UDC: 004.738.5 Info M str. 40-49

ANALIZA RANJIVOSTI KORPORATIVNIH RAČUNARSKIH MREŽA
VULNERABILIY ANALYSIS IN COORPORATE NETWORKS

Aleksandar Bratić

REZIME: Područje istraživanja ovog rada predstavlja oblast bezbednosti u okviru informacionih tehnologija. Ovaj rad ukazuje na neophodnost sistematičnog pristupa, zasnovanog na stručnim istraživanjima, dizajniranju arhitekture informacionog sistema kreiranja i unapređenja procesa kako bi se obezbedio visok nivo informacione bezbednosti. Predmet istraživanja su preduslovi, organizacioni i tehnički kao i alati koji se koriste u procesu upravljanja ranjivostima informacionih sistema. Predložen je način implementacije procesa upravljanja ranjivostima kako kroz upotrebu konkretnih tehnika, tako i kroz primenu najbolje prakse prilikom projektovanja arhitekture informacionih sistema. U posebnom poglavlju opisano je realno okruženje u okviru koga su pokazani delovi procesa i kao i unapređenje procesa koje se može primeniti u okviru korporativnih okruženja, a u svrhu veće efikasnosti pri upravljanju rizikom koji je identifikovan kroz proces upravljanja ranjivostima.

KLJUČNE REČI: upravljanje, ranjivosti, alati, procesi, metodologija

ABSTRACT: The field of research of this paper is the field of security in area of information technology. This paper will points out the necessity of a systematic approach, based on expert research, designing the architecture of the information system for creating and improving the process in order to ensure a high information security of level. The subject of the research are preconditions, organizational and technical as well as tools used in the process of managing the vulnerabilities of information systems. It is proposed how to implement the process of vulnerability managemetn both through the use of concrete techniques and through the application of best practice in designing the information system architecture. A special chapter describes the real environment in which parts of the process are demonstrated and the improvement of processes that can be applied within corporate environments and for the purpose of greater risk management efficiency identified through the process of managing vulnerabilities.

KEY WORDS: management, vulnerability, tools, processes, methodology

1 UVOD

Zaštita informacionih sistema je u današnje vreme postala jedna od najbitnijih komponenata informacionih sistema, kako živimo u vreme kada se traži velika dostupnost informacija, a naročito fleksibilnost i prilagodljivost krajnjem korisniku, tradicionalne arhitekture informacionih sistema se menjaju i potrebno je informacije koje su tradicionalno bile smeštene u internim izolovanim računarskim mrežama, dati na korišćenje i pristup kako korisnicima koji pripadaju informacionom sistemu tako i klijentima, koji pristupaju sa različitih mrežnih okruženja, različitih operativnih sistema i uređaja tako i sa različitim funkcionalnim zahtevima. Sve informacije koje se objavljuju korisnicima moraju biti sačuvane od neovlašćenog pristupa, izmene ili brisanja, kako bi informacioni sistem očuvao integritet, tajnost i dostupnost.

2 PROCES IDENTIFIKOVANJA I UPRAVLJANJA RANJIVOSTIMA INFORMACIONOG SISTEMA

Kompanije pri obavljanju svojih poslovnih aktivnosti zavise od obrade i upotrebe informacija. Narušavanje temeljnih načela IKT sistema može imati negativne posledice za kompaniju. Potrebno je primereno zaštititi informacije i upravljati bezbednošću IKT sistema kompanije. Potreba za zaštitom informacija i upravljanjem bezbednošću naročito je bitna u današnjem vremenu jer su IKT međusobno povezani i razmena informacija je dostigla visok nivo. Upravljanje bezbednošću IKT sistema je , između ostalog, sveobuhvatan, detaljan i sistematski proces identifikovanja potreba (zbog postizanja zadovoljavajućeg nivoa bezbednosti) kao i postizanja i održavanja nivoa bezbednosti IKT sistema.

2.1 *Ranjivost i proces upravljanja ranjivostima*

Ranjivost informacionog sistema je kako je definisano u ISO/IEC 27001:2013 (1)standardu predstavlja slabost informacionog dobra (asset), ili grupe dobara koja može biti iskorišćena od jedne ili više pretnji. Dok zajednica na Wikipediji ranjivost definiše kao slabost koja omogućava napadaču da smanji bezbednost informacija. Ranjivost je po Wikipediji, presek tri elementa: sistemski propust, napadač koji ima pristup propustu i napadačeva sposobnost da iskoristi propust. Kako bi iskoristio ranjivost, napadač mora da ima bar jedan alat ili tehniku kako bi mu ranjivost bila dostupna. U ovom smislu ranjivost se smatra površinom za napad.

ISC² (The International Information System Security Certification Consortium) (2) u svojim materijalima za pripremu CISSP sertifikata (Certified Information Systems Security Professional) opisuje da do ranjivosti može doći kroz mane informacionog sistema, loših konfiguracija (koje se u ovom slučaju posmatraju kao slabosti) i nedosledne primene bezbednosnih politika. Kao mere zaštite definisane su mere kao što su primena bezbednosnih zakrpa od strane proizvođača ili autora softvera, generisanje novog softverskog koda ili promena hardverskih komponenti.

2.2 *Proces upravljanja ranjivostima inforamcionog sistema*

Proces upravljanja ranjivostima u korporativnim računarskim mrežama predstavlja jednu od osnovnih mera koje se primenjuju prilikom upravljanja rizicima informacionih sistema kako prilikom identifikacije rizika, pri samom izvršavanju procesa upravljanja ranjivostima, tako i u delu upravljanja ri-

zicima i primenama mera za smanjenje ili uklanjanje rizika informacionih sistema. Proces upravljanja ranjivostima informacionog sistema, organizaciono gledano u zavisnosti od pozicije službe informacione bezbednosti može biti podeljen na više organizacionih jedinica ili ga može izvršavati više njih. Proces upravljanja ranjivostima se sastoji iz više koraka, u zavisnosti od veličine i kompleksnosti informacionog sistema kompanije i same kompanije odnosno njenog poslovnog modela, proces i koraci mogu biti različiti ali za potrebe ovog istraživanja identifikovaćemo sledeće korake:

- Utvrđivanje liste informacionih dobara
- Određivanje grupe resursa po kritičnosti
- Skeniranje resursa na ranjivosti
- Analiza nađenih ranjivosti
- Otklanjanje nađenih ranjivosti
- Provera rešenja
- Informacije i izveštaj o ranjivostima informacionog sistema

2.2.1 Utvrđivanje liste informacionih dobara

Ovaj korak u okviru koga se utvrđuju informaciona dobra za koja se radi identifikacija i uklanjanje ranjivosti. U praksi se utvrđivanje liste informacionih dobara radi automatizovano ili ručno. Kod automatizovanih lista informacionih dobara koriste se softveri koji automatski dodaju informaciono dobro u inventar, neki od proizvoda koji se koriste u ovu svrhu su IBM Watson (3), CA IT Asset Manager (4) ili Oracle Maintenance Management (5), neke od karakteristika ovih proizvoda su da automatski ažuriraju listu informacionih dobara i samim tim se može automatizovati ažuriranje liste u skeneru. Često je prepreka implementaciji ovakvih alata cena i nezrelost IKT procesa u okviru organizacije. Ručno dodavanje informacionih dobara je najčešći način upravljanja inventarom. Nedostatak ovakve metode je što je mogućnost ljudske greške velika i moguće je da neki delovi informacionog sistema ne budu evidentirani pa samim tim ne uđu u proces upravljanja ranjivostima informacionih sistema.

