Upravljanje sa ranjivostima informacionih sistema i savjetodavni servisi

Slobodan Pavićević i Božo Krstajić, member, IEEE

***Sadržaj* - Proces otkrivanja ranjivosti sistema i njegovo povezivanje sa savjetodavnim servisima je fundamentalni osnov za pravljenje bezbjednih sistema. Ovaj rad ima za cilj da generički prikaže vrijednost oba sistema, njihove komplementarne pozicije, da ukaže na moguće modele njihove integracije**.

***Ključne riječi* - Informacioni sistemi (IS), Ranjivosti IS-a, Zakrpe IS-a.**

I. UVOD

Zaštita IT resursa je kompleksan zadatak. Upravljanje sa ranjivostima informacionih sistema (Vulnerability Manegement - VM) je nezaobilazan u tom postupku. Može se pokazati da jedan VM sistem, u kompanijama koje vode računa o svojim resursima, nije dovoljan, odnosno da postoji i njegova nadogradnja. Nadogradnja takvog sistema u sistem za upravljanje ranjivostima IS-a sa savjetodavnim servisima (IS Vulnerability and Advisary Managemenet – VAM) je dodatna vrijednost VM.

Sistematičan pristup u primjeni VM i VAM sistema [1] i prepoznavanje značaja ovog procesa značajno doprinosi u opštem povećanju sigurnosti IT sistema.

II. UPRAVLJANJE SA RANJIVOSTIMA IS

A. *Opšte o VM*

Upravljanje ranjivostima sistema je proces pronalaženja i otklanjanja grešaka u software-u operativnih sistema i raznih aplikacija, kao i konfiguracionih grešaka u njima. To je proces u kojem se redovno i kontinuirano koriste posebni alati i procedure koje aktivno pomažu u eliminisanju rizika koje nose ranjivnosti sistema. Nadalje, taj proces ima i sledeće ciljeve: ispravka grešaka u programu koje imaju uticaja na sigurnost, performantnost i funkcionalnost sistema; uočavanje posebnih sigurnosnih opasnosti; promjene programskih konfiguracija sa ciljem smanjenja vjerovatnoće za napad, ubrzanja rada sistema i njegove funkcionalnosti i dokumentovanje stanja sigurnosnih sistema i njihove usaglašenosti sa zakonima, pravilima i poslovnim politikama

Svrha VM procesa je proaktivno djelovanje i sastoji se iz sledećih segmenata[2,3]:

Kreiranje VM politike [4], sigurnosnih procedura i kontrola. Svaka kompanija bi trebala da ima usvojen set sigurnosnih politika, kojim se definišu, pored ostalog, i standardne konfiguracije za sve sigurnosne uređaje i aplikacije, kakve su antivirusne kontrole, firewall-i, intrusion/prevention sistemi, enkripcija, VPN pristup itd.

Kreiranje baze podataka opreme i njihova kategorizacija - U ovom koraku se pravi inventar svog hardwera, softwera, aplikacija, servisa i konfiguracija od interesa. Segmentira se tj. kategorišu resursi po principu poslovne važnosti.

Skeniranje sistema - Ovo je najvažnija faza u VM, u kojoj se otkrivaju slabosti tj ranjivosti sistema. Skeniraju se uređaji, njihovi servisi, aplikacije, konfiguracije. Rezultati skeniranja su izvještaji koji sadrže informaciju o pronađenim ranjivostima i propustima na sistemima.

Poređenje ranjivosti sa svjetskim standardizovanim bazama otkrivenih ranjivosti - Kada se otkriju ranjivosti sistema tokom procesa skeniranja, postoji vjerovatnoća da je dio tih otkrića false-positive. Veliku ulogu u eliminisanju takvih slučajeve je korišćenje standardizovanih industrijskih baza podataka o otkrivenim ranjivostima, kao što su Common Vulnerability and Exposures (CVE) liste i NIST National Vulnerablity Database (NIST NVE), SANS Top 20, CERT Vulnerability Notes.

Klasifikacija i analiza rizika - Otkrivene ranjivosti nemaju sve isti značaj i prioritet. Stoga je potrebno napraviti plan šta je od najvećeg prioriteta za otklanjanje i usredsrediti se na brzu eliminaciju slabosti koje su proglašene kao ranjivosti visokog rizika odnosno prioriteta. Za slabosti nižeg prioriteta se prave dugoročniji planovi.

