U OVOM POGLAVLJU

- Koje ranjivosti treba prvo obraditi
- Krpljenje sistema
- Sigurnost sagledana u novom svetlu

Poglavlje 18
Zatvaranje sigurnosnih rupa

Pošto ste završili testiranje, želite da krenete putem ka većoj sigurnosti. Ali, pronašli ste neke sigurnosne ranjivosti – stvari koje treba obraditi (nadam se, ipak, ne mnogo ozbiljnih!). Zapušavanje ovih sigurnosnih rupa pre nego što ih neko iskoristi će zahtevati nešto truda. Potrebno je da smislite plan igre i odlučite koje sigurnosne ranjivosti treba prvo obraditi. Nekoliko zakrpa može biti prikladno, verovatno i povećanje sigurnosti sistema. Možda će biti potrebno da kupite neke nove sigurnosne tehnologije i da ponovo procenite dizajn vaše mreže kao i sigurnosnu infrastrukturu. U ovom poglavlju ću se dotaći nekih od ovih kritičnih oblasti.

Pretvorite izveštaje u akciju

Može vam se učiniti da je prva ranjivost koju treba obraditi očigledna, ali ne mora da bude tako. Prilikom pregledanja ranjivosti koje ste pronašli, razmotrite sledeće promenljive:

- Koliko kritičan je dati ranjivi sistem
- Koje osetljive informacije ili poslovni procesi su ugroženi
- Da li ranjivost može biti uklonjena

- Koliko je lako ukloniti datu ranjivost
- Da li treba da isključite sistem da biste rešili problem
- Koliko vremena, novca i truda bi trebalo uložiti u kupovinu novog hardvera ili softvera ili u prepravku postojećih radnih procesa da bi se zapušile rupe

U poglavlju 17 obradio sam osnovne probleme prilikom donošenja odluke koliko je važan ili hitan određeni sigurnosni problem. Na sigurnost bi takođe trebalo da gledate iz perspektive upravljanja vremenom i da rešite probleme koji su ujedno i važni (od velikog uticaja) i hitni (imaju veliku verovatnoću). Verovatno ne želite da pokušate da rešite ranjivosti koje su *samo* od velikog uticaja ili koje *samo* imaju veliku verovatnoću. Možete imati neke ranjivosti od velikog uticaja koje verovatno nikada neće biti iskorišćene. Slično tome, verovatno ćete imati neke ranjivosti sa velikom verovatnoćom da budu iskorišćene a koje ne bi napravile veliku promenu u vašem poslu. Ovakav pristup vam pomaže da se izdvojite od načina testiranja koje izvodi većina i koji će vam obezbediti buduća angažovanja.

Usmerite se na zadatke koji se najviše isplate na početku – oni koji su od velikog uticaja *i* sa velikom verovatnoćom. Ovi zadaci će verovatno biti u manjini. Pošto zapušite najkritičnije sigurnosne rupe, možete se usredsrediti na manje važne, manje hitne zadatke kada vreme i novac to dozvole. Pošto zapušite takve kritične rupe kao što je SQL injektovanje u veb aplikacijama i zakrpe koje nedostaju na važnim serverima, možda ćete želeti da ponovo napravite sigurnosne kopije i zaštitite lozinkom (ako šifrovanje nije dovoljno jako) da biste se zaštitili od radoznalih očiju u slučaju da vaše sigurnosne kopije dospeju u pogrešne ruke.

Krpljenjem do savršenstva

Da li ikada osećate da je sve što radite krpljenje sistema da biste sredili sigurnosne ranjivosti? Ako je vaš odgovor potvrdan, blago vama; vi makar obavljate posao! Ako osećate pritisak da zakrpite sisteme na pravi način ali nemate vremena, makar je taj posao nešto što znate da vas čeka. Mnogi profesionalci u IT-u i njihovi menadžeri ne misle o krpljenju sistema sve dok se ne dogodi proboj u sistem. (Pogledajte istraživanje u Verizon Data Breach Investigations Report [`https://www.verizonenterprise.com/verizon-insights-lab/dbir/`], na primer.). Rad sa zakrpama je veliki problem u mnogim firmama. Ako čitate ovu knjigu vi ste očigledno zabrinuti za sigurnost i nadam se, daleko ste od neadekvatnog rada sa zakrpama.

UPAMTITE

Štagod da uradite, koju god alatku da izaberete, i koje god procedure funkcionišu najbolje u vašem okruženju, neka vaši sistemi budu zakrpljeni! Ovo pravilo važi za operativne sisteme; veb servere; baze podataka; mobilne aplikacije; i čak i za upravljački softver (engl. *firmware*) na mrežnoj barijeri: usmerivačima (engl. *rooters*) i skretnicama (engl. *switches*). Posebno važne su softverske zakrpe prodavaca kao što su Oracle (Java) i Adobe (Reader, Flash itd.) Ove zakrpe se češće previde nego većina, a ipak one donose značajan rizik koji ostaje nerešen.

