

INFORMACIJSKA VARNOST V 2009 IN KAJ PRINAŠA 2010

Milan Gabor

Inštitut za varnost podatkov in informacijskih sistemov, ViRIS d.o.o., Likozarjeva 12, 1000 Ljubljana
milan@viris.si

Povzetek

Leto 2009 je kljub vsem krizam minilo. Če gledamo tipe in pogostost napadov, na tem področju ni bilo opaziti nobene krize. Seveda se je kriza čutila predvsem v aktivnostih pri sledenju novim tehnologijam, saj se je precej aktivnosti na tem področju v začetku leta 2009 ustavilo. Večjo aktivnost je bilo mogoče opaziti šele proti koncu leta, saj so se takrat začele stvari tudi tukaj premikati.

V samem prispevku bomo izpostavili nekaj največjih groženj, ki jih je bilo mogoče opaziti na globalni ravni, pa tudi na lokalni ravni. Z nekaterimi smo se srečali sami, z drugimi smo bili seznanjeni preko različnih kanalov.

Izpostavili bomo tudi nekaj primerov, na katere smo naleteli pri naših varnostnih pregledih in raziskovalnem delu na področju informacijske varnosti.

V prispevku bomo pozornost posvetili tudi predvidevanjem za leto 2010 in nevarnostnim, ki se nam obetajo v tem letu. Pregledali bomo nekaj največjih pretenj, ki nam po besedah analitikov grozijo v letu 2010.

Abstract

INFORMATION SECURITY IN YEAR 2009 AND WHAT BRINGS YEAR 2010

The year 2009 has passed despite it was a year of crisis. If we take a closer look at the type and frequency of attacks we can see that in this area there was no crisis. Of course there was crisis in new activities and implementation of new technologies, because a lot of already planned activities stopped in the year 2009. Some activities were seen at the end of the year 2009 when the crisis was settling down a bit.

In our article we will show some biggest threats which could be seen on the global scene. We will also show that our country is not an isolated island. Some of the shown threats are from our own experience; some other cases were introduced in the public.

We will also show some cases, which we handled in our security audits and in our own researches in the fields of information security.

At the end we will also show what we can expect from the year 2010. We will take a look in some of the highest risk threats that analytics are predicting to hit us in this year.

Ključne besede

Informacijska varnost, splet, izguba podatkov, spletni napadi, analiza varnosti, statistika

Key words

Information security, web, data loss, web attacks, security analysis, statistics

1 INFORMACIJSKA VARNOST V 2009

Kljub besedi kriza, ki je v letu 2009 močno odzvanjala v marsikaterih krogih, te besede ni bilo mogoče opaziti na področju informacijske varnosti. Sezname novih napadov, novih ranljivosti tako v programski kot tudi strojni opremi niso bili leta 2009 nič krajši. Dejstvo je, da so se

nekatero investicije na področju informacijske varnosti zaustavile ali pa v nekaterih primerih prestavile na bolj ugodne finančne pogoje. Ta ustavitev se je lansko leto lepo videla na primer na portalu javnih naročil, kjer so se stvari začele dogajati šele v jesenskem času. Seveda pa takšno stanje ni bilo samo pri nas, ampak se je podobno dogajalo v večini držav. Kljub načrtom za zamenjavo rešitev so se nekateri odločili in so raje počakali pri zamenjavi tako strojne kot tudi programske opreme.

Seveda na drugi strani izvornost napadalcev in njihova kreativnost ne poneha. To se je pokazalo tudi na različnih konferencah, kjer so bile prikazane različne ranljivosti. Nekatero ranljivosti, obelodanjene v letu 2009, so bile prisotne v nekaterih kanalih že nekaj časa, kar so seveda določene skupine s pridom izkoriščale. Tako smo lahko videli, kako lahko enostavna kombinacija povzroči veliko težav pri SSL/TLS protokolu in prelisiči mnoge uporabnike. Seveda v letu 2009 ni manjkalo kritičnih popravkov, brez katerih bi naši operacijski sistemi postali lahek plen napadalcev.

Seveda je področje informacijske varnosti precej široko področje in bi bilo preobsežna tematika za ta članek, zato si bomo v nadaljevanju ogledali nekaj podatkov iz leta 2009 v tujini in pri nas, v drugem delu pa bomo poskušali pripraviti napoved za leto 2010.