2.2.2 Određivanje grupe resursa po kritičnosti

Ovaj deo procesa ima za cilj određivanje prioriteta testiranja na ranjivosti informacionih dobara kako bi se informaciona dobra skenirala u skladu sa vrednostima koju imaju u okviru organizacije i na osnovu toga smanjio rizik u skladu da vrednostima dobara.

U ovaj deo proces moraju biti uključeni delovi organizacije koji su vlasnici informacija a samim tim i delova informacionih sistema, kako bi se što realnije odredila vrednost resursa.

2.2.3 Skeniranje resursa na ranjivosti

Centralni deo procesa upravljanja ranjivostima informacionog sistema, od kvaliteta ovog dela procesa praktično zavisi ceo proces. Odvija se posle obezbeđenih organizacionih, procenih i tehničkih preduslova. Sam proces mora biti dobro definisan, uloge podeljene i proces proveren u svim svojim delovima. Proces se odvija na osnovu prethodno utvrđenog rasporeda po kritičnosti delova informacionog sistema i dostupnih resursa za samo obavljanje procesa. Od efikasnosti procesa zavisi i nivo bezbednosti koji će organizacija postići, često se u praksi sama efikasnost procesa testira tako što se u okviru informacionog sistema postavi aplikacija sa poznatim ranjivošću pa se prati koliko brzo i efikasno će biti pronađena i identifikovana u okviru procesa skeniranja na ranjivosti.

2.2.4 Analiza nađenih ranjivosti

Analiza ranjivosti se odvija posle skeniranja informacionog sistema na ranjivosti i identifikacije ranjivosti. U okviru ovog procesa se definišu tehničke karakteristike ranjivosti, koliko stepen rizika nosi ranjivost i samim tim se određuje stepen prioriteta otklanjanja ranjivosti a u odnosu na delove informacionog sistema na kojima je identifikovana ranjivost pronađena.

Otklanjanje nađenih ranjivosti

Proces otklanjanja ranjivosti može uključivati u zavisnosti u kome delu informacionog sistema je ranjivost pronađena jednu ili više organizacionih jedinica. Preporuke za otklanjanje nađenih ranjivosti se nalaze u okviru skenera koji se koristi kako bi se identifikovala ranjivost, ali se može primeniti i druga tehnika zaštite u zavisnosti od karakteristika dela informacionog sistema u okviru koga je ranjivost pronađena.

Sve preporuke za otklanjanje ranjivosti moraju biti testirane pre primene na produkciono okruženje, a potrebno ih je primeniti u okviru uspostavljenog procesa upravljanja promenama. Pri otklanjaju ranjivosti potrebno je voditi računa o ceni koštanja primenjene tehnike zaštite kako ne bi došli u situaciju da je vrednost mere zaštite informacionog sistema veća od vrednosti informacija koje sama informacija a samim tim i informacioni sistem ima.

2.2.5 Provera rešenja

Nakon promenjenih mera zaštite i otklanjanja ranjivosti potrebno je izvršiti proveru rešenja datih mera. Ovim procesom se utvrđuje novi stepen bezbednosti informacionog sistema. Potrebno je pravilno izvršiti proveru primenjenih mera zaštite jer primenom tehnika zaštite neke vrste rizika otklanjamo, a moguće je da se samom primenom pojave novi rizici, koje je potrebno identifikovati i tretirati u skladu sa strategijom upravljanja rizikom i apetitom za rizik poslovodstva organizacije.

2.2.6 Informacije i izveštaj o ranjivostima informacionog sistema

Komunikacija informacija o ranjivostima informacionog sistema bitna je iz dva razloga: kako bi se ukoliko je ranjivost kritična i ugrožava rad informacionog sistema i samim tim organizacije, rukovodstvo moglo na pravi način da upravlja potencijalnom kriznom situacijom i drugi kako bi se mogla praviti baza znanja o identifikovanim i otklonjenim ranjivostima, ova baza znanja može da služi kako bi se unapredilo znanje zaposlenih o informacionog bezbednosti i kako bi se

na osnovu ove baze znanja moglo raditi planiranje strategije zaštite informacionog sistema u budućnosti. Svi ovi izveštaji po svojoj prirodi bi trebali imati internu klasifikaciju najmanje poverljivo a nekada i strogo poverljivo.

Analiza procesa upravljanja ranjivostima informacionog sistema

Proces upravljanja ranjivostima informacionog sistema mora biti kontinuiran i povremeno mora biti predmet revizije kako bi se proces unapredio a eventualni nedostaci ispravili. Analizu procesa upravljanja ranjivostima može da vrši spoljni revizorski tim ili interna ICT revizija, u zavisnosti od okruženja u kome se proces sprovodi.

2.3 *Preduslovi za efikasno sprovođenje procesa upravljanja ranjivostima informacionog sistema*

Da bi se proces upravljanja ranjivostima pravilno implementirao u okviru organizacije, potrebno je stvoriti preduslove za implementaciju.

Preduslove možemo da podelimo na sledeće:

1. Organizacione preduslove
2. Procesne
3. Tehničke

2.3.1 Organizacioni preduslovi

Unapređenje informacione bezbednosti, u okviru kompanija, veoma zavisi od organizacione strukture kompanije, dela u okviru koga se služba informacione bezbednosti nalazi. U samom smeštanju ove službe u okviru organizacije postoje više strategija, jedna strategija je da kompanije koje nemaju zreo proces upravljanja bezbednošću informacija i informacionih sistema, organizacionu jedinicu službe informacione bezbednosti stave u okviru organizacionog dela koji se bavi IKT infrastrukturom, kako bi operacije vezane za informacionu bezbednost bile efikasnije, manjkavost kod ove strategije je što je rukovodilac u sukobu interesa kada je poštovanje politika informacione bezbednosti u pitanju, tj. neko ko hijerarhijski odgovara rukovodiocu IKT treba da kontroliše usaglašenost sa politikama informacione bezbednosti i izveštava više rukovodioce (Izvršni odbor). Druga strategija je da se služba informacione bezbednosti posebna organizaciona jedinica kojoj je član izvršnog odbora direktno nadređeni i koji ima u svakom momentu pristup izvršnom odboru, dobra strana ovakvog pristupa je što se izbegava konflikt interesa prilikom kontrole usaglašenosti informacionog sistema sa politikama informacione bezbednosti, dok je loša strana to što operativni zadaci mogu da imaju duže i neefikasnije izvršenje.

