MARIBORSKI VODOVOD

INTERNO GRADIVO!

Informacijska varnost na delovnem mestu

mag. Rado Gornik

nov.,dec. 2015

VSEBINA

1. UVOD
2. VARNOSTNE GROŽNJE SPLETNEGA POSLOVANJA
3. ORGANIZACIJA INFORMACIJSKE VARNOSTI V DRUŽBI
4. UPORABNIŠKE VARNOSTNE POLITIKE

1.UVOD

- **Kaj** je informacijska varnost?
- **Zakaj** je pomembna ?
- **Kako** jo zagotavljamo?
- **Cilj**, ki ga zasledujemo

Kaj je informacijska varnost?

...gre za procese vezane na temeljne kategorije podatkov oz. informacij našega informacijskega sistema:

- **Zaupnost** – informacija/storitev je na voljo samo pooblaščenim osebam.

(Stranke pričakujejo zaupnost. Dostopnost nepooblaščeni osebi pomeni zlorabo stranke, zaposlenih, kršenje ZVOP-a, razkrivanje konkurenci...)

- **Celovitost** (Integriteta) – točnost in popolnost informacije, ki ni bila nedovoljeno spremenjena. (napačna informacija lahko povzroči izgubo zaupanja stranke, zaposlenih...)
- **Razpoložljivost** (Dostopnost) –informacija/storitev je dostopna pooblaščenim osebam, kadar jih potrebujejo. (nedosegljiva informacija lahko povzroči neizpolnjevanje pričakovanj stranke,...)

Informacijska varnost pomeni varstvo podatkov in informacijskih sistemov pred nezakonitim dostopom, uporabo, razkritjem, ločitvijo, spremembo ali uničenjem.

Zakaj je pomembna?

- Kar 80% ljudi bi zaupalo svoje uporabniško ime in kar 60% bi jih zaupalo svoje geslo osebi, ki bi se pretvarjala, da prihaja iz oddelka za računalniško podporo. (Bakshi in avt. 2009)
- Socialni inžinering in neprevidno ravnanje ljudi sta odgovorna **za več kot 1/2** vseh varnostnih zlorab. (Mackenzie 2006)
- Slovenija: zgolj 35% uporabnikov ocenjuje lasten IS, kot dober, ostala večina, kot nezadostnega ali slabega. (Bernik, Prislan, 2010)
- **Netehnični vidiki** so eneko pomembni, kot tehnični vidiki pri varovanju občutljivih in zaupnih informacij. (Alfawar in avt. 2010)
- Nacionalna Zakonodaja**: ZEKom-1, ZEPEP, ZVOP, ZVDAGA, ZVPot, ZFPPIPP...**
- Nagovor direktorja *"... Podatke in informacije smatramo kot najpomembnejšo poslovno dobrino, ki ima neposreden vpliv na poslovni uspeh podjetja, na njegovo vrednost in njegovo podobo v javnosti. Zavedamo se... "* – **Poslovnik VI podjetja MV**

Kako jo zagotavljamo?

- Z tehničnimi ukrepi, ki jih zagotavljajo sodelavci v Službi informatike
- Z organizacijski ukrepi (netehnični), ki jih zagotavlja vodstvo podjetja (organizacija, forum, politike,...)
- S sodelovanjem vseh uporabnikov v podjetju: od direktorja do slehernega zaposlenega!

Zaposleni:

- Varnost informacij/storitev je odvisna od najšibkejšega člena!
- Med zaposlenimi vlada bisteven razkorak med **poznavanjem** informacijskih groženj (vem-znam) ter **odnosom** do informacijske varnosti- vem a ne delam tako!
- *"Za varovanje informacij smo odgovorni vsi sodelavci podjetja MV, tako smo dolžni spoštovati določila Poslovnika informacijske varnosti in pripadajočih politik, ter smo odgovorni za izvajanje ukrepov v sistemu vodenja varovanja informacij."* Poslovnik VI

1. UVOD

- Cilj

...programa informacijsko varnostnega ozaveščanja je okrepiti zavedanje pomena varnosti IS v podjetju in zavedanje negativnih posledic varnostnih incidentov!

