Trendovi sigurnosti na Internetu (ili možda internetu?)

Početkom godine objavljuju se bilance i rekapitulacije zbivanja u protekloj godini, izvlače se zaključci koji bi nam trebali pomoći u predviđanju onoga što nas očekuje u narednom razdoblju. Takvi se pregledi objavljuju i na temu informacijske sigurnosti, a kompiliraju ih specijalizirane tvrtke koje se bave zaštitom.

No prije nego se posvetimo sigurnosti, osjećamo potrebu da se pozabavimo jednim jezičnim problemom: da li se piše Internet, ili internet? Za tehničare, pogotovo za mrežare, tu nema dileme: internet je svaka mreža koja povezuje odvojene mreže, a samo je jedan Internet, kojem je to ime, pa se onda piše velikim slovom. Veliko slovo označava da mislimo na globalnu informacijsku "autocestu", čije usluge svakim danom sve više koristimo, a ne na nekakvu privatnu među-mrežu kojom banke povezuju svoje poslovnice.

No jezikoslovci se ne slažu s nama. Oni smatraju da je internet naprosto infrastruktura, kao ceste, pruge, vodovod, pa se sukladno tome piše malim slovom. Oni i ne znaju da postoji mnogo interneta, a iskustvo iz razgovora s njima kaže mi da to ni ne žele znati... Dok im objašnjavam da postoje mnogi interneti, ali samo jedan Internet, oni gledaju kroz mene staklenim pogledom i zijevaju. Za njih je stvar jednostavna: Englezi i Amerikanci se razbacuju velikim početnim slovima, posebno u naslovima, pa smo mi naprosto nekritički preuzeli od njih tu "opciju".

Možda nam može priteći u pomoć zgodan primjer s našeg Jadrana. Dubrovnik je za mnoge samo još jedan grad, ali ne i za njegove stanovnike koji ga zovi Grad. Kad oni kažu Grad, to nije bilo kakva palanka, to je njihov jedan i jedini Grad. Kad sretnete gospara u Zagrebu i pitate ga otkuda je, reći će "Iz Grada".

Kad mene pitaju otkuda sam, ako sam dobre volje kažem da potičem s Interneta. Tu mogu naći većinu informacija koje mi trebaju, tu sam našao dragocjene i pametne ljude s kojima komuniciram. Jedini je problem preobilje, pa neprestano učim kako filtrirati nepotrebne, zastarjele informacije, poluistine i neistine. Ulogu zaštitnog uređaja obavlja moj preopterećeni frontalni korteks.

Radi svega toga u svojim tekstovima pišem Internet s velikim slovaom. S jedne strane zato da istaknem o kojem se internetu radi (o jednom jedinom globalnom međumrežju). S druge strane, veliko slovo stavljam i zbog poštovanja koje iskazujem Mreži koja je promijenila svijet, naše svjetonazore, način učenja, komuniciranja, a nastavlja nas mijenjati na načine koje još i ne možemo predvidjeti i u cijelosti sagledati.

Dakle što se može reći o stanju sigurnosti na Internetu u 2015-toj godini? U pomoć ćemo pozvati spomenuta godišnja izvješća. Možda su najpoznatija ona koje priprema tvrtka X-Force, koju je kupio IBM, ali ne zaostaju ni drugi, poput na primjer Symanteca, McAfee-ja, da ne nabrajamo dalje. Ako malo guglate, pronaći ćete ih s lakoćom. Zašto su nam ti izvještaji zanimljivi i zašto bi ih trebalo čitati? Očigledno je da su pisani s namjerom da nas uplaše i navedu na to da kupimo njihove zaštitne uređaje i prateće usluge. No ipak su ti izvještaji prava riznica znanja, jer se zasnivaju na faktografiji. Spomenute tvrtke prodaju uređaje koji obavljaju brojne zaštitne funkcije, postavljeni su na točkama gdje se privatne mreže spajaju s Internetom na brojnim lokacijama širom planeta. Svi oni šalju informacije u centralu, gdje se puni ogromna baza podataka.