2.3.2 Procesni preduslovi

Svi procesi u kompaniji imaju svoje međuzavisnosti pa tako i proces upravljanja ranjivostima informacionog sistema, za uspešno izvršavanje ovog procesa potrebno je stvoriti procesne preduslove koji mogu biti u okviru IKT organizacionog dela ili van njega. Procesi koji su potrebni da bi upravljanje ranjivostima informacionog sistema bilo uspešno su:

- Upravljanje inventarom informacionih sistema
- Proces upravljanja rizikom informacionog sistema
- Proces ažuriranja alata koji se koriste u procesu upravljanja ranjivostima
- Proces izveštavanja o ranjivostima informacionog sistema

Upravljanje inventarom informacionih sistema

Informacioni sistem predstavlja sveobuhvatni skup tehnološke infrastrukture (hardverske i softverske komponente), organizacije, ljudi i postupaka za prikupljanje, smeštanje, obradu, čuvanje, prenos, prikazivanje i korišćenje podataka i informacija. Dok resursi sistema obuhvataju softverske komponente, hardverske komponente i informaciona dobra

Kako bi se proces upravljanja ranjivostima informacionog sistema mogao efikasno i tačno izvršavati potrebno je imati ažuriran spisak delova informacionog sistema.

Proces ažuriranja inventara može biti automatizovan kada ovu aktivnost izvršava hardversko/softverska platforma koristeći skeniranje mreže i identifikaciju hardvera, softvera i servisa i automatski ažurirajući bazu inventara, slabost ovakvog načina ažuriranja može biti opterećenje mrežnog protoka. Drugi način koji se često sreće u praksi je da se ovaj inventar ažurira ručno, odnosno da zaposleni dodaje nove resurse u inventar. Slabost ovakvog sistema je što jedan deo resursa može ostati van inventara, a samim tim i van procesa upravljanja ranjivostima. Svakako ovaj način ažuriranja ima kašnjenje u odnosu na stvarno stanje resursa na mreži i visoko je podložan ljudskim greškama.

Proces upravljanja rizikom informacionog sistema

Kao pod proces upravljanja rizikom informacionog sistema, proces upravljanja ranjivostima veoma zavisi od efikasnosti procesa upravljanja rizikom, a naravno i proces upravljanja rizikom zavisi od procesa upravljanja ranjivostima informacionog.

Proces ažuriranja alata koji se koriste u procesu upravljanja ranjivostima informacionog sistema

Alati predstavljaju ključan resurs u procesu upravljanja ranjivostima informacionog sistema.

Pod alatima podrazumevamo automatizovanje skenere koji se za otkrivanje ranjivosti informacionog sistema, koji mogu biti open source (Open Vulnerability Assessment System (6),Retina CS Community (7), Nessus comunity (8), kao i komercijalni Qualys vulnerability management (7), Rapid 7 Nexpose (9), Tenable.io Vulnerability Management (10), skripte koje zaposleni u ICT organizacionom delu sami kreiraju na osnovu zahteva koji se u svakodnevnom radu postavljaju pred njih, aplikacije koje se instaliraju na operativni sistem pre procesa identifikovanja ranjivosti (Microsoft Baseline Security Analyzer (MBSA) (11)Belarc Adviser (12).Sve ove navedene vrste alata zahtevaju ažuriranje pre nego što se upotrebe u procesu upravljanja ranjivostima informacionog sistema. Preferirani način ažuriranja alata je automatsko, koje ažuriraju alat čim se pokrene ili ukoliko je u arhitekturi informacionog sistema alat instaliran da radi sve vreme onda se definicije sa-

kupljaju i instaliraju što je pre moguće. Kod specijalizovanih skriptova, potrebno je pre svakog korišćenja skripte proceniti da li je potrebno ažuriranje (npr. mrežnih segmenata, dns imena) ili ovaj proces uključiti u skriptu kako bi i on bio automatizovan. Aplikacije koje se pre provere ranjivosti instaliraju, imaju u sebi ugrađen proces ažuriranja, gde pre startovanja procesa aplikacija ažurira najnovije definicije.

Proces izveštavanja o ranjivostima informacionog sistema

Proces izveštavanja je bitan proces kako bi vlasnici informacionog sistema bili svesni ranjivosti informacionog sistema pod njihovim vlasništvom i kako bi bili u mogućnosti da pravilno upravljaju identifikovanim rizikom.

Sam proces mora biti pravilno definisan kako bi bio efikasan i moraju postojati načini izveštavanja u zavisnosti od stepena kritičnosti ranjivosti koja je otkrivena i uticanja na informacioni sistem i kompaniju u celosti.

2.4 TEHNIČKI PREDUSLOVI

2.4.1 Lista informacionih dobara

Lista informacionih dobara je važan deo tehničkih preduslova. Uglavnom uključuje sakupljanje detaljnih hardverskih i softverskih informacija o inventaru na osnovu kojih se donosi odluka o kupovini istih i njihovoj isporuci.

Upravljanje hardverskim sredstvima podrazumeva upravljanje fizičkim komponentama opreme i računarskim mrežama od nabavke do odstranjivanja. Učestala praksa obuhvata zahtev i proces odobravanja, upravljanje nabavkom, upravljački životni ciklus, isporuka odnosno raspoređivanje i upravljanje odstranjivanjem. Ključna komponenta je dobijanje finansijskih informacijama o životnom ciklusu hardvera koji pomaže organizaciji da donosi odluke na osnovu značajnih i merljivih finansijskih ciljeva.

Upravljanje softverskim sredstvima je sličan proces koji se fokusira na softverska sredstva, uključujući licence, verzije i instalirane agente na računarima.

Utvrđivanje liste informacionih dobara

Svi sistemi koji prenose, čuvaju ili obrađuju informacije a se nalaze u produkciji informacionog sistema kompanije moraju biti evidentirani i uključeni u proces upravljanja ranjivostima, kako bi se proces primenio na sve resurse koji se koriste u informacionom sistemu.