Rješavanje problema na testnim sistemima - Preporuke i načini kako se otkriveni problemi mogu riješiti mogu u pojedinim situacijama ugroziti funkcionalnost određenih poslovnih procesa. Dobra praksa je da se patchevi (zakrpe) testiraju prvo na testnom kompanijskom okruženju kako bi se smanjio rizik od eventualnih šteta.

Primjena patch-eva, ispravki i mogućih rješenja - Automatizovana, brza i sigurna rješenja distribucije patcheva i software vrlo su važna u ovom procesu.

Ponovno skeniranje odnosno verifikacija obavljenih ispravki - Nakon što se obavi proces ispravki sistema, potrebno je to i verifikovati ponovnim skeniranjem. Tokom ponovnog skeniranje se može ustanoviti u kojoj je mjeri proces popravki bio uspješan, ali takođe i otkriti da li se tokom tog procese pojavila i neka druga slabost ili ranjivost sistema.

B. *Zakoni ranjivosti sistema*

Cilj kojem teži osoblje IT odeljenja je da postigne veliki procenat sigurnosti svojih mrežnih i serverskih resursa. Od suštinske važnosti je da se upostave vremenski okviri u odnosu na koje je potrebno reagovati i otkloniti otkrivenu ranjivost. Analizirajući veliki broj otkrivenih ranjivosti u dvije odvojene statističke obrade iz 2004 godine [5] i 2008

Slobodan Pavićević, Crnogorski Telekom, Moskovska 29, 81000 Podgorica, Crna Gora (telefon: +38220433251; e-mail: slobodan.pavicevic@telekom.me).
Božo Krstajić, ETF Podgorica, Džordža Vašingtona bb, 81000 Podgorica, Crna Gora (telefon: +38220244406; e-mail: bozok@ac.me).

godine [6], baziranog na milione slučajeva skeniranja različitih mreža, Qualys je u svojem istraživanju uočio određene zakonitosti koje se odnose na vremena trajanja tj. uklanjana otkrivenih ranjivosti i kakav je njihov uticaj na sigurnost. Svaka organizacija bi morala proučiti ove zakonitosti i praksu, kako bi na adekvatan način uspostavila svoja pravila koja najbolje zadovoljavaju njihove potrebe.

Uspješnost primjene VM i sistema za ispravku programskih propusta (Patch Management – PM) statistički gledano ima svoje zakonitosti. [5,6]

The low of Half –Life: Polu život kritičnih ranjivosti sistema je oko 30 dana (30 dana u 2004 godini, 29,5 u 2008 godini) i udvostručuje se sa smanjenjem stepena kritičnosti. Podaci pokazuju da se, od kritičnih ranjivosti sistema otkrivenih u jednom mjesecu, otklone, prosječno samo polovina njih. *Dobra praksa je da se svi sistemi isprave u roku od 21 dana od dana otkrivanja ranjivosti, uzevši u obzir da je tempo kojim se otkrivene ranjivosti sistema eksploatišu sve brži tj. vrijeme eksploatacije ranjivosti kraće.*

The Low of Prevalence: Zakon opštosti kaže da se 50 % (2004 godina) ili 60 % (2008 godina) ozbiljnih i kritičnih ranjivosti (TOP 20) u jednoj godini zamijeni sa potpuno novim. Statistika pokazuje da polovina otkrivenih ranjivosti još uvjek postoje u mreži čak godinu dana nakon njihovog otkrića. *Dobra praksa je da se kritični resursi skeniraju na slabosti i ranjivosti svakih 5 do 10 dana.*

The Low of Persistence: Životni ciklus nekih ranjivosti je neograničen. Razlog za to mogu biti nove sistemske i programske instalacije tj. stavljanje novih sistema u mrežu koji nijesu prošli potrebna sigurnosna skeniranja, prije puštanja u produkciji. Najnovija istraživanja pokazuju da je procenat ranjivosti koje nikada ne budu ispravljene na nivou 5 do10 %, pa čak i za one koje se smatraju kritičnim. *Dobra praksa je da se prije puštanja nekog sistema u produkcijskom okruženju obavi skeniranje sistema na ranjivosti i otkrivene ranjivosti otklone.*