1.1 Nevarnosti v tujini in pri nas

Pri analizi nevarnosti v letu 2009 lahko opazimo, da so napadi precej podobni, kot so bili prejšnja leta, in se področja napadov dosti ne spreminjajo. Se pa spreminjajo tipi napadov in ti postajajo vedno bolj ciljani in vedno bolj sofisticirani. Tehnologija, aplikacije in sistemi so postali danes precej bolj kompleksni in zato za uspešen napad na neko tarčo ni dovolj le kanček sreče in malo znanja, ampak je obratno. Veliko znanja in kanček sreče.

Če povzamemo, lahko najpogostejše nevarnosti najdemo na teh področjih:

- Web 2.0 in socialna omrežja
- Uhajanje podatkov
- Spletne nevarnosti
- SPAM in nevarnosti z uporabo elektronske pošte
- Nezaželena programska oprema
- Brežžična omrežja
- Mobilne naprave

Socialna omrežja so postala v zadnjih letih hit in kdor ni vsaj v kakšnem spletnem socialnem omrežju, ne šteje. Tako najdemo v socialnih omrežjih vse tipe ljudi od politikov, estradnikov, športnikov, pa vse do navadnih ljudi in celo zelo mlade populacije. Socialna omrežja so lahko seveda zelo koristna, a se je potrebno zavedati njihove nevarnosti. Uporabniki hitro podležejo skušnjavam, naložijo precej osebnih podatkov, slik in kaj hitro lahko dobri opazovalci izkoristijo te podatke in jih zlorabijo. Seveda pa najdemo na teh omrežjih tudi druge zanimive podatke, tako na primer lahko izvemo da so določeni ljudje pod DDOS napadom. Če jih povežemo z organizacijo, kjer so zaposleni, pa lahko takoj ugotovimo, na koga napad poteka.



Iščem Cisco strokovnjaka, ki se spozna na nastavljanje firewalla
Cisco ASA. Potrebno je obraniti DDOS napad
February 16 at 4:22pm · Comment · Like

Slika 1: Strokovno pomoč pri DDOS iščejo tudi na Facebooku

Blog

Stran nedosegljiva

Danes je bilo omrežje ... za par trenutkov nedosegljivo. Bili smo tarča DDoS napada. Seveda smo poskrbeli, da so bili vsi IP naslovi zabeleženi in posredovani naprej.

Slika 2: DDOS napad tudi na preproste strani

Seveda pa se te stvari iz socialnih omrežij ne dogajajo samo pri nas. To je na primer lani izkusil šef britanske obveščevalne službe MI6, ko je njegova žena na Facebooku objavila veliko podrobnosti iz družinskega življenja in celo osebne slike. Glede na funkcijo omenjene osebe seveda takšno pojavljanje v socialnih omrežjih ni primerno, česar bi se morala zavedati tudi njegova žena. Ni potrebno posebej omenjati, da je bila omenjena spletna stran hitro umaknjena. Kljub temu pa je ta dogodek doživel kar precej medijske pozornosti.

Tudi aktualna politika ni izvzeta iz poskusov napadov. Tako lahko recimo v letošnjem letu zasledimo obvestilo SI-CERTa, ki opozarja, da so se tudi pri socialnih omrežjih naših politikov začeli različni tipov napadov, ki vodijo obiskovalce na spletne strani z zlonamerno kodo. V primeru, da uporabnik obiše spletno stran, ga ta preusmeri na drugo stran z obvestilom, da nima nameščene zadnje verzije Flash programa in mu ponudi namestitev. V tej namestitvi seveda ni program Flash, ampak IRC bot, ki po namestitvi spremeni sistem v potencialnega napadalca BOT omrežja.



Slika 3: Napadi tudi na politične strani [1]

Kljub napredovanju tehnologij pa se žal ne moremo izogniti SPAMu, ki v letu 2009 ni tako zelo rasel kot leta prej. Najbrž ni kriva recesija, saj se je tehnologija, ki preprečuje širjenje nezaželene pošte, precej napredovala. Na tem področju je bilo mogoče opaziti manj napadov v primerjavi s prejšnjim letom. So pa bili ti napadi v večini primerov vezani na izkoriščanje pomanjkljivosti v različnih dokumentih (pdf, word ali excel) in ob odkritju takšnih pomanjkljivosti se število napadov v tistem času poveča.

