arnes

POROČILO O OMREŽNI VARNOSTI ZA LETO 2011

NEVARNOST JE ODVISNA OD NAŠE VARNOSTI

si·cert

VARNI NA INTERNETU

si·cert

SI-CERT (Slovenian Computer Emergency Response Team) je nacionalni center za obravnavo omrežnih incidentov. Na elektronski naslov cert@cert.si ali preko telefona (01) 479 88 22 lahko prijavite vdor v računalnik ali poskus druge zlorabe prek omrežja.

Na podlagi Sklepa Vlade Republike Slovenije št. 38600-3/2009/21 z dne 8.4.2010 SI-CERT opravlja naloge centra za obravnavo incidentov v sistemih državne in javne uprave.

www.cert.si

Facebook: facebook.com/sicert

Twitter: twitter.com/sicert

si·cert

POROČILO CENTRA SI-CERT


WE ARE
ANONYMOUS
UNITED AS ONE / DIVIDED BY ZERO
WE STAND FOR GLOBAL FREEDOM
LEARN MORE AT
WWW.WHATIS-THEPLAN.ORG
PHASE_ONE: INITIATED
FUCK
THE
GOVERNMENT

Na spletu nikoli nisi sam

S stališča medijske pozornosti je bilo leto 2011 v znamenju hekerske skupine Anonimnih (Anonymous). Ti so z odmevnimi vdori v velika podjetja pokazali, da tudi ta velikokrat zatajijo na prav majhnih in enostavnih napakah ter postanejo lahka tarča z malo truda. Na drugi strani napredni napadi APT (Advanced Persistent Threat) delujejo pritajeno in potekajo tudi več mesecev, preden jih žrtev odkrije. Vdiralčevi programi na zlorabljenih sistemih čez dan spijo, ponoči pa počasi pretakajo podatke na tuje strežnike. Pred njimi ni bil imun niti Google, še bolj pa dajeta misliti vdora v Lockheed-Martin, ki proizvaja napredne sisteme za ameriško vojsko.

Vdori v omrežja overiteljev digitalnih potrdil (CA, Certification Authority) Comodo in DigiNotar ter ponudnika identifikacijskih naprav RSA so zamajali zaupanje v sam sistem zagotavljanja digitalne identitete in porajajo vprašanja o ustreznosti komercialno zasnovanega modela overiteljev in infrastrukture javnih ključev (PKI). Nobenega dvoma ni več, da za nekaterimi napadi stojijo varnostne ali vojaške službe nekaterih držav.

Doma smo največ časa posvečali vdorom v strežnike manjših podjetij in s tem povezano analizo podtaknjene programske kode. Neustrezno vzdrževanje za seboj vedno pusti varnostne luknje, ki napadalcem iz vsega sveta omogočajo podtikanje lažnih (phishing) strani in »drive-by download« napade, ki okužijo spletne obiskovalce. V sklopu SI-CERT smo za potrebe ozaveščanja javnosti pred podobnimi nevarnostmi v preteklem letu uspešno aktivirali projekt Varni na internetu.

Dobili smo tudi prva opozorila o izpostavljenosti sistemov za nadzor industrijskih procesov. Ob neustrezni zaščiti bi lahko bil prek njih možen vdor v posamezen gradnik v kritični infrastrukturi. Sistemi SCADA (Supervisory Control And Data Acquisition) postajajo most med virtualnim in fizičnim svetom, vdor vanje pa ima lahko resne in otipljive posledice v naših življenjih.

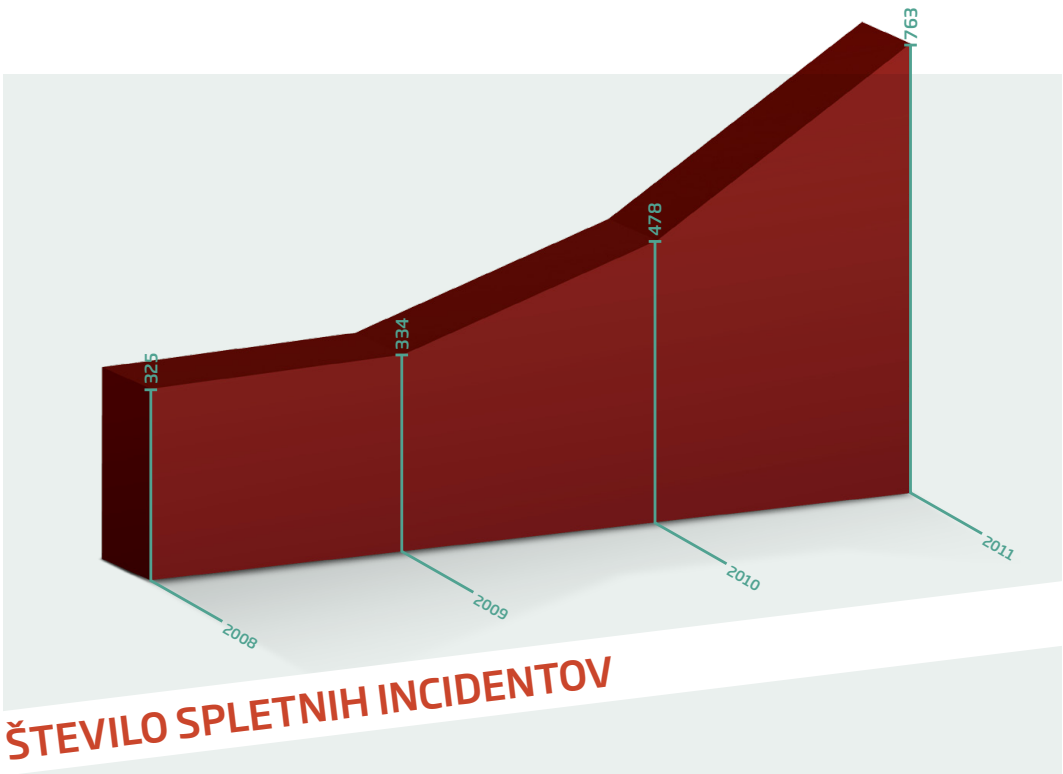
Leto se je končalo z objavo ukradenih posnetkov zaprtih sej Vlade RS na spletnem portalu Youtube. Ta incident je pokazal, da nas čaka še veliko dela pri zagotavljanju varnosti informacijskih virov, kot tudi pri koordinaciji odzivanja na omrežne incidente v državni informacijski infrastrukturi.