The Low of Exploitation: Osam procenata dostupnih exploit-a (načina zloupotrebe) za ranjivosti sistema se pojavi u roku od 60 dana od kada se ranjivost objavi (2004 godine). Od trenutka kada se objavi ranjivost sistema počinje trka između napadača koji to hoće iskoristiti i kompanije da na odgovarajući način zakrpi ranjivost. U 2008 i 2009 godini, trendovi su se promijenili dramatično pokazujući da je sada prosječno potrebno 10 dana da mnogi exploit-i budu dostupni u javnost. Još više, postojanje (notirano oko 56) „zero-day“ exploita (exploit je dostupan na korišćenje u istom danu kad je objavljena ranjivost) govori da je bitno biti brz u otklanjaju ranjivosti. *Dobra praksa kaže da je neophodno pažljivo pratiti sve objave glavih proizvođača software-a o dostupnim zakrpama za sisteme, donositi timske odluke u vezi sa njihovom primjenom i što više integrisati VM sisteme sa sistemima za upravljanje zakrpama i sistemima za kontrolu konfiguracija. Takođe, potrebno je imati odgovarajuću proceduru kao odgovor na urgentne rizike.*

Analize ovih rezultata daju sledeće bitne preporuke: Moraju se pokriti svi nivoi infrastrukture, posebno interni resursi i oni resursi koji napuštaju lokalno mrežno okruženje. Mora se ubrzati ciklus zakrpa, fokusirajući se na smanjenje half-life parametra ispravljanjem aplikacija i segmentiranjem resursa u one kojima je potrebna brza, srednja i spora zakrpa sistema

III. SERVIS OBAVJEŠTAVANJA O RANJIVOSTIMA I ZAKRPAMA I SISTEM UPRAVLJANJA SAVJETODAVNIM SERVISIMA

A. *Opis servisa i različiti modeli*

Servis obavještavanja o otkrivenim ranjivostima i zakrpama i sistem upravljanja sigurnosnim savjetima je korisna alatka u funkciji zaštite IT resursa. Uloga ovog servisa je da obezbijediti svim zainteresovanim korisnicima tj. kompanijama lak pristup do informacija o bezbjednosnim propustima koji su upravo otkriveni ili već postoje, sa jedne strane, ali i da prepuruči metode za rješavanje tih propusta, sa druge strane. Servis koji se nudi je baziran na upotrebi ekspertize i znanja koje imaju kompanije koje se bave ovom djelatnošću, a ima za cilj da u najkraćem roku dostavi korisnicima informacije o otkrivenim ranjivostima, exploitima, sigurnosnim opasnostima, sa kategorizacijom nivoa sigurnosne opasnosti i detaljnim opisom uočenog ponašanja opasnosti, kao i precizna i jasna uputstva i instrukcije za njihovo prevazilaženje.

Pored VM rješenja koji predstavlja dobar izvor informacija o ranjivostima i slabostima sistema, kao i zakrpama, na već opisan način, postoji još nekoliko različitih tipova izvora informacija [1], sa svojim prednostima i manama:

Sajtovi velikih proizvođaca software-a i njihove mailing liste - Veoma popularan izvor informacija. Patchevi se izdaju od samih proizvođača SW, što daje dodatnu sigurnost u njegovu primjenu. Gotovo sigurno su oslobođeni od zlonamjernog koda i po pravilu sadrže sve potrebno za eliminaciju ranjivosti. Potencijalno je loše što neki od otkrivenih problema neće biti proslijeđeni prije nego se ne nađe odgovarajuća zakrpa, a administratori sistema su prinuđeni da prate više proizvođača i više aplikacija na različitim mjestima

Posebni specijalizovani sajtovi (third party sites) - U principu nijesu vezani ni za jednog velikog proizvođača posebno, a karakteriše ih: brzo objavljivanje otkrivenih slabosti i rješenja, mogućnost praćenja više različitih proizvođača i proizvoda sa jednog mjesta, mogućnost specijalizacije po određenom proizvodu, mogućnost uključenja mailing lista, mogućnost filtriranja podataka od interesa. Takođe, nekada podaci dobijeni od specijalizovanih sajtova jesu bolja alternativa od samih proizvođača SW i mogu se dobiti informacije koje sam proizvođač SW ne daje u javnosti. Potencijalno postoji opasnost da patchevi imaju teže posledice na funkcionalnost SW koji se štiti ili da sadrže maliciozni kod, a nekad nije dovoljna informacija koja je dostupna za zaštitu sistema, već je potrebno i dalje istraživati za kvalitetno rješenje.