Krpljenje se može izbeći ali je neophodno. Jedini način da se eliminiše potreba za krpljenjem jeste da se na prvom mestu razvije siguran softver, ali to se neće

skoro desiti, ako se ikada i desi. Softver je isuviše kompleksan da bi mogao da bude savršen. Veliki broj sigurnosnih incidenata se može sprečiti valjanim krpljenjem, tako da prosto nemate nikakav razlog da izbegavate rad sa zakrpama.

Upravljanje zakrpama

Ako ne možete da se izborite sa poplavom zakrpa za sisteme, ne očajavajte; još uvek možete da savladate problem. Ovo su moji osnovni principi za primenu zakrpa da bi sistem ostao siguran:

- Budite sigurni da svi ljudi i odeljenja uključeni u primenu zakrpa u sistemima vaše organizacije misle slično i prate slične procedure.
- Obezbedite zvanične procedure za ove procese od kritičke važnosti:
  - Obezbedite upozorenja o zakrpama od prodavaca, uključujući i zakrpe trećih strana
  - Procenite koje zakrpe utiču na sistem
  - Odlučite kada da primenite zakrpe
- Uvedite pravila i procedure za testiranje zakrpa *pre* nego što ih primenite na server za javni pristup. Testiranje zakrpa pošto ih primenite nije toliko važno u radnim stanicama, ali serveri su potpuno druga priča. Mnoge zakrpe imaju nedokumentovane karakteristike i prateće posledice, koje sam iskusio. Netestirana zakrpa je poziv za prekid rada sistema.

Automatizacija

Sledeći odeljci opisuju raznovrsne alatke za rad sa zakrpama.

Komercijalne alatke

Preporučujem otpornu aplikaciju za automatizaciju zakrpa, pogotovo ako su sledeći faktori uključeni:

- Velika mreža.
- Mreža sa više operativnih sistema (Windows, Linux, Mac OS itd.)
- Puno softverskih aplikacija od treće strane, kao što su Adobe i Java.
- Više od nekoliko desetina kompjutera.

SAVET

Obratite pažnju na ova rešenja za automatizaciju rada sa zakrpama

- :Ecora Patch Manager (`www.ecora.com/ecora/products/patchmanager.asp`)
- GFI LanGuard (`www.gfi.com/products-and-solutions/network-security- solutions/gfi-languard`)
- PDQ Deploy (`https://www.pdq.com/pdq-deploy`)

Besplatne alatke

Upotrebite jednu od ovih besplatnih alatki koje će vam pomoći u automatskom krpljenju:

- Windows Server Update Services (`https://technet.microsoft.com/en-us/library/cc539281.aspx` or System Center Configuration Manager (`https://www.microsoft.com/en-us/cloud-platform/system-center-configuration-manager`)).
- Windows Update, koji je ugrađen u Microsoft Windows operativni sistem
- Microsoft Baseline Security Analyzer (`https://www.microsoft.com/en-us/download/details.aspx?id=7558`).
- Ugrađene alatke za rad sa zakrpama za sisteme zasnovane na Linuxu (kao što su Yellowdog Updater, Modified i YaST Online Update).

Jačanje sistema

Pored primene zakrpa na vašim sistemima, budite sigurni da su vam sistemi obezbeđeni (zaključani) od ranjvosti koje zakrpe ne mogu da poprave. Otkrio sam da mnogi ljudi stanu kad obave proces sa zakrpama, misleći da su njihovi sistemi obezbeđeni, ali to nije tako. Tokom godina, viđao sam administratore mreže kako ignorišu preporuke takvih organizacija kao što su Nacionalni institut za standarde i Tehnološko-kompjuterski centar za sigurnosne resurse (`http://csrc.nist.gov/publications/PubsSPs.html)i` Centar za sigurnost na internetu (`www.cisecurity.org`), ostavljajući mnoge sigurnosne rupe širom otvorene. Ipak, verujem da ni sistemi za osnaživanje protiv zlonamernih napada nisu pouzdani. Zato što je svaki sistem drugačiji i potrebe svake organizacije su drugačije, nema rešenja koje odgovara svim situacijama, tako da morate da pronađete ravnotežu a da se previše ne oslanjate ni na jedno rešenje.

UPAMTITE

Pošto primenite zakrpe, dobra je ideja da ponovo proverite sisteme na ranjivosti da potvrdite da su se zakrpe primile.

Ova knjiga predstavlja kontramere za jačanje koje možete da primenite na mreži, kompjuterima, pa čak i fizičkim sistemima i ljudima. Pronašao sam da ove kontramere najbolje funkcionišu.

Primena makar osnovnih sigurnosnih postupaka je od kritične važnosti. Bilo da instalirate mrežni bedem ili zahtevate od korisnika da imaju jake lozinke putem Windows active direktorijuma domen GPO, morate obratiti pažnju na osnove ako želite da imate bilo kakav delić sigurnosti. Osim zakrpa, ako pratite kontramere koje sam zabeležio, dodajete druge dobro poznate sigurnosne postupke za mrežne sisteme (rutere, servere, radne stanice itd.) koji su slobodno dostupni na internetu i izvodite tekuće sigurnosne testove, možete biti uvereni da dajete sve od sebe da održite sigurnost organizacije.