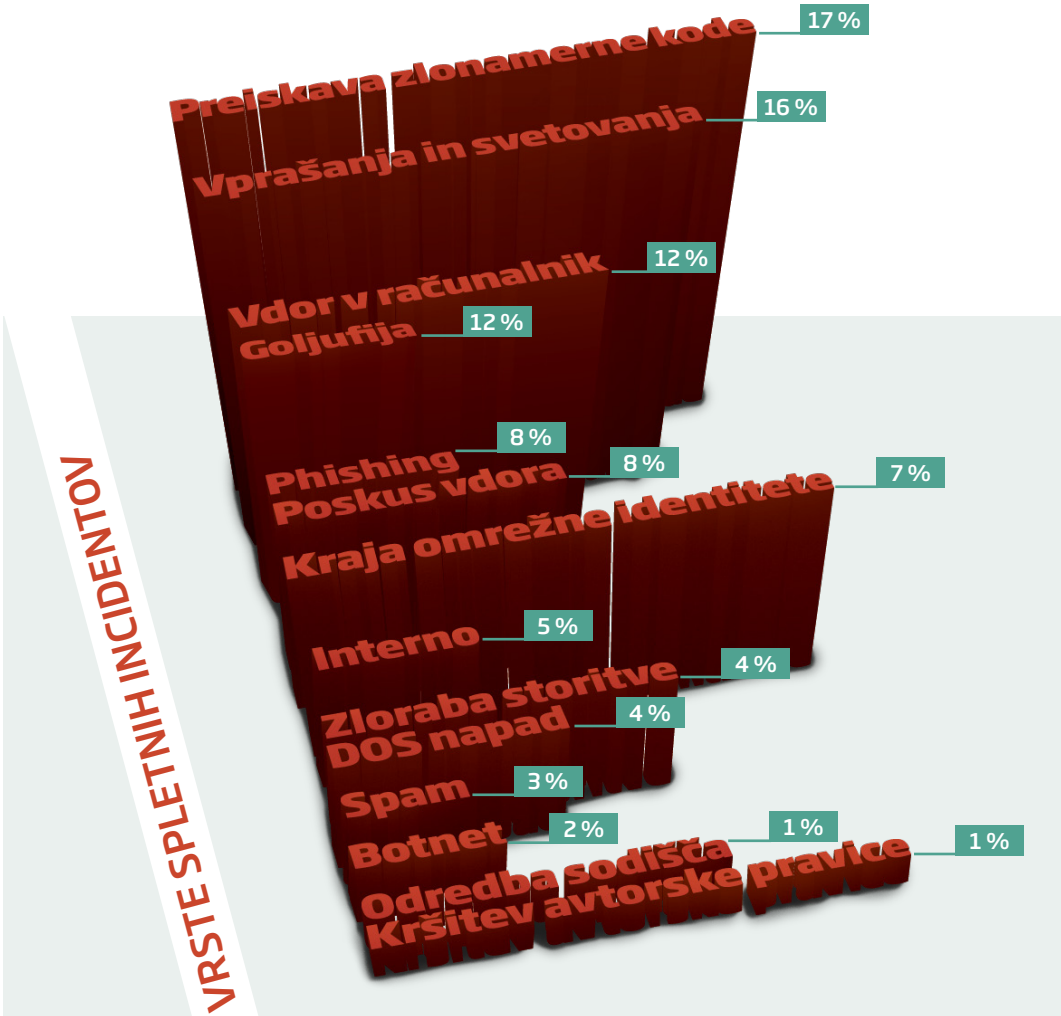
Gorazd Božič, *vodja SI-CERT*

Statistika spletnih incidentov

Preglejmo letne statistične podatke in zanimive izsledke. SI-CERT sprejema prijave vdorov ali poskusov vdorov v računalniške sisteme, prijave napadov z motenjem storitve (denial of service ali DOS napad), prijave podtikanja virusov ali trojanskih konjev in prijave drugih zlorab ali spletnih goljufij.

Število prijav vdorov v sisteme in z njimi povezanih incidentov se je v primerjavi z letom 2010 povečalo za 62 % (s 197 na 320). V to kategorijo zlorab štejemo phishing spletne strani in podtaknjeno zlonamerno kodo na strežnikih. Posebej relevanten je podatek, da je **število goljufij in kraj identitete je poraslo kar za 92 %** (s 136 na 261). Med njimi je **največ nigerijskih prevar**, svoje žrtve pa goljufi iščejo tudi na slovenskih spletnih forumih in v oglasnikih.




VRSTE SPLETNIH INCIDENTOV
Preiskava zlonamerne kode
17 %
Vprašanja in svetovanja
16 %
Vdor v računalnik
12 %
Goljufija
12 %
Phishing
8 %
Poskus vdora
8 %
Kraja omrežne identitete
7 %
Interno
5 %
Zloraba storitve
4 %
DOS napad
4 %
Spam
3 %
Botnet
2 %
Odredba sodišča
1 %
Kršitev avtorske pravice
1 %

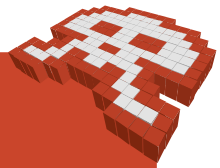
Vrste in primeri spletni incidentov

Vdori v strežnike

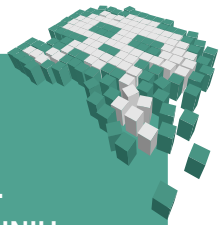
Zloraba lahkih tarč na internetu je v preteklem letu predstavljala količinsko najbolj pomemben del dejavnosti. Manjša podjetja velikokrat nimajo urejenega ustreznega vzdrževanja svojih spletnih strežnikov in sistemov za upravljanje vsebin (CMS). Začudenje skrbnikov ali odgovornih oseb ob vdoru v sistem kaže na še vedno prisotno napačno razumevanje motivov napadalcev. Ti ne izbirajo tarč glede na njihovo vnaprej ocenjeno vrednost, temveč izberejo tarče, ki so v tistem trenutku na voljo.