U okviru liste informacionih dobara treba da se nalazi najmanje:

- Ime sistema (DNS ime i/ili deskriptivni opis)
- Vlasnik sistema (ili glavni poslovni korisnik)
- Sistem administrator zadužen za sistem
- Fizička lokacija
- Port na koji je resurs priključen
- Softverska konfiguracija
- Vrsta operativnog sistema i verzija
- Instalirani softverski paketi
- Uključeni mrežni servisi
- IP adresa (ukoliko je statička, ili pul adresa ukoliko je resurs dobija IP adresu od DHCP)

Hardverska konfiguracija

- Procesor, Memorija , Prostor na diskovima (kapacitet, iskorišćenost), Eternet adresa, I/O kapacitet , Verzije firmvera

Određivanje grupe resursa po kritičnosti

Kako bi se skeniranje na ranjivosti moglo obaviti efikasnije i po prioritetima koji resursi i servisi imaju u okviru informacionog sistema, a u skladu sa potrebama i mogućim troškovima. Svi resursi koji se nalaze u informacionom sistemu po stepenu kritičnosti dele se na:

- Kritične
- Visoko
- Srednji
- Nizak

U zavisnosti od kritičnosti informacionog sistema i njegovih delova proces upravljanja ranjivostima mora se izvršavati u skladu sa nivoom rizika koje rukovodstvo organizacije prihvata. Optimalni intervali skeniranja informacionih dobara po nivoima kritičnosti i vremenski rok otklanjanja ranjivosti su dati u tabeli 1:

Tabela 1. – *Preporučeni intervali skeniranja skeniranje informacionih dobara po nivoima kritičnosti i rok otklanjanja ranjivosti*

Rb	Nivo kritičnosti	Raspored skeniranja (minimum)	Rok rešavanja pronađenih ranjivosti po kritičnostima
1	Kritični	Nedeljno	Odmah
2	Visok	Dvonedeljno	Nedeljno
3	Srednji	Mesečno	U roku od 3 nedelje
4	Nizak	Kvartalno	Kvartalno

Ukoliko postoji velika promena ili identifikovana nova ranjivost potrebno je aktivirati proces skeniranja kako bi ranjivosti bile identifikovane i otklonjene.

2.4.2 Skeniranje resursa na ranjivosti

Sva informaciona dobra koja se koriste u kompaniji moraju proći test ranjivosti, kako bi od strane rukovodstva definisan nivo rizika bio ostvaren na efikasan i sistematičan način. U zavisnosti od načina skeniranja i mogućeg uticaja na performanse i funkcionalnost sistema, termin za analizu se mora definisati tako da ne ugrozi rad produkcionog okruženja.

Sam proces skeniranja mora biti autorizovan od strane vlasnika informacionog sistema, koji je upoznat sa rasporedom skeniranja. Često se dešava u praksi da se skeniranje vrši van produkcionog vremena ili van radnog vremena pa je potrebno dozvoliti zaposlenima koji vrše skeniranja udaljeni pristup sistemima koji se skeniranju. Prilikom podešavanja skenera potrebno je obratiti pažnju da se ne naruši integritet informacionog sistema, u ovoj varijanti potrebno je podesiti skener tako da ne može vršiti promene na ciljanom operativnom sistemu ili apli-

kaciji. Rezultati skeniranja se klasifikuju kao strogo poverljivi i u skladu sa time se mora postupati sa ovim informacijama. Sam skener ne bi trebao biti aktivan na mreži ukoliko se ne koristi kako se bi došlo do kompromitovanja i neovlašćenog pristupa informacijama.

2.4.3 Alati za detektciju ranjivosti

Alati za detekciju ranjivosti, služe za skeniranje informacionog sistema, na poznate ranjivosti. Sastoje se od baze podataka koja sadrži identifikovane ranjivosti informacionog sistema. U okviru ove baze nalaze se informacije koje pomažu pri detekciji ranjivosti kao što su: servis, port, tip paketa, opis ranjivosti. Neke od osnovnih funkcionalnosti koje alati za detekciju ranjivosti imaju su:

- Ažuriranje baze podataka sa najnovijim ranjivostima
- Detekcija ranjivosti sa što manje grešaka
- Paralelno skeniranje resursa informacionog sistema
- Generisanje izveštaja sa kompletnim procesom otkrivanje ranjivosti (zahtev i odgovor)
- Preporuke kako popraviti ranjivost

Glavne razlike između besplatnih i komercijalnih verzija su:

Obim skeniranja – besplatni skeneri imaju ograničenja po broju IP adresa koje se mogu skenirati.

Broj napada i signatura – besplatni skeneri mogu imati značajno manji broj signatura i opisa ranjivosti, što je ključna karakteristika skenera.

Detaljnost izveštaja - Kod nekih besplatnih skenera detaljnost izveštaja može biti nedostatak, kao i izveštavanje po predefinisanim zahtevima standarda (recimo PCI DSS).

Po vrsti skeniranja koje mogu da izvrše skenere možemo da podelimo na:

- Mrežne skenere
- Host skenere
- DB skenere
- Skenere web aplikacija
- Multilevel skeneri

Mrežni skeneri - Automatizovani softver koji analiziraju jedan ili više sistema ili uređaja koji su povezani u mrežu kako bi pronašli indikatore ranjivostima na tim sistemima ili uređajima.

Host skeneri – Automatizovani softver koji analiziraju instancu operativnog sistema instaliranu na kojoj je skener instaliran, kako bi identifikovali ranjivosti tog operativnog sistema.

DB skeneri – Softver koji analizira instancu baze podataka, koji se nalazi na istoj ili različitoj platformi kao i baza podataka.

Skeneri web aplikacija – aktivni softver koji analizira instance web aplikacija, podešavanja servera i baza podataka koje rade u pozadini. Mogu biti instalirani na istoj platformi kao i web aplikacija ali se najčešće koriste kao poseban deo informacionog sistema. Neki skeneri ove vrste imaju arhitekturu klijent server, gde se klijent instalira na server koji hostuje aplikaciju a serverski deo na poseban host. U ovako opisanom scenariju identifikacija ranjivosti se sprovodi brže i efikasnije.

Multilevel skeneri – Ova vrsta skenera identifikuje ranjivosti na više nivoa informacionog sistema, kombinuje nekoliko karakteristika i kapaciteta dva ili više navedenih skenera.