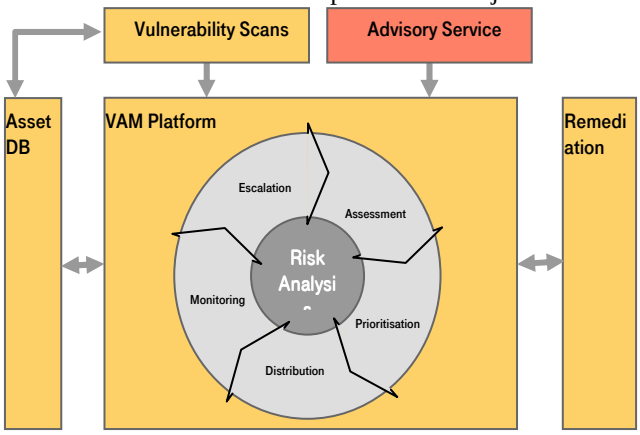
Posebne specijalizovane mailing liste i newsgroups - Ovaj tip izvora informacija je baziran na e mail servisu i kerakteriše ga: mogućnost razmjene informacija i iskustava između administratora, smanjuje se broj sajtova koje treba istražiti u rješavanju problema, moguće je doći brže do improvizovanih rješanja ukoliko patch još nije izdat. Sa druge strane, ogroman broj e-mailova treba obraditi, potencijalno je moguće i prisustvo zlonamjernog koda.

Svjetske i standardizovane baze podataka ranjivosti - Neprocjenjiv izvor informacija u vezi sa otkrivenim ranjivostima, koje imaju tendenciju da u jako kratkom roku izdaju informacije o otkrivenim slabostima. Pokrivaju ogroman broj sistema i prozvoda i nezavisne su od proizvođača softvera i obično su javno dostupne. Sadrže tipove informacija po CVE standardu.

Rješenja prilagodljiva potrebama korisnika - (mogući model opisan u sledećem poglavlju). Klasifikovane i odabrane informacije se dobijaju u realnom vremenu i ne troši se vrijeme na pretrage po drugim sajtovima i izvorima podataka. S druge strane takva rješenja mogu da koštaju i kvalitet rješenja je zavistan od baze informacija koju dostavlja korisnik.

B. *Generički model prilagodljivog rješenja za upravljanje sigurnosnim savjetima*

Generička šema veze VAM platforme data je na Sl. 1:

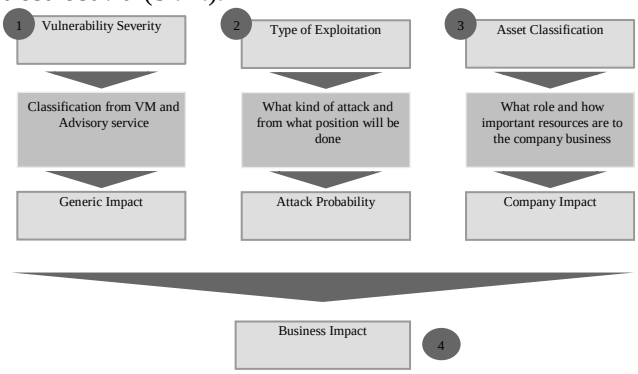


Sl. 1 Model VAM platforme

Glavni cilj – savjetodavna uloga u ovom modelu je da se u najkraćem roku, po tačno definisanom procesu, otkrivena ranjivost, u skladu sa modelom za prioritizaciju, dostavi tačno utvrđenim i odgovornim licima na izvršenje tj. ispravku ranjivosti. Praćenje i eventualna eskalacija u procesu rješavanja je sastavni dio platforme. Njegova najznačajnija uloga je da nadopuni standardni proces VM i pomogne u rješavanju slučajeva gdje je potrebna hitna reakcija, koja ne može da čeka izvršavanje rutina obuhvaćenih standardnim VM i PM procesom.

Metod utvrđivanja stepena prioriteta i posledično tome, načina i brzine ispravke sistema, bazira se na risk analizi. Model risk analize bi se generički mogao prikazati kao procesiranje određenih ulaznih parametara, kroz međusobne relacije, koje kao rezultat daju parametar koji definiše aktivnosti nad određenim sistemima.

Model risk analize uzima više glavnih ulaznih parametara, a kao izlaz se dobija težinski kvalifikovan parametar - poslovni uticaj, koji određuje vrstu i način aktivnosti koje treba obaviti (Sl. 2.).