CMS
Content Management System. Med najbolj priljubljenimi: Joomla in Wordpress

Hekerski skupini Anonimni in LulzSec sta uporabili takorekoč banalne metode za vdor v prestižne tarče, kot sta Sony in HB Gary, ter sicer enostavna in ponavljajoča se gesla in vrivanje SQL stavkov. Analiza razkritih gesel strank zasebnega obveščevalnega podjetja Stratfor je v samo petih urah zlomila 82.000 gesel (od skupaj 860.000).



NEPOOBLAŠČEN VSTOP V SISTEM PREK NEZAŠČITENE STORITVE WINDOWS REMOTE DESKTOP IN ŠIBKEGA GESLA OMOGOČI NAPADALCU, DA NA SPLETNE STRANI PODTAKNE ELEMENTE, KI POSKUSIJO OKUŽITI OBISKOVALCE SPLETNEGA MESTA PODJETJA. VSAK OKUŽEN RAČUNALNIK OBISKOVALCA SE JAVI NADZORNEMU SISTEMU, KI NAPADALCU OMOGOČA KRAJO GESEL IN DOKUMENTOV.



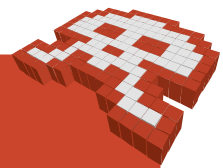
VARNOSTNI UKREPI:

- **OMEJEVANJE DOSTOPA DO STREŽNIKOV PODJETJA.**
- **GOSTOVANJE IN VZDRŽEVANJE PRI SLOVENSKEM PONUDNIKU.**
- **OZAVEŠČANJE IN IZOBRAŽEVANJE MALIH PODJETIJ IN SAMOSTOJNIH PODJETNIKOV S PROGRAMOM VARNI NA INTERNETU.**
- **ANALIZA PODTAKNJENE SPLETNE KODE IN OBVEŠČANJE TUJIH CERT CENTROV. SVETOVANJE PODJETJU PRI VDORU IN ODPRAVA POSLEDIC.**

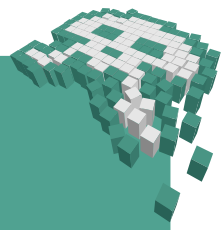
Nadzor industrijskih procesov in naprav

Sistemi za nadzor industrijskih procesov SCADA omogočajo pregled, nadzor in upravljanje proizvodnih linij, elektrarn, plinovodov, železniškega omrežja in še marsikaj. Če je bila zanesljivost in robustnost delovanja teh sistemov od nekdaj v jedru razvoja nadzorne programske opreme, pa z varnostjo le ni vedno tako. Ker so bila omrežja za nadzor procesov v industriji v začetku lokacijsko omejena in ločena, se je že ta izolacija sama smatrala za zadostno zaščito.

Ponavadi se izkaže, da se je zloraba celotne organizacije začela z majhno varnostno napako spletne aplikacije, ki je nihče ni jemal resno.



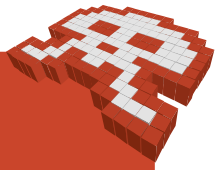
OBRAVNAVALI SMO IZPOSTAVLJENOST VEČJEGA ŠTEVILA TOPLOTNIH POSTAJ, KI JIH JE MOGOČE NADZIRATI PREK INTERNETA. ODPRTI SPLETNI VMESNIKI S ŠIBKIMI GESLI IN Z NEŠIFRIRANIM PRENOSOM PODATKOV PO NEPOTREBNEM IZPOSTAVLJAJO NADZORNI MEHANIZEM CELOTNEMU INTERNETU. VDIRALCI LAHKO POVZROČIJO MOTNJE ALI PREKINITEV OGREVALNIH CIKLOV V DOMOVIH IN USTANOVAH, KOT SO, DENIMO, ŠOLE ALI BOLNIŠNICE.



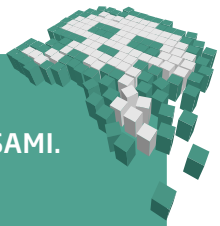
VARNOSTNI UKREPI:

- **NEPOSREDEN KONTAKT Z ZASTOPNIKI IN S PRODAJALCI.**
- **DOSEGANJE BOLJŠE ZAŠČITE ŽE OB PRVI NAMESTITVI.**
- **STIK Z UPRAVLJAVCI TOPLOTNIH POSTAJ IN NAVODILA ZA NJIHOVO ZAŠČITO.**

Primer črva Stuxnet iz leta 2010 kaže, da prepletenost informacijskih sistemov pušča odprta vrata, ki jih ne moremo več zapreti. Počasno širjenje Stuxneta zgolj prek izmenljivih USB ključev do iranske jedrske elektrarne je na koncu kljub vsemu zadelo svoj cilj in okvarilo centrifuge za bogatenje urana.



ENA IZMED SLOVENSKIH ELEKTRARN JE SISTEMSKO OMOGOČALA PRIJAVO PREK SPLETNEGA VMESNIKA. PROGRAMSKA KODA, KI JE BILA JAVNO DOSTOPNA, JE RAZKRIVALA STRANSKA VRATA (POSEBNO UPORABNIŠKO IME IN GESLO V BERLJIVI OBLIKI).



VARNOSTNI UKREPI:

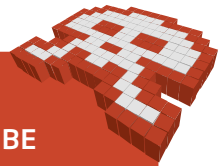
- **SEZNANITEV VODSTVA ELEKTRARNE Z NEPRIMERNIMI PRAKSAMI.**
- **OMEJITEV DOSTOPA DO VMESNIKA.**
- **PREDLAGANA NEODVISNA VARNOSTNA OCENA RAZVITE PROGRAMSKE OPREME IN REŠITVE.**

Napredne in ciljane grožnje

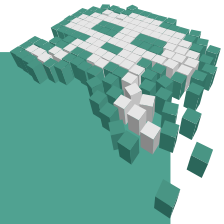
Za hekerske napade navadno pravimo, da so oportunistični in da izrabljajo cilje z jasno vidnimi ranljivostmi, ki jih lahko izrabijo. Leto 2011 je prineslo določeno spremembo v vedenju kršiteljev, ki se usmerjajo v vedno bolj napredne napade na vnaprej določene tarče. Napadi so ponavadi vnaprej načrtovani, nameni vdora pa opredeljeni v razponu od objestnosti do vedno bolj pogoste kraje podatkov iz informacijskih sistemov. Napadalci spretno pazijo, da se izognejo zaznavi in tako »letijo pod radarjem«.

