SQL koda” http://www.cis.hr/files/dokumenti/CIS-DOC-2011-09-025.pdf

[9] Centar informacijske sigurnosti, “Zaštita baza podataka”, http://www.cis.hr/files/dokumenti/CIS-DOC-2012-08-059.pdf

[10] Windows dev center, “HTTP Cookies” https://msdn.microsoft.com/en-us/library/windows/desktop/aa384321(v=vs.85).aspx

[11] IBM, “Prevent cross-site scripting attacks by encoding HTML responses “ http://www.ibm.com/developerworks/library/se-prevent/

[12] IBM, “Signature-Based Detection With YARA” https://securityintelligence.com/signature-based-detection-with-yara/

[13] ISACA journal volume 4, “State and impact of governance of enterprise IT in organizations”, 2015

[14] SANS, “A Practical Methodology for Implementing a Patch management Process” https://www.sans.org/reading-room/whitepapers/bestprac/practical-methodology-implementing-patch-management-process-1206

[15] NIST, “Computer Security Incident Handling Guide” http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

ABSTRACT

This paper describes the importance of IT audit and contribution to protect increasingly ever-present IT threats in the form of APT attacks. IT audit is a function that is necessary (often required by the regulator) in any company that uses information technology. Through IT audit is carried out validation quality of internal controls and the level of protection of information resources. Protection of information resources shall be established in order to preserve the confidentiality, integrity and availability, principles which are basic safety principles. IT threats are aimed at jeopardizing the security principles and facilitate the realization of certain benefits which attackers exploit them through specific types of attacks where APT is globally currently the most dominant. Through the work analyzes the characteristics of APT attacks, the methodology used by the attackers and the role and importance of IT audit as one of the functions which contribute to the prevention of IT threats. Conducting IT audit tested existing control, resistance to APT attacks and give recommendations based on practical experience from auditing and best practices are currently the only way of protection.

IT AUDIT ROLE IN APT PREVENTION

Rodoljub Kajganić, Biljana Radulović