

10 Mitova sigurnosti

Kada govorimo o sigurnosti informacija danas, obavezno ćemo se susresti sa velikim brojem popularnih mudrosti, koje u većini slučajeva ne mogu baš da pomognu povećanju stepena sigurnosti, ali zato definitivno mogu da nas dodatno zbune ili odvedu u pogrešnom smeru. Jedini ispravan način da sigurnost u vašoj firmi dostigne viši nivo je da se vešto probijete kroz najezdu saveta, razdvajajući realnost od mitova. Predstavljamo vam 10 glavnih mitova koji vam mogu pomoći prilikom budućih planova u pogledu sigurnosti.

Mit prvi: Firme su danas mnogo sigurnije nego par godina ranije.

Većina firmi danas, je već preduzela određene korake u pravcu zaštite informacija. Ova vrsta zaštite se više ne smatra pukim troškom nego planiranom investicijom. U svakom slučaju, nove pretnje i tehnologije zaštite se svakodnevno menjaju i neminovno utiču na promene infrastrukture. Sistem administratori su primorani da kontinualno skeniraju svoje okruženje u potrazi za novim slabostima, da se svakodnevno usavršavaju i da periodično preispituju uvedene sigurnosne polise. Sigurnosne procedure i polise koje su uvedene godinu dana ranije možda ne odgovaraju tekućim potrebama firme.

Mit drugi: Prisustvo ili odsustvo propisa važni su u pogledu zaštite podataka.

Sa državnim regulativom ili bez nje, firme su dužne da štite svoje osetljive podatke. Greška npr. u proceduri zaštite podataka o klijentima, može dovesti do gubitka poverenja, što se posredno može odraziti na pad prometa, gubitak tržišta i druge loše konotacije. Nemojte biti u zabludi da postojanje državne regulative u ovoj oblasti automatski znači i da su osetljivi podaci sigurni!

Mit treći: Spoljni konsultanti znaju mnogo više o sigurnosti od osoba unutar firme.

Ljudi najčešće veruju da konsultanti poseduju specijalne alate i napredne tehnike koje nedostaju unutar njihove firme. Ipak, da li je baš tako!? Pre nego angažujete konsultanta, proverite sposobnosti vaših kolega. Neretko, većina sistem administratora, rešava probleme sigurnosti na dnevnoj bazi unutar svoje nadležnosti, i verovatno uz malu doobuku mogu postići mnogo više.

Razmotrite angažovanje konsultanta kao dopunu/obuku sopstvenog osoblja. Ako se ipak odlučite za potpuno angažovanje spoljnog konsultanta, onda proverite njegove kvalifikacije, stručnost i reference na tržištu i obavezno odredite jednu osobu iz lokalnog tima za komunikaciju sa konsultantima.

Mit četvrti: Briga o sigurnosti informacija zbog efikasnosti mora biti poseban sektor u firmi.

Možda smatrate da je formiranje jedinstvenog sektora za sigurnost dobra ideja. Smatrate da ovaj tip profesionalaca priča istim jezikom i da dele istu brigu. U svakom slučaju, ovakva grupa mora da pruža podršku svim sektorima u firmi i pre ili kasnije će doći do suprostavljanja stavova i ciljeva, a time i do loše poslovne klime.

Menadžment mora razumeti da problem sigurnosti informacija nije samo odgovornost IT osoblja, nego jedna od briga firme gde svaki sektor ponaosob mora da doprinese. Firme koje brinu o tome na pravi način uviđaju da sigurnost treba da evoluiru u sektor podrške, pre nego u posebno izdvojenu grupu.

Mit peti: Kompleksne i često promenjive lozinke će osigurati osetljive informacije.

Niko ne kaže da lozinke od 18 znakova mogu lako da se pogode. Ali, takođe teško se i pamte! Ako zahtevate od korisnika da menjaju svoje kompleksne lozinke svakih mesec dana, oni će neminovno početi da ih zapisuju, a to je upravo ono što ste hteli da izbegnete. Nasuprot tome, kreirajte fleksibilnu politiku formiranja lozinki koja će pomoći korisnicima da generišu jednostavnije i nekompromitovane lozinke, ali ih istovremeno obavezati da vode računa o sigurnosti istih. Lozinke zapisane na papirićima ili snimljene u Excel fajl su daleko veća pretnja od samog razbijanja lozinki.