Na področju spletnih aplikacij je bilo mogoče opaziti enako sliko kot leta prej. Kljub temu da je bilo mnogo naporov vloženih v smeri ozaveščanja in priprave različnih slovenskih distribucij, ki omogočajo hitre vzpostavitev CMS sistemov, je mogoče opaziti, da je pri nas še vedno precejšnje število razobličenen strani. Na seznamu, ki je na voljo na eni izmed spletnih strani, napadalci tekmujejo v zbiranju točk s tem, kdo bo opravil največ razobličenenj. Za strani, ki so še posebej pomembne, lahko dobi napadalec še posebno čast, ki jo označijo z zvezdico. Na naslednji sliki lahko vidimo nekaj takšnih zadnjih razobličenenj spletnih strani.

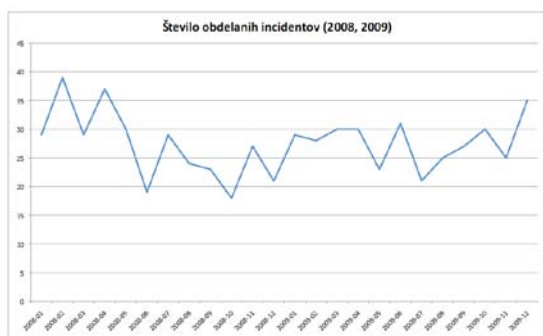
KHG	M	suzuki.panjan.si/sl/predstavit...	FreeBSD
KHG	M	★ www.rks.si/docs/	FreeBSD
KHG	M	www.isuzu.si/ff/	FreeBSD
KHG	M	linuxdan.si/docs/index.htm	FreeBSD
KHG	M	www.antivirus.si/docs/	FreeBSD
1923Turk		tvojportal.si/jomtube/sploni-p...	Unknown
1923Turk	M R	www.simbioza.si/index/index.ph...	Linux
funky_still	H M	rozica.si	Linux
funky_still	H M	studio2010.si	Linux
KHG	M	www.softnet.si/ff/index.htm	FreeBSD
KHG	M	www.ro.softnet.si/ff/index.htm	FreeBSD
KHG	M	www.cn.softnet.si/ff/index.htm	FreeBSD
KHG	M	www.rcl.si/ff/docs/index.htm	FreeBSD
KHG	M	★ bayerschering.bayer.si/docs/	FreeBSD
khg	M	★ www.bayer-pharma.si/docs/	FreeBSD
KHG	M	★ www.healthcare.bayer.si/docs/	FreeBSD
Z7FaaN H4Ck3R		dat.si/publikacije	Linux
KHG	M	★ www.bayer.si/docs/	FreeBSD
KHG	M	★ www.thenorthface-slovenija.si/ff/	FreeBSD
KHG		★ www.suzuki.si/sl/predstavitev_...	FreeBSD
KHG	M R	★ www.suzuki-odar.si/sl/avtomobi...	FreeBSD
funky_still	H M	kmetijatavcar.si	Linux

Slika 4: Seznam zadnjih razobličenenj spletnih strani pri nas

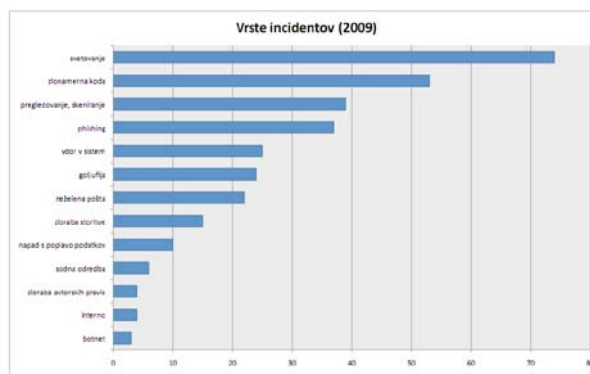
1.2 SI-CERT

SI-CERT je Slovenski center za posredovanje pri omrežnih incidentih, ki deluje v okviru javnega zavoda Arnes. SI-CERT deluje že od leta 1995 in med drugim sprejema prijave zlorab na internetu ter prejme letno okrog 1700 prijav. Po njihovih besedah reševanje teh primerov na nacionalni ravni že nekaj let poteka usklajeno. Težave se pojavijo, ko zaradi narave Interneta pride do napadov preko mednarodnega omrežja, saj so te preiskave po navadi težavne. V večini zlorab ki jih dobijo, pa je vpletenih več kriminalnih skupin iz različnih držav.