Sa stanovišta instalacije instance skenere delimo na :

- Instalirane i hostovane u okviru informacionog sistema
- Instalirane i hostovane u okviru klaud (cloud) okruženja

Skeneri instalirani u okviru informacionog sistema – instalirani na poseban uređaj ili aplajans (appliance) koji se nalazi u virtuelnoj infrastrukturi, mora imati ograničen pristup samo zaposlenima koji rade na procesu upravljanja ranjivostima informacionog sistema ili zaposlenima koji koriste izveštaje (obično revizorima informacionog sistema)

Skeneri hostovani u klaud okruženju – ova vrsta skenera je popularna u poslednjih par godina kako klaud servisi sve više ulaze u korporativno okruženje, svi najveći dobavljači skenera nude za svoje skenere i opciju skeniranja iz klauda. Često se ova vrsta skenera koristi u procesu evaluacije pre kupovine skenera, ili ukoliko je skener potreban kao dodatno sredstvo verifikacije. Postavlja se pitanje poverljivosti informacija u klaud okruženju, ali postoje tehnike zaštite koje mogu da obezbede poverljivost izveštaja skenera hostovanih u klaud okruženju.

3 PROCES UPRAVLJANJA RANJIVOSTIMA U KORPORATIVNIM OKRUŽENJIMA

3.4.1 Bežično (wireless) okruženje

Među najčešćim rizicima koji se mogu sresti u korporativnim okruženjima predstavljaju nepromenjene inicijalne lozinke, ovakva vrsta ranjivosti informacionog sistema može da nanese veliku štetu pošto je ove vrste napada jako teško identifikovati i samim tim i reagovati.

```
root@winxp:~# hydra -l admin -P /root/wordlist/wordlist 10.12.11.132 http-post-form "
      /login.php:Login="^USER^"&Password="^PASS^":Invalid"
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service
 organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-02-14 14:00:40
[DATA] max 3 tasks per 1 server, overall 64 tasks, 3 login tries (l:1/p:3), ~0 tries pe
r task
[DATA] attacking service http-post-form on port 80
[80][http-post-form] host: 10.12.11.132   login: admin   password: Admin
[80][http-post-form] host: 10.12.11.132   login: admin   password: nesto
[80][http-post-form] host: 10.12.11.132   login: admin   password: admin
1 of 1 target successfully completed, 3 valid passwords found
```

Slika 1. - *Hydra*

root@winxp:~# hydra -l admin -P /root/wordlist/wordlist 10.12.11.132 http-post-form "/xcisco/login.php:Login="^USER^"&Password="^PASS^":Invalid"

U posmatranom okruženju kontrolerima bežične mreže se može pristupati preko veb interfejsa logovanjem u kombinaciji korisničko ime i lozinka.

Hydra alat koristi se za napad rečnikom (*Dictionary attack*), koji se sastoji od pokušaja logovanja na udaljeni sistem tako što se veliki broj reči koje se nalaze u rečniku pokušava upotrebiti kao lozinka. Ovaj alat na distribuciji Kali Linux dolazi u dve varijante jedna je kao alat koji je integrisan kroz komandnu liniju i kroz grafički interfejs.

Testiranje ove vrste ranjivosti izvodimo na Kali Linux distribuciji, koristeći komandnu liniju (*Command line interface CLI*).

Ovim alatom je utvrđeno da postoji administratorski nalog kojim se može pristupiti uređaju preko veb interfejsa, a da koristi podrazumevanu lozinku i lozinku koju je lako pogoditi a nalazi se u rečniku pa je moguće izvršiti tzv. napad rečnikom.

Ovaj deo infrastrukture koji se nalazi pokriven bežičnom mrežom smatramo kritičnim pošto kroz ovu infrastrukturu prolaze informacije koje mogu biti klasifikovane kao tajne, a dostupnost i integritet ovog dela informacionog sistema mora biti visok.

Sve pronađene ranjivosti su po klasifikaciji spadaju u kritične pa se mora odmah pristupiti otklanjanju

Interna klasifikacija i uklanjanje ranjivosti za bežično (wireless) okruženje dato je u tabeli 2.

Tabela 2. - *Interna klasifikacija i uklanjanje ranjivosti*

Rb.	Ranjivost	Predložene mere bezbednosti	Procenjeno vreme implementacije	Uticaj na produkciju
1	Slaba lozinka za administratorski pristup pristupnim tačkama bežične mreže	Promena administratorske lozinke, u lozinku koja nije bazirana na rečniku i sadrži brojeve , velika i mala slova, specijalne karaktere	0.5 radni dan	Nema

3.4.2 Serversko okruženje

Serversko okruženje je sastavljeno od vindovs (*Windows*) operativnih sistema, u okruženju koje posmatramo. Za otkrivanje ranjivosti koristimo Nessus skener instaliran ha posebnom hostu koji ima mogućnost pristupa raznim mrežnim segmentima, kako bi se smanjio rizik kompromitovanja ovaj host nije aktivan kada se ne vrši skeniranje. Pošto se skenira vindovs (Windows) okruženje skener je podešen da koristi takozvani autentifikovani sken, gde se u procesu skeniranja aplikacijama i operativnom sistemu pristupa sa korisnikom koji se može autentifikovati. Ovaj sken smo izvršili koristeći nalog sa administratorskim privilegijama, kojim se mogu otkriti ranjivosti brže i efikasnije. Ovaj nalog ima lokalna administratorska prava, a u principu se aktivira samo kada se izvršava proces upravljanja ranjivostima, kada se proces ne izvršava, ovaj nalog se deaktivira, a lozinka za pristup ovom nalogu se menja i kovertira, kako ne bi došlo do kompromitovanja ovog naloga sa visokim privilegijama. Uključeni plaginovi (*plugins*)u skeneru su Windows, Windows Microsoft buletins, Windows user managment.

Tokom skeniranja otkrivene su ranjivosti koje su date u tabeli 3.

Tabela 3. - *Ranjivosti serverskog okruženja*

Plugin ID	Risk	Port	Name
97833	Critical	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
90510	Medium	49156	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
10150	None	445	Windows NetBIOS / SMB Remote Host Information Disclosure
10394	None	445	Microsoft Windows SMB Log In Possible
10736	None	135,445,49155,49156,49154,49153,49152	DCE Services Enumeration
10785	None	445	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
11011	None	445	Microsoft Windows SMB Service Detection
11219	None	135	Nessus SYN scanner
11219	None	445	Nessus SYN scanner
19506	None	0	Nessus Scan Information

Interna klasifikacija i uklanjanje ranjivosti za serversko okruženje dato je u tabeli 4

Tabela 4. - *Interna klasifikacija i uklanjanje ranjivosti u serverskom okruženju*

Rb.	Ranjivost	Predložene mere bezbednosti	Procenjeno vreme implementacije	Uticaj na produkciju
1	MS17-010: Security Update for Microsoft Windows SMB Server	Ažuriranje operativnog sistema	0.5 radni dan	Restart produkcionih sistema van produkcionog vremena
2	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)	Ažuriranje operativnog sistema	0.5 radni dan	Restart produkcionih sistema van produkcionog vremena

3.4.3 Mail server

Mail server koji posmatramo u ovom radu služi za distribuciju internih obaveštenja sa IKT sistema i u okviru skenera su uključeni plaginovi (*plugins*) Windows, Windows Microsoft buletins, Windows user managment i Mail.