PLAĆANJE GREŠAKA

Jednom sam bio uključen u projekat koji je bio odgovor na incident gde je bilo uključeno više od 10 000 Windows servera i radnih stanica zaraženih ciljanim zlonamernim programom. Još napredniji zlonamerni program je uzeo maha. Kompanija je zarazu pronašla brzo i mislili su da je IT tim sve očistio. Neko vreme je prošlo, a posle godinu i više u kompaniji su shvatili da nisu sve očistili. Taj zlonamerni program se osvetnički vratio, do te mere da je čitava njihova mreža bila pod nadzorom stranih, kriminalnih hakera, sponzorisanih od strane države.

Pošto je više od desetine ljudi provelo sate da dođu do korena problema, bilo je odlučeno da odeljenje IT-a nije uradilo ono što je trebalo da uradi što se tiče krpljenja i jačanja sistema. Takođe je došlo do ozbiljnog prekida u komunikaciji između odeljenja IT-a i drugih odeljenja, uključujući bezbednost, pomoć klijentima i radnih odeljenja. Ovaj slučaj gde je bilo „isuviše malo, isuviše kasno" uvukao je veliku kompaniju u veliku nevolju. Lekcija koja se može naučiti iz ovoga je da neadekvatno osigurani sistemi mogu da stvore ogromanu muku u poslu..

Procena sigurnosne infrastrukture

Pregled sigurnosne infrastrukture na sledeće načine može da obezbedi snagu vašim sistemima:

- **Pogledajte kako je sveukupna mreža dizajnirana.** Razmotrite organizacione stavke da li su sva pravila uspostavljena, da li se održavaju ili čak da li se ozbiljno prihvataju.. Odredite da li članovi uprave prihvataju informacionu sigurnost i usaglašavanje sa njom ili prosto odgurnu date mere kao nepotrebni trošak ili prepreku u poslovanju.
- **Mapirajte mrežu koristeći informacije koje dobijete iz sigurnosnih testova u ovoj knjizi.** Ažuriranje postojeće dokumentacije je od velike važnosti. Iscrtajte IP adrese, servise koji rade i sve drugo što možete da otkrijete. Nacrtajte dijagram mreže. Dizajn mreže i sigurnosne probleme je mnogo lakše proceniti kada radite sa njima vizuelno. Iako više volim da koristim tehnički program za crtanje kao što je Microsoft Visio ili Cheops (`http://cheops-ng.sourceforge.net`) da napravim mrežne dijagrame, takva alatka nije neophodna. Možete nacrtati svoju mapu na tabli.

  Ažurirajte dijagrame kada se mreža promeni ili jedanput godišnje i sl.

UPAMTITE

- **Razmišljajte o pristupu kako da smanjite ranjivosti i da povećate sveukupnu sigurnost organizacije .** Da li ste usmerili sav vaš napor na sporedne stvari a ne na složeni sigurnosni pristup? Mislite o tome kako su većina prodavnica i banaka zaštićene. Bezbednosne kamere su usmerene na kase, kompjutere blagajnika i okolinu - ne samo na parking i ulaze. Posmatrajte sigurnost iz perspektive odbrane koja zadire u dubinu. Primenite više slojeva bezbednosti tako da napadač mora da pređe preko drugih prepreka da bi izvršio uspešan napad.
- **Razmišljajte o sigurnosnim i poslovnim procesima na višem nivou vaše kompanije.** Zabeležite koji sigurnostni postupci i pravila postoje i da li se primenjuju. Odredite koji rizici postoje na način da sigurnost bude nadgledana i sprovedena. Nijedna organizacija nije imuna na praznine u ovoj oblasti. Posmatrajte ukupnu sigurnosnu kulturu u vašoj organizaciji da biste videli kako izgleda iz perspektive spoljašnjeg posmatrača. Posmatrajte je i kroz oko unutrašnjeg posmatrača. Otkrijte šta vaši klijenti ili poslovni partneri misle o tome kako se vaša organizacija odnosi prema osetljivim informacijama. Mogu reći, sa sto posto sigurnosti, da nešto – i to nekoliko stvari - može biti poboljšano vašem sistemu.

SAVET

Pružanje podrške sigurnosti nije samo pitanje zakrpa i drugih tehničkih sigurnosnih kontrola. Ponekad IT i program upravljanja sigurnošću treba poboljšati. Ponekad je potrebno da započnete nešto novo. Ponekad je prosto potrebno da prestanete da radite određene stvari. Tokom godina sam naširoko pisao o pogrešnom i pravilnom korišćenju IT-a i sigurnosnih programa i veći deo tog sadržaja možete naći na mojoj veb stranici `https://www.principlelogic.com/management.html`.

Sagledavanje vaše sigurnosti sa višeg nivoa i iz netehničke perspektive daje vam novi uvid u sigurnosne rupe i ukupne poslovne rizike. Taj proces zahteva vreme i trud, ali pošto ste utvrdili osnovnu liniju sigurnosti, upravljanje novim pretnjama i ranjivostima postaje mnogo lakše.