Najbolj splošen vektor napada je napad preko elektronske pošte z uporabo socialnega inženiringa, ki deluje na temelju preiskovanja dostopnih podatkov o žrtvah. S preiskovanjem podatkov o strukturi zaposlenih lahko napadalec sestavi elektronsko sporočilo, ki daje vtis, da prihaja iz verodostojnega vira in ponuja informacije, ki se nanašajo na aktualne dogodke.

Ciljani napadi vsebujejo po meri izdelane viruse in trojanske konje, ki jih protivirusni programi še ne poznajo, zato zanašanje le na te v tem primeru ni učinkovito.



SPOROČILO, KI NA PRVI POGLED PRIHAJA IZ SLUŽBE EVROPSKE KOMISIJE ALI ENE IZMED EVROPSKIH AGENCIJ, SPOROČA SPREMEMBE DNEVNEGA REDA ZA NASLEDNJI SESTANEK. PRILOŽENA PDF DATOTEKA VSEBUJE ŠKODLJIVO PROGRAMSKO KODO, KI POSKUSI OKUŽITI RAČUNALNIK S TROJANSKIM KONJEM. KO NASLOVNIK ODPRE DATOTEKO, NAPADALEC VSTOPI V OMREŽJE MIMO POŽARNIH PREGRAD.



VARNOSTNI UKREPI:

- **PREVERJANJE VIRA SPOROČILA.**
- **STROKOVNA ANALIZA VSEBINE IN KONTEKSTA SPOROČILA.**
- **SPREMLJANJE VZORCEV IZHODNEGA PROMETA OMREŽJA.**
- **DIGITALNO PODPISOVANJE KORESPONDENCE.**

Sedem (7) priporočil si-certa

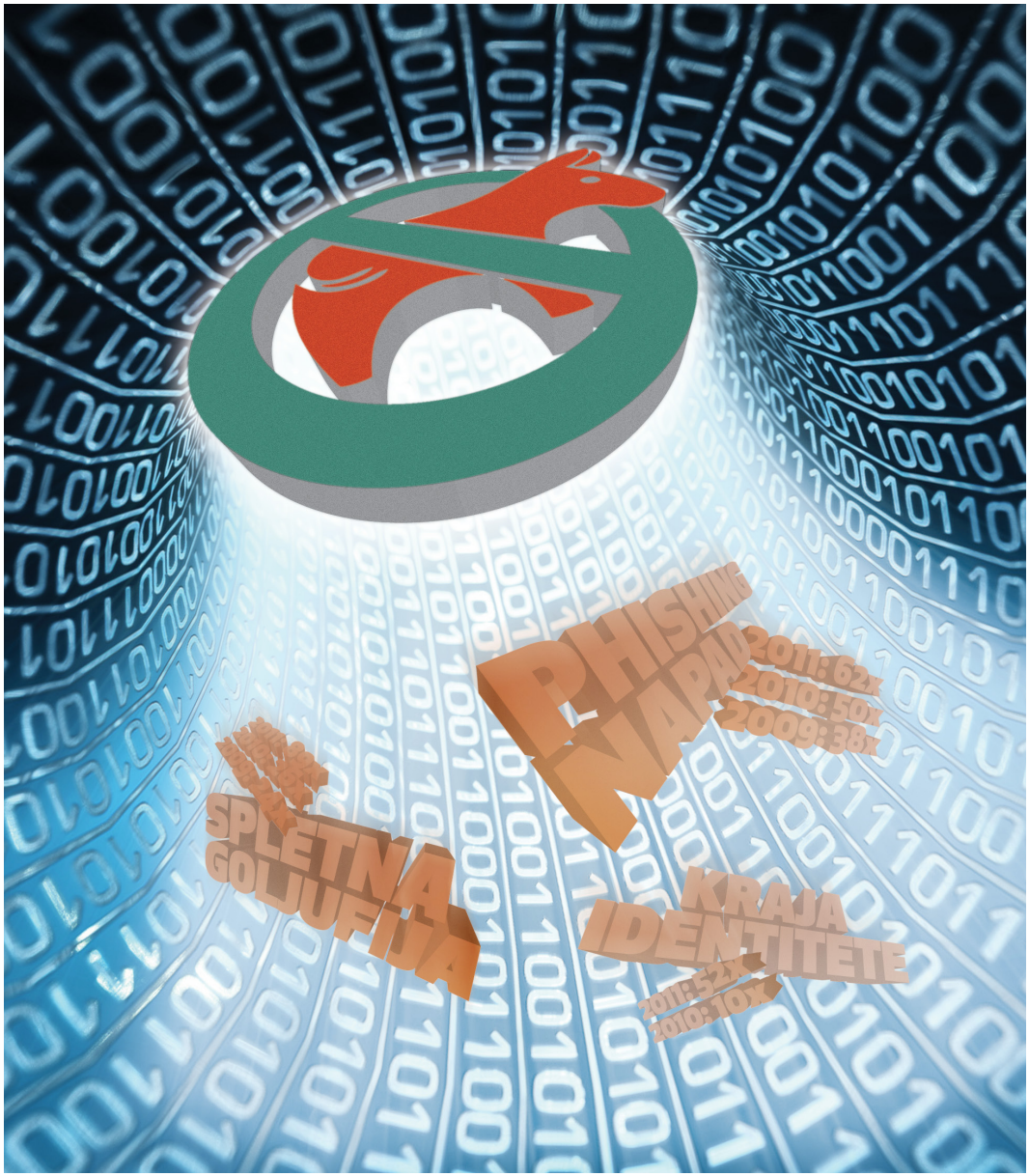
- **Nasvet številka 1**
  Redno in strokovno kompetentno vzdrževanje omrežnih naprav in strežnikov je pomemben del zagotavljanja informacijske varnosti v podjetjih in vseh drugih ustanovah.
- **Nasvet številka 2**
  Organizacije naj načrtujejo izvedbo penetracijskega testa v lastno omrežje s pomočjo neodvisnega zunanjega podjetja, ki ima ustrezne strokovne reference.
- **Nasvet številka 3**
  Razvoj spletnih aplikacij naj sledi smernicam združenja OWASP. Skladnost z njimi naj bo del razpisne dokumentacije za proračunsko financirana naročila.
- **Nasvet številka 4**
  Razvoju spletnih aplikacij naj sledi strokovni varnostni pregled izvorne kode. Na aplikaciji naj se izvede varnostni pregled. Zahteva za izvedbo neodvisnega varnostnega pregleda naj bo del proračunsko financiranih naročil.
- **Nasvet številka 5**
  Neodvisni varnostni pregled in penetracijski test naj postaneta nujna za vse sisteme, ki so del kritične infrastrukture. Varnostna ocena naj bo izvedena tudi za sisteme za upravljanje pametnih števcev na daljavo.
- **Nasvet številka 6**
  Digitalni podpis omogoča dodatno preverjanje vira sporočila in zmanjšuje možnost okužbe preko zlonamernih priponk. Državne ustanove naj pričnejo z uporabo digitalno podpisanih sporočil v vsej komunikaciji po elektronski pošti.
- **Nasvet številka 7**
  Občutljivi podatki naj bodo pri hranjenju in posredovanju šifrirani.