Sumarni pregled ranjivosti koje su identifikovane na mail serveru date su u tabeli 4.

Tabela 4. - *Ranjivosti koje su identifikovane na mail serveru*

Plugin ID	Risk	Port	Name
97833	Critical	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
90510	Medium	49156	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
10150	None	445	Windows NetBIOS / SMB Remote Host Information Disclosure
10394	None	445	Microsoft Windows SMB Log In Possible
10736	None	135, 445, 49155, 49156, 49154, 49153, 49152,	DCE Services Enumeration

Interna klasifikacija i uklanjanje ranjivosti data je u tabeli 5.

Tabela 5. - *Interna klasifikacija i uklanjanje ranjivosti na mail serveru*

Rb.	Ranjivost	Predložene mere bezbednosti	Procenjeno vreme implementacije	Uticaj na produkciju
1	MS17-010: Security Update for Microsoft Windows SMB Server	Ažuriranje operativnog sistema	0.5 radni dan	Restart produkcionih sistema van produkcionog vremena
2	Nessus SYN scanner - list of open ports	Revizija otvorenih portova	1 radni dan	Moguće zatvaranje portova
3	SSL Certificate Cannot Be Trusted	Ažuriranja i zamena sertifikata, sertifikatom koj je izdat od autorizovanog sertifikacionog tela	0.5 radni dan, sama zamena sertifikata, kupovina sertifikata 3 nedelje	Nema uticaja na produkciju
4	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)	Ažuriranje operativnog sistema	1 radni dan	Restart van produkcionog vremena
5	ICMP Timestamp Request Remote Date Disclosure	Promena mrežnih parametara servera	1 radni dan	Restart van produkcionog vremena

Identifikovane ranjivosti na mail serveru možemo svrstati u različite grupe, one koje će se ukloniti u svakodnevnom operativnom radu (ranjivosti u tabeli 4 pod rednim brojem 1,2 i 4),ranjivosti koje moraju biti tretirane kao deo strateških promena (ranjivosti u tabeli 4 pod rednim brojem 3) i ranjivosti niske kritičnosti koje se tretiraju i uklanjaju u okviru promene arhitekture bezbednosti informacionih sistema i strategije zaštite (ranjivosti u tabeli 5. pod rednim brojem 5).

Ranjivosti koje su niskog prioriteta i uklanjaju se kada se menja arhitektura bezbednosti i strategije zaštite, često se u praksi reše tako što proizvođači softvera (software) i proizvođači operativnih sistema ovakve propuste reše pa se u korporativnom okruženju ovakvi propusti reše ažuriranjem aplikacije ili operativnog sistema.

3.4.4 Web aplikacija

Interna veb aplikacija koja se koristi kao interni portal za distribuciju obaveštenja zaposlenima i sadrži podatke o zaposlenima. Autentifikacija ove aplikacije se vrši na preko LDAP servera, koji je deo vindovs (*Windows*) aktivnog direktorijuma. Pri skeniranju su korišćeni plaginovi (*plugins*) CGI abuses, CGI abuses XSS. Settings, Web servers, Web applications.

Tabela 6 - *Ranjivosti koje su identifikovane na veb aplikaciji*

Plugin ID	Risk	Port	Name
39466	High	80,443, 8080, 8443	CGI Generic XSS
44136	High	80,443, 8080, 8443	CGI Generic Cookie Injection Scripting
85582	High	80,443, 8080, 8443, 9080, 9443	Web Application Potentially Vulnerable to Clickjacking
10677	Medium	80	Apache mod_status /server-status Information Disclosure
10677	Medium	443	Apache mod_status /server-status Information Disclosure
11213	Medium	80,443	HTTP TRACE / TRACK Methods Allowed
11229	Medium	80, 443, 8080, 9080, 9443	Web Server info.php / phpinfo.php Detection
11447	Medium	80, 443, 8080, 9080, 9443	Nuked-Klan index.php Multiple Module Vulnerabilities
24726	Medium	80, 443, 8080,	SQLiteManager SQLiteManager_ currentTheme Cookie Traversal Local File Inclusion
40984	Medium	80, 443, 8080, 9080, 9443	Browsable Web Directories
46803	Medium	80, 443, 8080, 9080, 9443	PHP expose_php Information Disclosure
47831	Medium	9080, 9443	CGI Generic XSS (comprehensive test)
49067	Medium	80,443, 8080, 8443	CGI Generic HTML Injections (quick test)
51425	Medium	80,443, 8080, 8443	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)
57640	Medium	80, 443, 8080, 9080, 9443	Web Application Information Disclosure
88098	Medium	80, 443	Apache Server ETag Header Information Disclosure
10107	None	80	HTTP Server Type and Version

Tabela 7. - *Interna klasifikacija i uklanjanje ranjivosti na veb aplikaciji*

Rb.	Ranjivost	Predložene mere bezbednosti	Procenjeno vreme implementacije	Uticaj na produkciju
1	CGI Generic XSS	Validacija i enkodiranje korisničkih inputa	6 radnih dana	Promena parametara aplikacije, nema uticaja na produkciju
2	CGI Generic Cookie Injection Scripting	Promena konfiguracije httpd. conf fajla	1 radni dan	Promena parametara aplikacije, nema uticaja na produkciju
3	Web Application Potentially Vulnerable to Clickjacking	Uključiti X-Frame-Options or Content-Security-Policy u okviru HTTP hedera.	2.5 radna dana	Nema uticaja na produkciju
4	Apace mod_status /server-status Information Disclosure	Isključivanje mod_status opcije na Apache serveru	1 radni dan	Nema uticaja
5	HTTP TRACE / TRACK Methods Allowed	Ukidanje navedenih metoda na veb serveru	1 radni dan	Nema uticaja
6	Web Server info. php / phpinfo.php Detection Nuked-Klan index.php Multiple Module Vulnerabilities	Uklanjanje navedenih fajlova sa servera	0.5 radni dan	Nema uticaja
7	SQLiteManager SQLiteManager_ currentTheme Cookie Traversal Local File Inclusion	Promena konfiguracije SQL manager	1 radni dan	Nema uticaja
8	Browsable Web Directories PHP expose_php Information Disclosure	Promena konfiguracionog fajla php.ini	05. radni dan	Nema uticaja
9	CGI Generic HTML Injections (quick test)	Validacija i enkodiranje korisničkih inputa	2 radna dana	Nema uticaja
10	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)	Validacija i enkodiranje korisničkih inputa	2 radna dana	Nema uticaja
11	Web Application Information Disclosure	Filtriranje informacija o putanjama na serveru	2 radna dana	Nema uticaja
12	Apache Server ETag Header Information Disclosure	Promeniti HTTP ETag heder na veb serveru da ne uključuje inodove fajlova u ETag hederu.	2 radna dana	Nema uticaja
13	HTTP Server Type and Version	Ne tretirati ranjivost	-	-

3.4.5 FTP server

U okviru korporativnog okruženja koristi se FTP (File Transfer Protocol) server koji služi za razmenu velikih fajlova u okviru iste interne mreže ili za prevlačenje verzija korisničkih aplikacija. Korišćeni su plaginovi (*plugins*) prilikom ovog skeniranja su Windows, Windows Microsoft buletins, Windows user managmeent , FTP.