Sl. 2. Ulazni parametri za dobijanje parametra poslovnog uticaja

Glavni ulazni parametri su:

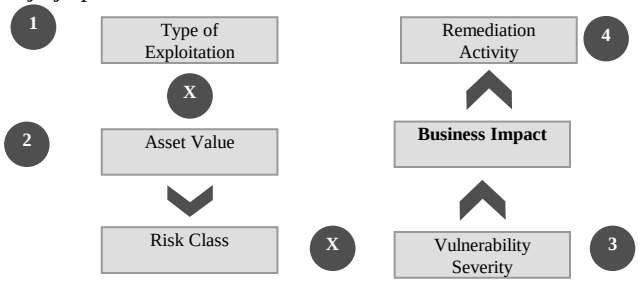
Ozbiljnost otkrivene ranjivosti, dobija se tokom procesa VM skeneranja. *Tip eksploatacije ranjivosti*, definiše se kao pozicija i način sa koje se ostvaruje eksploatacija ranjivosti. *Klasifikacija sistema* po važnosti za korporativni posao, definiše se kroz različite uloge i važnosti koje sistem ima za kompanijske potrebe

Ozbiljnost otkrivene ranjivosti je njihova klasifikacija po stepenu opasnosti koje predstavljaju za sistem. Obično sam VM skener ima predefinisane kategorije, kao što su: Critical, Serious, Moderate, Low.

Tipovi različitih napada se mogu podijeliti sa stanovišta da li se dešavaju sa eksternih pozicija (sa Interneta) ili sa internih pozicija (lokalna mreža). Podjela može biti i da li se napadi dešavaju kroz FW zaštitu, kroz određene protokole ili bez FW zaštite, direktnim pristupom. Težinski se kvalifikuju različite vrste napada.

Klasifikacija sistema je nešto što sama kompanija procjenjuje što vrijedi štititi i što ima najveću vrijednost za nju. Na primjer, poslovna vrijednost visokog prioriteta su sistemi koji su od vitalne važnosti za kompaniju (finansijski sistemi, sistemi koji su pod SOX kontrolom), mogu biti externo vidljivi sistemi – korporativni sajtovi itd. Srednjeg prioriteta bi bili sistemi interno vidljivi po određenim portovima, sa manjim poslovnim značajem – npr. interni web porta. Niskog prioriteta bi bili svi oni sistemi za koje se procjenjuje da ne mogu imati bitan uticaj na kompaniju.

Matrica za dobijanje konačnog parametra poslovnog uticaja je prikazana na Sl. 3.



Sl. 3. Proces dobijanja parametra poslovnog uticaja

Poslovni uticaj je determinanta u odnosu na koju se definišu potrebne aktivnosti u savjetodavnom i procesu ispravljanja sigurnosnih propusta, kao i praćenje njegove uspješnosti. Jedna od mogućih podjela je na sisteme sa: kritičnim, ozbiljnim, umjerenim, slabim uticajem.

Osnovna uloga VAM sistema je da djeluje proakivno tj. da obezbijedi potrebne i valjane informacije administratorima sistema o uočenim ranjivostima. Fokus je na ranjivostima koje imaju poslovni uticaj nivoa kritičnog.
Za tako dobijene slučajeve, propisuje se kritično (jako kratko) vrijeme oporavka, utvrđuju se kontakti za rješavanja problema, prate se sve aktivnosti na rješavanju, utvrđuje se metod eskalacije problema.
Za ostale slučajeve se definiše vrijeme oporavka u skladu sa opštim, standardizovanim procedurama i politikama koje se odnose na VM i PM.

Druga savjetodavna uloga ovakvih sistema je i u opštem obavještavanju svih zainteresovanih korisnika o otkrivenim ranjivostima i slabostima OS, baza podataka, aplikacija itd, kao metodom obrazovanja i podizanja nivoa znanja i svijesti o sigurnosnim propustima i rizicima. Svaki ovakav sistem može biti ili je kompanijsko specifičan, jer je baziran na znanjima i uslovima koje se traže u kompanijskom okruženju.
Implementacija VAM sistema je bazirana na jednom važnom ulaznom podatku – informacijama o uređajima koji postoje u kompaniji. Pravljenje precizne baze podataka svih uređaja/sistema od interesa čine najvažniji element u ovom sistemu. Informacije koje se sakupljaju o uređajima su raznorodne i svaka organizacija pravi svoj izbor u skladu sa svojim opštim potrebama [1]. Informacije mogu biti tipa: ime sistema, vlasnik sistema, sistem administrator, fizička lokacija, mrežni portovi, operacioni sistem i verzije sistema, softverski paketi i brojevi verzija, mrežni servisi, IP adresa, kategorija rizika, svrha sistema, potreba za usaglašavanjem sa određenim standardima itd.
Preciznost i validnost ovih podataka je osnov za kvalitetno funkcinisanje čitavog VAM sistema.