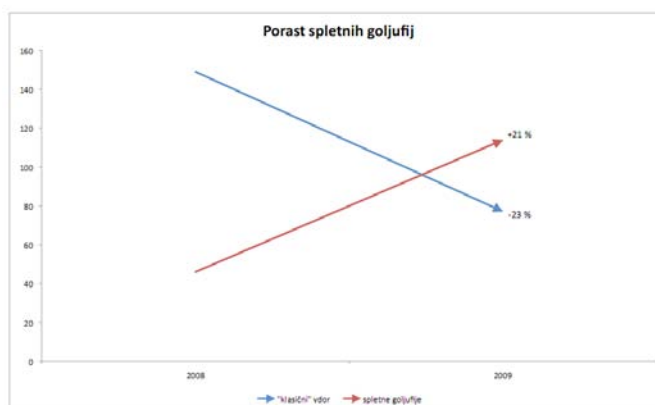
Če pogledamo statistiko SI-CERTa v številu obdelanih incidentov v letu 2008 in 2009, lahko opazimo, da je v povprečju število primerov konstantno in se veliko ne spreminja. Če analiziramo vrsto incidentov, vidimo, da prevladuje predvsem zlonamerna koda in phishing. Sledijo še vdori v sistem, goljufije in zloraba storitev. V nadaljevanju lahko opazimo še, da se število klasičnih incidentov vdora v sistem zmanjšuje, zvišuje pa se trend porasta spletnih goljufij.



Slika 5: Število obdelanih incidentov [3]



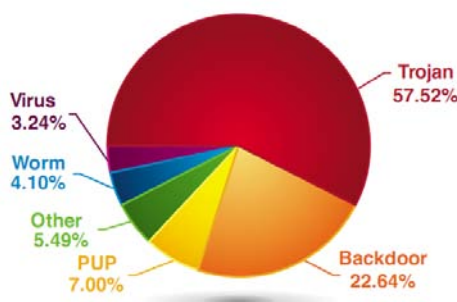
Slika 6: Vrste incidentov [3]



Slika 7: Trend porasta spletnih goljufij [3]

Pri vseh teh statistikah se moramo zavedati tudi dejstva, da veliko število varnostnih incidentov ne pride v statistike. Razlogov za to je več. Primarni razlog je seveda ta, da nihče noče na veliki zvon obešati informacij o tem, da so bili tarča napada na informacijski sistem in da so lahko potencialno izgubili kakšne podatke. Zato točne statistike s tega področja ni ali pa je precej pomanjkljiva.

Glede na to, da tudi pri nas pri incidentih prednjači zlonamerna koda, je zanimivo videti, kakšni tipi zlonamerne kode prevladujejo na svetovni ravni. Pri rezultatih presenetljivo vodijo različni trojanci in pa koda, ki namesti skrivna vrata za dostop do sistema. Ti dve kategoriji dejansko obsegata večino zlonamerne kode. Presenetljivo malo je klasičnih virusov, kar kaže, da so virusi nekako stvar preteklosti.



Slika 8: Zlonamerna koda [2]

1.3 Pravno področje informacijske varnosti

Seveda so se stvari dogajale v letu 2009 tudi na področju prava, saj smo konec leta dočakali popravke Kazenskega zakonika, kjer so se malo spremenile definicije vstopa ali vdora v informacijski sistem. Stari kazenski zakonik je tako navajal neupravičeni vstop v informacijski sistem, v popravku pa se govori o vdoru v sistem. Načeloma razlika ni velika, a je vsekakor ne smemo zanemariti. In o tem že teče debata, ki bo pokazala, ali je bila sprememba res potrebna in predvsem, ali je bila sprememba pravilna. Najbrž bo prave posledice pokazala šele pravna praksa.

1.4 Naše izkušnje

V letu 2009 smo tako kot prejšnja leta največkrat naleteli na pomanjkljivosti pri spletnih aplikacijah. Opažamo, da se sicer stanje na tem področju izboljšuje, ampak počasi. Med drugim smo tudi imeli opravka s strežniki, ki so bili tarča napadov. Te strežnike so napadalci potem uporabljali kot IRC strežnika in phishing strežnike ali celo v DDOS napadih.