Tabela 7 prikazuje sumarno ranjivosti koje su identifikovane na FTP serveru:

Tabela 7. - *Ranjivosti koje su identifikovane na FTP serveru*

Plugin ID	Risk	Protocol	Port	Name
10081	Critical	tcp	21	FTP Privileged Port Bounce Scan
97833	Critical	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
90510	Medium	tcp	49156	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

Interna klasifikacija i uklanjanje ranjivosti prikazane su u tabeli 8.

Tabela 8. - *Interna klasifikacija i uklanjanje ranjivosti na FTP serveru*

Rb.	Ranjivost	Predložene mere bezbednosti	Procenjeno vreme implementacije	Uticaj na produkciju
1	FTP Privileged Port Bounce Scan	Promena konfiguracije FTP servera	0.5 radni dan	Restart produkcionih sistema van produkcionog vremena
2	MS17-010: Security Update for Microsoft Windows SMB Server (4013389)	Ažuriranje operativnog sistema	1 radni dan	Restart produkcionih sistema van produkcionog vremena
3	MS16-047: Security Update for SAM and LSAD Remote Protocols	Ažuriranje operativnog sistema	1 radni dan	Restart produkcionih sistema van produkcionog vremena

3.4.6 FTP server varijanta 1

U ovom delu ćemo posmatrati, konfiguraciju FTP servera i Windows XP operativnog sistema koji je u ovom momentu nema zvaničnu podršku Majkrosoft korporacije, (zvanično je podrška prestala 08.04.2014 godine). Pri konfiguraciji skenera korišćena su podešavanja kao

Dobijeni su identični rezultati ali kada se identifikuju ranjivosti drugačijom metodom i alatima dobijaju se drugačiji rezultati.

Kada se ovaj deo IKT sistema proveri sa nmap alatom dobijamo sledeće rezultate.

root@winxp:~# nmap -sS -O -sV 10.12.11.137

Gde je: *-sS skeniranje portova Syc scan*
-sV verzionisanje servisa i aplikacija koje su aktivni na otvorenom portu
-O otkrivanje operativnog sistema

Kada rezultate ovog skena potražimo u Metasploitu dobijamo sledeće rezultate:

Ova verzija FTP servera je ranjiva, ima bafer overfolov (*Buffer overflow*). Podešavamo Metasploit kako bi proverili da li ranjivost stvarno postoji.

root@winxp:~# msfconsole

msf > use exploit/windows/ftp/freefloatftp_user

msf exploit(freefloatftp_user) > set RHOST 10.11.12.137

msf exploit(freefloatftp_user) > set payload windows/meterpreter/reverse_tcp

msf exploit(freefloatftp_user) > set LHOST 10.11.12.13

msf exploit(freefloatftp_user) > exploit

Kada se pokrene komanda ranjivost je potvrđena tako što je uspostavljena sesija na udaljenom računaru.

Na slici 2 se vidi kako je preuzeta kontrola na računarom, koji je u okviru korporativne mreže.

Ovim slučajem je pokazano kako skener koji je korišćen u svrhu ovog rada nije prepoznao ranjivost FloatFTP servera koji je ranjiv ukoliko se koristi na XP operativnom sistemu. Svakako da je u ovom slučaju veći rizik predstavlja korišćenje zastarelog operativnog sistema.

4 REZULTATI TESTIRANJA, ANALIZA SISTEMA I METODOLOGIJE, PREDLOZI ZA POBOLJŠANJE

U okviru ovog procesa identifikovanja ranjivosti identifikovane je 19 kritičnih ranjivosti, 13 ranjivosti sa visokim rizikom i 3 ranjivosti koje su klasifikovane kao niske.

Ovaj broj predstavlja visok nivo otkrivenih kritičnih ranjivosti, koje su po svojoj strukturi možemo svrstati u dve grupe, jedna grupa je ranjivosti koje nastaju iz drugog neefikasnog procesa (u ovom slučaju neefikasnog procesa upravljanja bezbednosnim zakrpama (*eng. Patch management*) (13). Drugu grupu ranjivosti možemo okarakterisati kao ranjivosti nastale usled pogrešno konfigurisanih delova IKT sistema odnosno potrebno je unaprediti proces upravljanja promenama (*eng. Change management*) (14).

Ovo je dobar primer kako sam proces upravljanja ranjivostima može uticati na ostale procese u okviru IKT dela kompanije ali i na ostale poslove delove.

Potrebno je naglasiti da se ova tri procesa moraju sinhronizovati kako bi se dobio kvalitetan rezultat, tj. potrebno je izvršiti proces upravljanja bezbednosnim zakrpama, pa upravljanje promenama, a onda kao kontrolna funkcija može da se izvrši proces upravljanja ranjivostima.

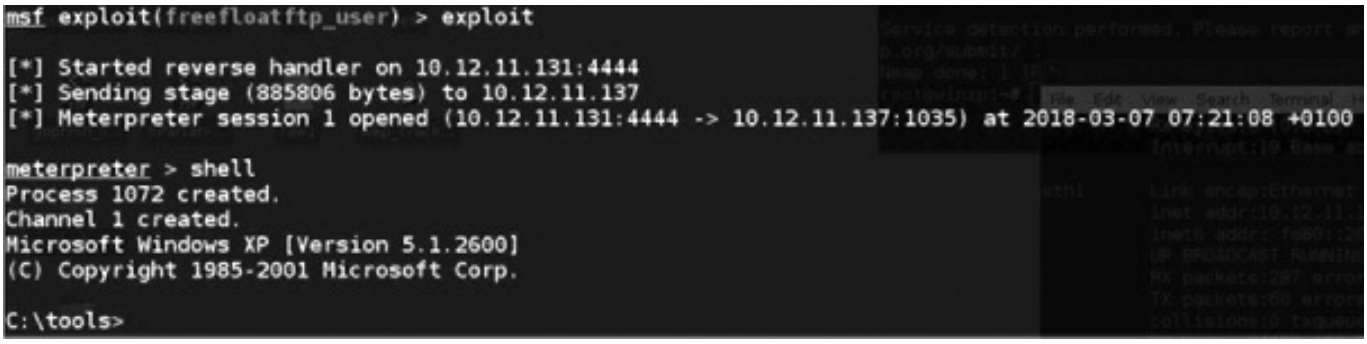
Ono što predstavlja kritičan deo celog procesa upravljanja ranjivostima je inventar informacionih dobara, ono što se u praksi često sreće je da popis informacionih dobara nije potpun i da deo informacionog sistema ostane van procesa upravljanja informacionim sistemima.