Postoje više modela po kojim se pravi baza resursa. *Ručno sakupljanje podataka*, lako za netehničko osoblje ali podložno greškama i nepodobno za veliki broj resursa. Korišćenjem raznih *programa/skripti* za automatsko sakupljanje podataka. Veliki broj korisnih informacija se može sakupiti i postiže se visok stepen automatizacije. Korišćenje *VM skenera* koji imaju razvijenu logiku za prepoznavanje većine potrebnih informacija i integracija dobijenih izvještaja sa bazom podataka. Kvalitet informacija zavistan od kvaliteta skenera, postoji mogućnost dobijanja false positive podataka
Bez obzira koliko programska rješenja bila dobra, neke informacije se ne mogu automatizovano dobiti, npr fizička lokacija ili kategorija rizika, što ukazuje da neophodnost djelovanja ljudskog faktora u ovom procesu.

C. *Primjena akcija na zaštiti sistema*

Jedna kvalitativna osobenost VAM sistema je da ima dobro razrađen mehanizam obavještavanja i praćenja aktivnosti na zaštiti sistema. Model obavještavanja se zasniva na hijerarhijskom grupnom modelu, sa podijeljenim operativnim i funkcionalnim cjelinama. Grupisanje IT resursa se može raditi po modelu [7], koji preporučuje da se u istoj grupi nalaze: sistemi koji se nalaze pod istom direktnom manadžerskom kontrolom, sistemi koji imaju isti funkcionalni cilj, sistemi koji imaju iste sigurnosne karakteristike i ciljeve, sistemi koji već postoje u istom uopštenom generalnom okruženju.
Integracija sa postojećim kompanijskim sistemima za praćenje rješavanja problema bi trebala biti moguća. Ovim se postiže da svaki zahtjev za rješavanje sigurnosnog propusta bude adekvatno ispraćen preko zvaničnih sistema kojim se može mjeriti efikasnost procesa ali i odgovornost pojedinaca zaduženih u tom procesu. Obavještavanje o kritičnim slučajevima mora biti sigurno tj enkriptovano.
Definišu se tri primarne metode zaštite koje se primjenjuju na sisteme koji su pod uticajem opasnosti [1]: primjena odgovarajućeg patch-a, primjena odgovarajućih konfiguracionih izmjena i uklanjanje samog SW ili servisa
Dodatno ovome, mogu se primijeniti i privremene mjere tipa: uticanje na konektivnost prema resursima i prihvatanje rizika – zahtjeva uključivanje viših vodećih struktura u kompaniji.

IV. Zaključak

Može se izvesti zaključak da je glavni cilj dobrog VM i VAM procesa da mjeri, upravlja i smanji sigurnosni rizik u korporativnom okruženju. Zreli VM model je onaj koji objedinjuje: široko primijenjene korporativne VM politike, integrisane sa korporacijskim sistemom za upravljanje rizika, sistemom za upravljanje procesima, sa jasno definisanom metrikom uspjeha, sa uspostavljenim proaktivnim procesom sistematskog skeniranja i praćenja novih ranjivosti koje se mogu naći u svjetskim priznatim bazama ranjivosti. Sinergija VM procesa sa javno dostupnim savjetodavnim servisima o ranjivostima je ključ uspjeha.

Zahvalnica

Ovom prilikom se zahvaljujemo Prof. Dr Christoph Strassburger-u na saradnji i korisnim savjetima.

Literatura

[1] Creating a Patch and Vulnerability Management Program, Special Publication 800-40 Version 2, NIST
[2] Planning and Deploying an Effective Vulnerability Management Program,By Jonathan Bitle, Technical Director, Qualys, Inc
[3] Guide to Effective Remediation of Network Vulnerabilities and Compliance, White Paper, Qualys
[4] Tim Proffitt, Creating a Comprehensive Vulnerability Assessment Program for Large Company Using QualysQuard, SANS Institute 2008
[5] Dynamic Best Practices of Vulnerability Management, Security Solutions & Services, by Eric Ogren, March 2004
[6] The Lows of Vulnerabilities, Black Hat 2009 Edition, Wolfgang Kandec, CTO, Qualys, July 28, 2009
[7] NIST Special Publication (SP) 800-18

Abstract

IS vulnerability management, together with advisory services related to vulnerabilities is important base in establishing overall security in IT systems. Complementary functions and synergy of these two processes contribute a lot in eliminating security risks toward company resources.

IS Vulnerability and Advisory Management

Slobodan Pavićević, Božo Krstajić