Da citiramo početak jednog takvog izvješća: "Symantec je sastavio opsežan izvor podataka o prijetnjama na Internetu koje prikuplja SymantecTM Global Intelligence Network, koju sačinjava više

od 57.6 miliona sensora razmještenih u 157 država i koja bilježi tisuće događaja u svakoj sekundi." Slične rečenice naći ćete u uvodu svakog od takvih izvješća.

Dakle tu se prikupljaju podaci, obrađuju da postanu informacije i na kraju ih specijalisti pretvaraju u znanje. Znanje se ugrađuje u zaštitne uređaje, bez kojih se danas sve teže spajati na Internet. Tih uređaja ima različitih vrsta, neki su usko specijalizirani, kao na primjer *e-mail gateway*, koji se u DNS-u prijavljuje kao MS record, ali obavlja samo filtriranje poruka, tražeći viruse i spam, pa onda prosljeđuju sanitizirane poruke pravom mail serveru. Druga vrsta su IDS-ovi i IPS-ovi, uređaji koji prepoznaju napade i blokiraju ih. Neki od njih nude zanimljivu funkciju virtualnog *patchiranja* - svi znamo da nam aplikativci često ne daju da redovito stavljamo zakrpe na servere, jer postoji opasnost da aplikacije nakon toga neće raditi. Kako svi nemamo lab, gdje bi mogli na kloniranoj virtualki isprobati jesu li zakrpe bezazlene, dopuštamo da su nam serveri ranjivi. Virtualno patchiranje tu uskače u pomoć: IPS zna da je naš server ranjiv, pa umjesto njega odgovora na probe, šaljući odgovor koji bi poslao zakrpan server. Napadači tako misle da su nam serveri sigurni. Obrada logova i stvaranje korelacija među događajima još je jedna od dragocjenih funkcija koje nude zaštitni uređaji.

Dok neki proizvođači prodaju više takvih uređaja sa usko specijaliziranom funkcionalnošću, drugi nastoje u njih zapakirati što više zaštitnih funkcija. Nazivaju ih vatrozid nove generacije (NGF), UTM (Universal Threat Management), SIEM (Security Information and Event Management) itd. Tako jedno računalo obavlja ulogu klasičnog vatrozida (filtriranje prometa po portovima i protokolima), IDS-a (deep packet inspection, otkrivanje napada), IPS-a (to je IDS koji aktivno odgovara na napade), filtriranje web sadržaja (blokada siteova s opasnim ili nedoličnim sadržajima), nadzor prometa svih protokola, a ne samo e-maila, kako bi se zaustavio maliciozan promet koji ide na pr. preko FTP-a, IM, HTTP-a itd. Neki od takvih uređaja u stanju su analizom prometa ustanoviti koje su uobičajene aktivnosti u određeno doba dana, pa upozoravaju ako se događa nešto što odudara od prosjeka. Dakle na raspolaganju nam je cijeli arsenal zaštitnih funkcija koji nam može olakšati posao i učiniti boravak na Internetu sigurnijim. Kako iza takve tvrtke stoje timovi profesionalaca i ogromne baze znanja, oni su u stanju pratiti zbivanja i brzo reagirati na najnovije prijetnje.

Takav se uređaj može integrirati s Active Directoryjem, pa se na njemu mogu zadavati pravila prilagođena za određene grupe korisnika. Zaposlenicima možete braniti pristup Facebooku, ili dozvoliti čitanje, ali ne i slanje postova. Mogu obavljati i ulogu VPN-a, omogućavati spajanje izvana u privatnu mrežu ustanove uz autentikaciju korisnika. Ako ste paranoični i želite u potpunosti nadzirati što vaši korisnici rade na Internetu, oni mogu preuzeti hakersku ulogu "čovjeka u sredini" - klijentu se predstave kao server, serveru kao klijent, pa preuzmu razmjenu ključeva. Na način HTTPS promet na samom uređaju više nije kriptiran.

Jedini problem je u cijeni takvih uređaja i cijeni godišnjeg održavanja. Cijena je prilagođena poslovnim korisnicima, koji su je spremni platiti i mogu trošak ugraditi u cijenu svojih proizvoda/usluga. U Akademskoj zajednici uobičajeno je stanje kronične besparice, čak ni znanstvenici se ne mogu više tako lako pretplatiti na stručnu literaturu. Osim toga, smatra se da naše ustanove ne raspolažu vrijednim podacima, pa nema opravdanja za "nepotreban" trošak. U pogonu su serveri koji je davno trebalo rashodovati, a sposobni kolege se dovijaju na razne načine, stvaraju clustere od dotrajalih i novih servera, ne bi li preduhitrili kvarove i ispade.