OWASP
The Open Web Application Security Project

VARNI NA INTERNETU

Od mene je odvisno vse.

POROČILO PROJEKTA VARNI NA INTERNETU


PHISHING
NAPADI
2011: 624
2010: 507
2009: 387
SPLETNA GOLJUFIJA
KRAJA IDENTITETE
2011: 52
2010: 107

Najboljša zaščita je preudarno spletno vedenje

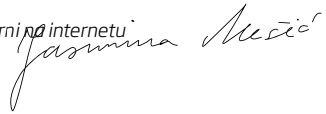
Za trenutek se postavimo v vlogo povprečnega spletnega uporabnika. »Imam naložen antivirusni program in ničesar ne prenašam na svoj računalnik s sumljivih spletnih strani. Ali ni to dovolj?« Odgovor je, na žalost, ne, saj zgolj programska oprema ne more zagotoviti varnosti na internetu. V SI-CERT-u se že od leta 2009 soočamo z vedno večjim porastom različnih oblik spletnih goljufij, socialnega inženiringa in kraje identitete.

Opozorila o zaščiti pred zlonamerno kodo so seveda še vedno na mestu, vendar so časi »Iloveyou« virusa, ki se je širil preko priponk v elektronski pošti, minili. Danes spletne nevarnosti prevzemajo vedno bolj človeško podobo, lahko rečemo, da so spletni goljufi naredili korak naprej in uporabljajo sociološke metode. Skupni imenovalec spletnih prevar je namreč postala manipulacija človeških čustev. Spletni goljufi igrajo na karto človeškega pohlepa, strahu, sočutja, lahkovernosti ali prevelike zaupljivosti. Pred temi nevarnostmi nas ne more zaščititi še tako napreden antivirusni program. Za najboljšo rešitev se tako še vedno izkaže preudarno spletno vedenje.

Spletni goljufi ažurno sledijo tudi aktualnim dogodkom. Tako smo na SI-CERT-u obravnavali več lažnih humanitarnih pozivov k donacijam ob orkanu Katrina ali pa ob potresu na Japonskem. Posodobile so se tudi nigerijske prevare. Če so nas včasih kontaktirale nigerijske vdove, ki so potrebovale pomoč pri prenosu velike količine denarja, nam danes pišejo marinci iz Iraka, ki so našli Sadamov zaklad, ali pa uslužbenec grške banke, ki je tik pred zlomom. Zato je še toliko bolj pomembno, da se spletni uporabniki ves čas izobražujejo o novih oblikah spletnih tveganj.

Projekt Varni na internetu je odziv na naraščajoče število različnih oblik spletnih goljufij. Poleg izvajanja rednih dejavnosti je SI-CERT v začetku leta 2011 prevzel tudi koordinacijo nacionalnega programa ozaveščanja javnosti o informacijski varnosti, ki ga v celoti financira Direktorat za informacijsko družbo. Program Varni na internetu smo zasnovali prav z namenom pomoči, ozaveščanja in izobraževanja širše javnosti glede varne uporabe interneta in prepoznavanja tveganj. Izkazalo se je, da smo imeli prav.

Jasmina Mešić, *koordinatorka programa Varni na internetu*



Varni na internetu

Cilji projekta

Skozi dejavnosti programa Varni na internetu ne poudarjamo zgolj tehničnih vidikov zaščite, temveč je na prvem mestu izobraževanje spletnih uporabnikov. Cilji našega projekta so:

- podučiti spletne uporabnike o različnih oblikah spletnih goljufij, o načinih prepoznavanja nevarnosti in ukrepih za zagotavljanje njihove varnosti,
- informirati o varni uporabi spletnega bančništva in varnem spletnem nakupovanju,
- podučiti spletne uporabnike tudi o tem, kako naj zavarujejo svojo osebno identiteto na spletu, zlasti na družabnih omrežjih.

Dolgoročna razvojna naloga projekta Varni na internetu je »vzgojiti« informacijsko pismenega spletnega uporabnika, ki bo znal informacijsko-komunikacijske tehnologije uporabljati varno in odgovorno.