Jedno od rešenja ovog izazova se rešava tako što se u proces upravljanja ranjivostima doda i proces identifikacije informacionih dobara. Ovim procesom se dobija na tačnosti u okviru procesa upravljanja ranjivostima. Međutim primenom ovog procesa može doći do produženja samog procesa identifikacije ranjivosti, kao i do narušavanja performansi korporativnih mreža usled skeniranja i procesa otkrivanja informatičkih dobara.

Svakako se pažljivim konfigurisanjem opcija skeniranja mreža i odgovarajućim podsistemom može postići efikasno otkrivanje novih informacionih dobara. Ali je potrebno naglasiti da bi zbog efikasnosti ovaj proces trebao biti uspostavljen u okviru IKT okruženja, a da proces upravljanja ranjivostima koristi resurse iz njega.

Jedna od opcija je da se u postojećoj mrežnoj infrastrukturi identifikuju novi operativni sistemi i da se na početku procesa posmatraju kao uljezi u mrežu i da se na osnovu toga radi prvo detaljno skeniranje i identifikacija ranjivosti.

Drugi problem predstavlja scenario sa FTP serverom na operativnom sistemu Windows XP, gde u procesu skeniranja, skener nije prepoznao ranjivost samog FTP servera. U ovom



Slika 2. - *Metasploit kontrola nad udaljenim računarom*

scenariju, ranjivosti samog operativnog sistema bi mogle biti rešene dodatnim merama bezbednosti (zatvaranjem portova, aktiviranjem HIPS (*eng. Hostbased Intrusion Detection System*) sistema, itd.)

Kako bi se sam proces identifikacije ranjivosti unapredio, potrebno je da se ranjivosti identifikuju alatima koji imaju različite baze podataka i različitu logiku rada, kako bi se pokrio što veći broj ranjivosti i vairjeteta ranjivosti.

5 ZAKLJUČAK

Proces upravljanja ranjivostima može značajno unaprediti ICT procese pre svega proces upravljanja incidentima i ova dva procesa se mogu uspešno kombinovati, na način da se sve pronađene ranjivosti prebace u laboratoriju i da se iskorištavanje ranjivosti proba identifikovati kao deo procesa identifikacije i upravljanja incidentima. Ovako kombinovanje procesa može biti korišćeno za praćenje performansi i jednog i drugog procesa i te se performanse na planiran i proveren način mogu unaprediti. Svakako skener koji se koristi u procesu identifikovanja ranjivostima može se na ovaj način testirati ali i tehnički sistemi koji se koriste da identifikaciju incidenata kao što su *SIEM* (eng. *Security information and event management*) i drugi alati. Tradicionalno poslovanje, ubrzano se menja, naročito podstaknuto razvojem informaciono-komunikacionih tehnologija. Tradicionalno zatvoreni IKT sistemi postaju sve otvoreniji, a informacije koje su se koristile isključivo sa internog a nekada i fizički odvojenih IKT okruženja postaju dostupne sa Interneta. Proces upravljanja ranjivostima predstavlja jedan od ključnih procesa za zaštitu informacionih sistema. Efikasnim i zrelim procesom upravljanja ranjivostima, površina za napad na informacioni sistem se smanjuje, a mogućnost da napad bude otkriven višestruko se povećava. Pravilno definisan i primenjen proces upravljanja ranjivostima može uveliko da doprinese unapređenja nivoa informacione bezbednosti, otklanjanjem ranjivosti, podizanjem svesti zaposlenih u okviru IKT organizacionog dela ali i rukovodstva koje se upoznaje sa identifikovanim i otklonjenim ranjivostima. Pravilna primena procesa dovodi do unapređenja celokupnog informacionog sistema pošto se identifikacija ranjivosti može proširiti i šire IKT procese kao što je upravljanje identitetima, zaštita od odliva informacija i druge. Kao što je pokazano u ovom tekstu, praktična primena procesa nije nimalo jednostavna i rutinska operacija. Potrebno je mnogo znanja, resursa kako kadrovskih tako i tehničkih da bi se primenile najbolje prakse pri projektovanju i izgradnji bezbednih informacionih sistema.

6 LITERATURA

[1] International Organization for Standardization ISO/IEC 27000 family - Information security management systems. *International Organization for Standardization.* [Na mreži] Januar 2018. https://www.iso.org/isoiec-27001-information-security.html

[2] (ISC)². Certified Information Systems Security Professional. *ISC2 Consortium* . [Na mreži] Januar 2018. https://www.isc2.org/Certifications/CISSP

[3] IBM Asset management tool. [Na mreži] https://www.ibm.com/internet-of-things/business-solutions/asset-management

[4] CA Asset managmeent tool . [Na mreži] http://www.ca.com/us/intellicenter/ca-it-asset-manager.aspx

[5] Oracle Asset management tool. [Na mreži] https://www.oracle.com/applications/supply-chain-management/solutions/maintenance-management/asset-maintenance.html.

[6] Open Vulnerability Assessment System. [Na mreži] http://www.openvas.org/

[7] Retina CS Community. [Na mreži] Retina CS Community

[8] Nessus comunity . [Na mreži] https://www.tenable.com/downloads/nessus

[9] Rapid 7 Nexpose . [Na mreži] https://www.rapid7.com/products/nexpose/

[10] Tenable.io Vulnerability Management . [Na mreži] https://www.tenable.com/products/tenable-io

[11] Microsoft Baseline Security Analyzer (MBSA). [Na mreži] https://www.microsoft.com/en-us/download/details.aspx?id=7558

[12] Belarc Adviser. [Na mreži] https://www.belarc.com/products_belarc_advisor

[13] Patch management . [Na mreži] https://en.wikipedia.org/wiki/Vulnerability_management.

[14] Change management . *Wikipedia.* [Na mreži] https://en.wikipedia.org/wiki/Change_management_(engineering).

[15] Qualys vulnerability management . [Na mreži] https://www.qualys.com/apps/vulnerability-management/

Aleksandar Bratić, Javno preduzeće "Elektroprivreda Srbije"
Kontakt: aco@bratic.rs
Oblasti interesovanja: bezbednost informacija i informacionih sistema, privatnost ličnih podataka, implemenatacija sistema bezbednosti, enterprise architecture