Mit šesti: Ikonica u vidu "katanca" tokom SSL sesije u Web čitaču znači da su moji podaci bezbedni.

Ovo je netačno! Ova ikonica koja se može videti u donjem delu ekrana Web čitača, samo znači da su podaci u saobraćaju između vašeg uređaja i Web lokacije koju pregledate kriptovani – to ne znači da je i sama Web lokacija bezbedna. Ništa nije 100% sigurno, pa čak ni Web lokacije koje koriste 128-bit enkripciju.

Mit sedmi: Prelazak sa Internet Explorera na Mozilla Firefox će učiniti moju firmu sigurnom.

Ako je otkriven sigurnosni propust u operativnom sistemu ili aplikaciji, vaš računar je potencijalno ranjiv bez obzira koji Web čitač koristite. Pravi i najveći rizik leži u činjenici da korisnici i dalje nastavljaju da klikću mišem na zaražene priloge koji dolaze uz e-mail i tako se direktno kompromituju bez obzira koji Web čitač koriste.

Kako raste popularnost Web čitača Firefox, tako se povećava i broj otkrivenih propusta. Male firme i pojedinci ne bi trebali da imaju problema da pređu na ovaj softver, jer je to upravo ciljna grupa korisnika u ovom segmentu tržišta. Ipak, srednja i velika preduzeća, mogu naići na izvesne poteškoće. Prvo, tu je nedostatak upravljačkog sistema, što administratorima otežava kontrolu posećivanja određenim sadržajima na Internetu. Drugo, ako firma poseduje određen broj Web baziranih aplikacija koje su projektovane za Internet Explorer, migracija na Firefox može da dovede do dodatnih troškova za prilagođavanje tih aplikacija kao i troškove samog uvođenja Firefoxa. Nasuprot tome, restrikcija određenih Internet sadržaja kao i obuka u pogledu „pravilnog“ pregledavanja sadržaja može više doprineti sigurnosti od razmatranja prelaska na neki drugi Web čitač.

Mit osmi: Povećani troškovi za sigurnost rezultuju i većom sigurnošću.

Ovo je netačno. Firme često koriste neki vid metrike za pravdanje troškova u pogledu sigurnosti. Ovo može proizvesti samo dodatno trošenje sredstava, ali nikako i povećanje stepena sigurnosti. Svaka firma ima jedinstven profil rizika koji određuje investiciju u pogledu sigurnosti. Ne mogu se generalizovati potrebe za sigurnosnim mehanizmima. Potrebno je sagledati rizike, ako je moguće uklopiti ih u predviđeni budžet i izvršiti mudru nabavku koja će odgovarati ustanovljenom riziku. Ne zaboravite i edukaciju kao sastavni deo dobro utemeljene sigurnosti.

Mit deveti: Bežične mreže nisu sigurne.

U ranoj fazi ovaj vid umrežavanja je bio mnogo nesigurniji od klasičnog žičnog modela, mahom zahvaljujući WEP protokolu na kome je zasnovan i brojnim sigurnosnim propustima koje je imao. Danas, poštujući standarde za autentifikaciju i umrežavanje, napredne funkcije Wi-Fi opreme možete dobiti sigurnu bežičnu mrežu mnogo fleksibilniju nego što bi to bio sličan žični model.

Mit deseti: Prelazak sa Windows platforme na Linux će poboljšati sigurnost.

Adekvatnim planiranjem možete postići visok nivo sigurnost postavljajući i Windows i Linux platformu. Mada, broj pretnji za Windows je mnogo veći nego za Linux, ali ni Linux nije baš tako čist iako je podržan od ogromne programerske komune širom sveta koja brine o sigurnosti. Ipak, loše konfigurisan Linux server je isto tako ranjiv kao i bilo koji loše konfigurisani Windows server.

Pa onda da li odbaciti postojeću Windows platformu i preći na Linux? Za većinu preduzeća, odgovor je ne. Sve dok softver za Linux ne postane šire dostupan, firme će provoditi mnogo vremena u potrazi za raznim verzijama za Linux softvera koji im je potreban za posao. Posao koji se mora obaviti za prelazak na Linux (Testiranje poslovnih aplikacija u novom okruženju, ponovna obuka korisnika...) čini sam prelazak teškim i problematičnim po pitanju ekonomske isplativosti na duži period. Bolja alternativa tome je da se Linux implementira tamo gde se pokaže evidentno bolji u konkretnom poslovnom okruženju.

Autor: Velibor Simikić