Ciljna skupina projekta

Vsebine programa Varni na internetu naslavljajo široko slovensko spletno javnost, ciljamo pa predvsem na uporabnike, starejše od 25 let, saj ta populacija že uporablja storitve spletnega bančništva in tudi opravi največji delež spletnih nakupov. Kampanja torej cilja predvsem na odrasle uporabnike interneta. Poseben sklop vsebin namenjamo manjšim podjetjem, ki pri svojem poslovanju prav tako uporabljajo spletno bančništvo in spletne trgovine. Predvsem samostojni podjetniki, obrtniki, manjša podjetja z enim do pet zaposlenimi, zaradi omejenih kadrovskih ali finančnih resursov, pogosto kar sami skrbijo za svoj »IT oddelek«. Pri tem so izpostavljeni različnim tveganjem in potrebujejo bolj specifične informacije, kako varno poslovati na spletu.

Od mene je odvisno vse

Poglavitno sporočilo programa smo strnili v slogan »Od mene je odvisno vse«, saj lahko spletni uporabniki sami storijo največ, da zmanjšajo tveganja. Vendar pa potrebujejo jasna, natančna in razumljiva navodila, kako naj zavarujejo svojo spletno identiteto, računalniško opremo in nenazadnje

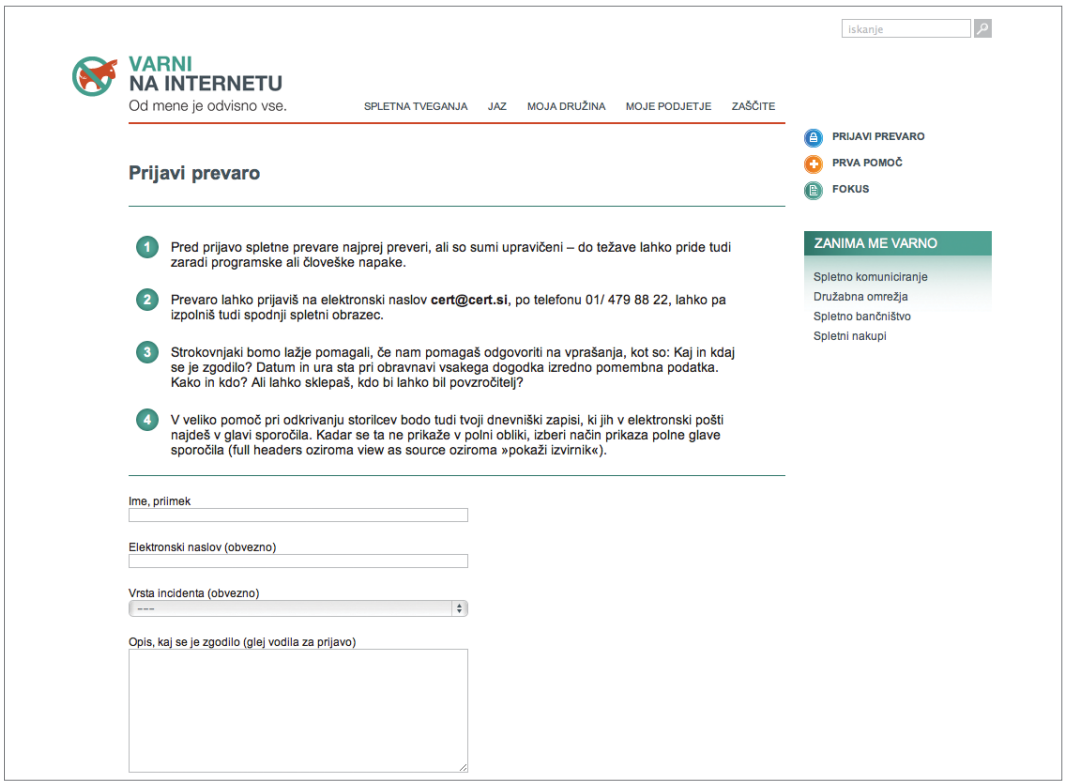
tudi svoj bančni račun. In prav to je naša naloga – preko različnih komunikacijskih kanalov in dejavnosti si prizadevamo izobraževati, pomagati, obveščati, opozarjati in deliti znanje s široko spletno javnostjo. Predvsem si želimo zagotoviti celostno platformo za uporabnike, ki sega od izobraževanja do pomoči.

Vedeti, kako je razumeti, zakaj.

V središče programa ozaveščanja postavljamo izobraževalni portal www.varninainternetu.si, na katerem gradimo zbirko znanja s področja informacijske varnosti. Problematiko varnosti na spletu obravnavamo celostno. Podajamo opredelitve izrazov, opise spletnih prevar, študije konkretnih primerov, usmeritve na ustrezne zunanje vire, nasvete – tudi v obliki video navodil. Blog Fokus bolj poglobljeno obravnava izbrane varnostne teme.

Prijava je prvi korak

Na portalu je vzpostavljena prijavna točka oz. spletni obrazec, preko katerega lahko oškodovanci prijavijo omrežni incident (vdor, goljufija, kraja identitete, itd.). Gre za nacionalno prijavno točko. Pomagamo in svetujemo strokovno usposobljeni sodelavci nacionalnega centra SI-CERT, naše znanje je na voljo vsem spletnim uporabnikom brezplačno. Statistika SI-CERT-a kaže, da se je število vseh prejetih prijav, v primerjavi z letom 2010, povečalo za skoraj 60 %. Porast lahko gotovo pripišemo tudi novemu komunikacijskemu kanalu, ki ga je spletna skupnost dobro sprejela.



Nasvet iz prve roke

V letu vzpostavitve projekta smo posebno pozornost usmerili v promocijo projektne platforme. V mesecu maju, ki je bil v znamenju varne rabe interneta, smo z mobilno info točko obiskali večja nakupovalna središča v Celju, Ljubljani in Mariboru, naše vodilo pa je bilo – nasvet iz prve roke. Obiskovalci so lahko izvedeli vse o kraji gesel, lažnih Facebook profilih, spletnih goljufijah in drugih spletnih nevarnostih. Vsak obiskovalec je dobil posebno darilo - zobno ščetko z enkratno zgodbo. Naše dejavnosti naslavljajo le del precej širokega področje problematike informacijske varnosti, zato je pomembno sodelovati in deliti izkušnje s sorodnimi organizacijami. Tako smo v letu 2011 več akcij izvedli v sodelovanju z Združenjem bank Slovenije, Zvezo potrošnikov Slovenije, s Centrom za varnejši internet SAFE-SI in z uradom Informacijskega pooblaščenca, ki prav tako podpirajo varnejšo in odgovornejšo rabo spleta. Naš cilj je skupen – zmanjšati tveganja, ki smo jim izpostavljeni, in v polni meri izkoristiti vse prednosti, ki jih internet prinaša.