Opazili smo tudi, da je vedno več podatkov shranjenih na različnih spletnih strežnikih, do katerih imajo potem vsi dostop. Tako se lahko najdejo med temi tudi kakšni poslovni načrti, pogodbe in drugi zanimivi podatki. Tukaj je predvsem premalo pozornosti tistih, ki objavljajo te podatke na različnih strežnikih, brez da bi se zavedali, da jim lahko takšne objave škodijo.

Pri interni raziskavi smo recimo tudi preverili, koliko DNS strežnikov še vedno omogoča prenos con in bili presenečeni nad rezultatom. Po naših analizah to omogoča okrog 25 % izmed 500 domen največjih slovenskih podjetij. Pri podobni raziskavi smo raziskovali tudi, kaj shranijo iskalniki v svoje podatkovne baze in v kakšnih kotičkih Interneta je mogoče najti naše podatke. Kot primer smo navedli Google, ki je v svoji bazi shranil tudi nekatere internetne strani ene izmed slovenskih bank.

2 KAJ PRINAŠA 2010

Različni viri napovedujejo za leto 2010 povečan obseg napadov na socialna omrežja, bančna omrežja, kot tudi ciljane napade na uporabnike, podjetja in aplikacije. Pri teh napadih ne gre pozabiti tudi na povečane napade iz Botnet omrežij. Napoveduje se tudi povečana aktivnost s strani zakonskih regulatorjev, ki bodo aktivno stopili v napad proti cyber kriminalu.

2.1 Nevarnosti socialnih omrežij

Socialna omrežja, kot na primer Facebook, se bodo soočala z vedno bolj naprednimi nevarnostmi, saj število uporabnikov nenehno raste in s tem tudi raste število potencialnih tarč.

Eksplozija aplikacij na socialnem omrežju Facebook in drugih podobnih omrežjih bo pomenila idealno podlago za cyber kriminalce, ki bodo izkoristili zaupljivost prijateljev v socialnih omrežjih in bodo lahko prepričali uporabnike, da bodo kliknili na povezave, ki jih drugače ne bi kliknili in tako bodo lahko posledično tisti manj previdni namestili nezaželeno ali celo zlonamerno kodo.

2.2 Napadi na razširjene produkte

Cyber kriminalci že nekaj časa izbirajo za napade produkte podjetja Microsoft zaradi njihove popularnosti. Tako smo že videli, da so ti napadi na različne tipe dokumentov stalnica. V

2010 smo že bili priča takšnemu tipu napada z izkoriščanjem Microsoft Help pomoči. V 2010 lahko pričakujemo, da se bodo na prvo mesto povzpeli Adobe produkti, še posebej Acrobat Reader in Flash tehnologija, in prevzeli primat Microsoftu.

2.3 Bančni trojanci in BOT omrežja

Bančni trojanci bodo postali še bolj zahtevni in sofisticirani, saj bodo omogočali tudi prekinitev legalnih transakcij in bodo omogočali nepooblašene transakcije brez vednosti uporabnika. Trenutno je na črnem trgu že možno kupiti precej sofisticirane programe, ki omogočajo lastno prireditev določenih parametrov programa in je z njimi mogoče izvajati krajo pri bančnih transakcijah.

Botnet omrežja pomenijo že v tem trenutku vodilno infrastrukturo za cyber kriminalce, ki izkoriščajo ta omrežja za različne tipe napadov od pošiljanja nezaželene pošte, kraje identitete pa do DOS napadov. Ta omrežja bodo s kombinacijo nevarnosti za socialne omrežja pomenila v letu 2010 veliko nevarnost.

2.4 Nevarnosti v oblaku

Glede na velike napovedi selitve storitev in programske opreme v oblake bo o varnosti v oblaku v letu 2010 veliko govora. Sama tehnologija veliko obeta, a se ob njej poraja veliko neznank tudi na področju varnosti. Poleg varnosti same pa bodo še aktualna vprašanja o lokalnih pristojnostih glede varnosti podatkov, saj so lahko storitve in podatki v oblaku porazdeljeni po različnih državah, kjer veljajo različni zakoni s tega področja. Bo pa potreben dober premislek glede varnosti v oblakih.

3 VIRI IN LITERATURA

- [1] SI-CERT obvestilo, <http://www.cert.si/obvestila/obvestilo/article/politika-je-lahko-tudi-nevarna/35.html>.
- [2] IBM Internet Security Systems X-Force Threat Insight Quarterly, Oktober 2009,
- [3] SI-CERT, poslano slikovno gradivo.