Dakle sistemcima ne preostaje drugo nego nadati se da smo premala meta, da "neće udariti baš po nama", ili se dovijati u okviru mogućnosti koje su im na raspolaganju. Postoje besplatni alati, poput popularnog IDS-a snorta, od kojeg je nastao komercijalni proizvod. I dalje možemo koristiti besplatnu verziju, ako nas ne smeta što najnovije zaštite dobijamo sa zakašnjenjem. U komercijalnoj verziji plaća se ažurnost i brzina reakcije, a uz to dobijamo gotov, konfiguriran uređaj, po sistemu ključ u ruke.

Vratimo se našim godišnjim izvješćima. Možda sada još nisu dostupna ona koja obrađuju prošlu godinu, jer su još u izradi, ali isplati se čitati i ona za 2014. Sama količina informacija i bezbroj načina na koji smo ugroženi na Internetu dovoljna je da nas zabrine. Naravno, svrha te zabrinusti jest da nam olakša donošenje odluke za nabavu sigurnosnih uređaja. Bilo bi dobro da ih svi imamo, jer bi tada za našu sigurnost brinuli giganti informatičke industrije.

Nedavno su me kolege, sjećajući se moje uloge CISO-a, zamolilo da im pomognem oko *cryptolockera* kojeg su pokupili njihovi korisnici. Moram reći da ga moji korisnici nisu dobili - zahvaljujući jednom takvom uređaju koji nas štiti. Dakle, na popis novogodišnjih želja mogli bismo staviti nabavku jednog UTM-a, IDS-a, IPS-a, NGF-a, ili kako se već to zove, pa makar to bile puste sanje. Iskoristite priliku, ako dekan ili ravnatelj pokupi *cryptolockera* - tada je prilika da se na stol gurne već ranije pripremljena ponuda. :))

A što se predviđa za godinu koja je pred nama? Ukratko, očekuje se veći broj sofisticiranih napada na Appleove proizvode, jer raste njihova zastupljenost na tržištu. Očekuju se veliki sigurnosni problemi s uređajima koji spadaju u grupu *Internet of things* - sve je tu još novo, pa proizvođači nisu svjesni načina na koje se njihovi uređaji mogu zloupotrijebiti. Očekuje se da će se poraditi na regulativi i njenoj internacionalizaciji, kako se napadači ne bi skrivali iza lokalnog zakonodavstva koje ih (nepotrebno) štiti. Očekuje se da će se pooštriti odgovornost, pa i kazne, za organizacije koje su bile žrtve napada i krađe podataka svojih klijenata, kako bi ih se natjeralo da ulože u bolju zaštitu. Očekuje se da će se i dalje voditi rasprave na temu što je važnije, nacionalna sigurnost ili briga za privatnost pojedinca. Očekuju se daljnji poslovni gubici u komercijalnom sektoru radi hakerskih napada. Očekuju se napadi hakera koji rade za svoje vlade, u svrhu zaštite nacionalnih interesa. Očekuje se da će oni koji imaju potrebne resurse i dalje prikupljati naše informacije, obrađivati ih i zarađivati na prodaji anonimiziranih, obrađenih informacija, usprkoj regulativi koja im to brani. Očekuje se porast cijena otkrivenih ranjivosti nultog dana, za koje ne postoji obrana, jer se najsofisticiranji napadi obavljaju upravo pomoću njih.

Ukratko, očekuje se mnoštvo problema od kojih nas unaprijed boli glava. Što jedan običan sistemac može uraditi protiv tolikih nadmoćnih protivnika? Obrazovati se, primjenjivati alate koji su mu na raspolaganju i nadati se najboljemu? A što drugo...

sub, 2016-02-13 17:57 - Aco Dmitrović**Kategorije:** Kolumna [1]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1613

Links
[1] https://sysportal.carnet.hr/taxonomy/term/71