Vsebinsko zasnovo in komuniciranje projekta je zaznala tudi strokovna javnost, ki je spletni strani varninainternetu.si podelila nagrado Netko 2011 v kategoriji predstavitve institucij s področij državne in javne uprave.

Abc varnosti na spletu

Vsak izobraževalni projekt potrebuje svoj priročnik, zato smo izdali Hitri vodnik, ki kratko in enostavno opisuje najpogostejše spletne prevare, obenem pa podaja vodila varnega spletnega nakupovanja, bančništva in družabnega mreženja. Knjižica je izšla z osrednjima dnevnikoma Delo in Večer, prejeli pa so jo tudi naročniki revije VIP, ki jo izdaja Zveza potrošnikov Slovenije. Vodniku so sledili še oglasi na televizijskih in radijskih postajah, spletne pasice ter oglasi v podjetniških revijah.

Primeri spletnih nevarnosti

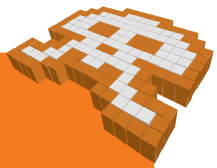
Primer številka 1: ukradeno geslo

Prek prijavne točke portala Varni na internetu smo v letu 2011 zabeležili največ vprašanj in prijav na temo: »Ukradli so mi geslo, kaj naj storim?« V večini primerov je šlo za onemogočen dostop do uporabniškega računa Gmail in Facebook. To enostavno zaporedje črk in številk na tipkovnici ne izkazuje zgolj uporabnikove identitete, temveč obenem tudi varuje podatke. Pomislite samo na vaš e-poštni predal ali Facebook profil – koliko kontaktov, slik, dokumentov in osebnih podatkov je na voljo. Prav iz tega razloga smo posebno pozornost namenili nasvetom o skrbnem ravnanju z uporabniškimi računi e-pošte in Facebooka. Na portalu www.varninainternetu.si smo pripravili navodila, kako lahko uporabniki pridobijo informacije o prijavah v račune Gmail in Facebook. Gre za prvi korak k odkrivanju morebitnih zlorab uporabnikovega računa. Prav tako smo pripravili navodila za ponovno pridobitev dostopa in nadzora nad uporabniškim računom, ki pa je pri tujih ponudnikih pogosto otežen. Ker se večina ponudnikov spletnih storitev (npr. Gmail, Hotmail, Facebook) nahaja v ZDA, čaka uporabnike dolg in zapleten postopek, da jih prepoznajo kot prave lastnike računov.

(NE)VARNO DEJSTVO:
GOLJUFI PRIDOBIJO GESLA NA RAZLIČNE NAČINE. LAHKO GA UGANEJO, KADAR JE RES ENOSTAVNO (NPR. 123456) ALI GA PRESTREŽEJO PREK PODTAKNJENEGA ZLONAMERNEGA PROGRAMA NA DOMAČEM RAČUNALNIKU. ŠE NAJBOLJ POGOST PA JE PHISHING NAPAD, KJER UPORABNIKA Z LAŽNIM OBVESTILOM PREPRIČAJO, DA MORA PRI PONUDNIKU SPLETNE POŠTE IZ TEGA ALI ONEGA RAZLOGA »PREVERITI RAČUN« IN PONOVNO VNESTI SVOJE PODATKE.

Primer številka 2: lažne spletne trgovine UGG

»Uggice« so bile odlična krinka za spletne goljufije tudi v letu 2011. Gre za znano blagovno znamko (za vse nepoznavalce, to so modni zimski škornji), ki so jo so že v preteklih letih goljufi izkoriščali za privabljanje kupcev v lažne spletne trgovine. Tudi lani smo odkrili več lažnih Ugg spletnih trgovin, vse z zelo podobnim videzom in seveda zelo nizkimi cenami (uggbootseurope.com, uggsale.cc, uggboots-euro.com, uggeden.com). Konkretno, trgovina uggbootseurope.com s svojim imenom nakazuje, da gre za spletno trgovino s sedežem v EU, vendar smo ugotovili, da je bila domena registrirana na Kitajskem, spletno mesto pa se je nahajalo na strežniku v Panami. Obvestili smo ponudnika gostovanja spletne trgovine in dosegli njen umik, prav tako smo stopili v stik z Zvezo potrošnikov Slovenije. Sodelovanje z ZPS nadaljujemo tudi v prihodnje, saj imamo skupen cilj – opozarjati na pasti spletnega nakupovanja.



(NE)VARNO DEJSTVO

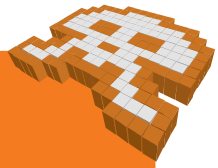
PRED NAKUPOM V SPLETNI TRGOVINI POIŠČITE ELEKTRONSKI NASLOV PRODAJALNE OZIROMA NJIHOV SPLETNI OBRAZEC ZA KONTAKT S STRANKAMI. POSTAVITE VPRAŠANJE O KAKŠNEM IZDELKU. ODGOVOR BOSTE PREJELI PO ELEKTRONSKI POŠTI. ČE BOSTE ODGOVOR PREJELI OD KAKŠNEGA VELIKEGA PONUDNIKA BREZPLAČNE ELEKTRONSKE POŠTE KOT SO, DENIMO, GMAIL, HOTMAIL ALI YAHOO, POTEM JE TO ZNAK ZA ALARM, SAJ RESNA PODJETJA UPORABLJAJO SVOJE LASTNE DOMENE.

Primer številka 3: kredit kar prek spleta

Na slovenskih spletnih mestih, ki ponujajo pomoč v stiski, ali pa samo male oglase za različne storitve, smo v letu 2011 zasledili tudi ponudbe kreditov. *Ena izmed njih se glasi: »Ali ste v finančni krizi? Ali ste že zavrnili banke za posojilo? Ali potrebujete denar nujno? Ste prišli na pravo mesto. To posojilo je 100 % zagotovljena. Contact me zdaj in dobili kakovostne storitve. Gospa Ebis Vivian (finaid45@hotmail.com).«*

Odločili smo se preveriti, kako prevara deluje, zato smo »gospe Vivian« poslali povpraševanje za kredit. Izbrali smo vsoto 4.200 evrov. Še isti dan smo dobili odgovor, da lahko dobimo kredit za obdobje 36 mesecev, mesečni obrok pa je 128 evrov; torej 10-odstotne obresti na celoten znesek. Gospa Vivian je končala svoj odgovor takole: »Če ste v redu s pogoji zgoraj, nazaj k meni, tako da lahko gremo na naslednji korak.« V naslednjem koraku smo morali posredovati svoje osebne podatke, telefonsko številko, višino mesečnega dohodka in podobno. Torej vse tisto, kar bi tudi sicer pričakovali pri najemu kredita. Posredovali smo izmišljene podatke in telefonsko številko pri spletnem ponudniku telefonije. No, »pristojbino« v višini 100 evrov naj bi plačali prek sistema Western Union. Zelo nenavadno je, da bi banka, ki ponuja kredite, za svoje stroške prejemala plačilo prek plačilnega sistema Western Union.

Skratka, šlo je za še eno obliko nigerijske prevare, v tem primeru pod krinko ponujanja hitrih kreditov. Stroške za odobritev kredita je bilo treba poravnati prek sistema Western Union in zaključek zgodbe – denar ste nakazali v Nigerijo, od kredita pa ni bilo nič.

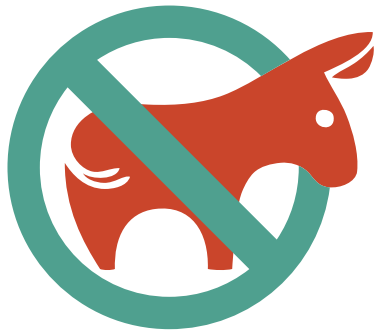


(NE)VARNO DEJSTVO

KUPLJENIH PREDMETOV ALI STORITEV NA SPLETU NE PLAČUJTE Z WESTERN UNION ALI S SISTEMOM MONEYGRAM. SISTEMA STA NAMENJENA HITREMU NAKAZILU GOTOVINE POSAMEZNIKOM IN JU ZARADI TEŽAV S SLEDLJIVOSTJO S PRIDOM UPORABLJAJO SPLETNI GOLJUFI.

Šest (6) priporočil za varno rabo interneta

- **Nasvet številka 1**
  Gesla varujte, kot varujete zobno ščetko – ne posojajte jih in jih redno menjajte!
- **Nasvet številka 2**
  Ne uporabljajte zgolj enega gesla za vse uporabniške račune (ustvarite različna gesla za npr. elektronsko pošto, Facebook, forume, spletno bančništvo).
- **Nasvet številka 3**
  Premislite, ali ne bi za elektronsko pošto in druge spletne storitve uporabljali poštnega naslova pri slovenskem ponudniku. Pri teh je urejanje težave izgubljenega oziroma ukradenega gesla veliko bolj zanesljivo, preprosto in hitro.
- **Nasvet številka 4**
  Osnovno pravilo varnega spletnega nakupovanja je izogibanje neverjetno ugodnim ponudbam. Kadar neka ponudba po predstavitvi, ceni ali lastnostih odstopa od ostalih, potem je to zanesljiv razlog za previdnost.
- **Nasvet številka 5**
  Presodite, ali razlika v ceni nakupa pri ponudniku v tujini odtehta tveganje, ki ga pri tem prevzamete.
- **Nasvet številka 6**
  Znak za alarm so spletne trgovine, ki omogočajo plačilo izključno s sistemoma Western Union ali MoneyGram. Tovrstni obliki plačila ne omogočata sledenja nakazilu in obstaja velika verjetnost, da gre za lažno spletno trgovino.



www.varninainternetu.si

Izdajatelj: Akademska in raziskovalna mreža Slovenije

Oblikovanje in izvedba: Zadrga, komunikacijska agencija

Tisk: Dosa - Dornik, Ljubljana

februar 2012

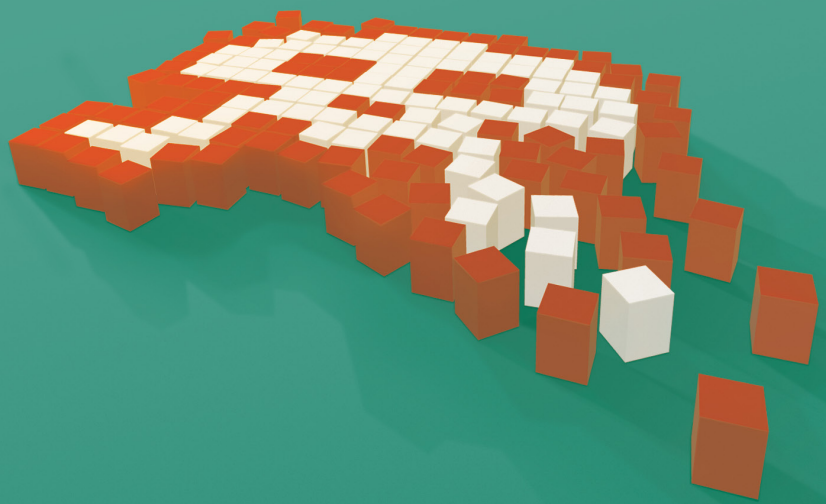
VARNI
NA INTERNETU

Projekt Varni na internetu izvaja Slovenski center za posredovanje pri omrežnih incidentih SI-CERT, ki deluje pod okriljem javnega zavoda Arnes.

www: www.varninainternetu.si

Facebook: facebook.com/varninainternetu

Twitter: twitter.com/varninanetu



arnes

si·cert

VARNI
NA INTERNETU