2. VARNOSTNE GROŽNJE

•Uporaba omrežja nam olajša komunikacijo, a nas izpostavlja različnim grožnjam.

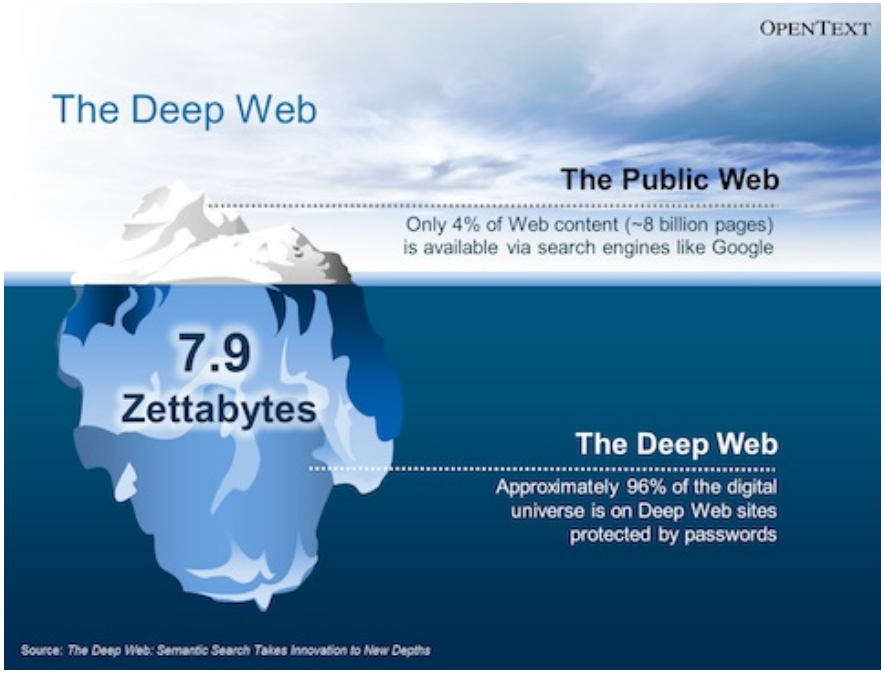
Z izkoriščanjem:

- varnostnih lukenj sistemov,
- ranljivosti v programski opremi,
- naših vedenjskih vzorcev,

lahko tujci pridobijo nadzor nad opremo, zaupnimi (osebnimi) podatki podjetja in denarjem.

INTERNET – Kibernetski (virtualni) prostor

Kjer se srečujemo vsi: virtualne identitete -> **realne škode**!



Deep web: 96% vseh internet vsebin - ilegalne vsebine (Silk Road 2.0)
Uporabniki: kriminalci, tajne službe, policija, raziskovani novinarji… vedno več navadni uporabniki , ki si želijo zasebnosti.

2. VARNOSTNE GROŽNJE

• **OKUŽBE:**

Tipične grožnje **nekoč**: Virusi, trojanci, črvi,...zlonamerna programska koda (ang. Malware) je bila namenjena zabavi, pogosto uničevanju...

Tipične grožnje **danes**: zlonamerna koda služi kraji identitete in vdorom, posledično kraji podatkov in denarja.

• **SPAM**: nezaželjena oglasna pošta, pogosto tudi oglaševanje dvomljivih izdelkov ali goljufije in prevare (nigerijska prevara)

• **RIBARJENJE** (ang. Phishing): storilec nas poskuša zvabiti na lažno stran spletne storitve (pogosto Amazon, LinedIN, Ebay, **SLO BANKE 2015**), pod pretvezo preverjanja podatkov, z namenom pridobitve naših podatkov (upor.ime, geslo, kreditna kartica...)

2. VARNOSTNE GROŽNJE

• **VDORI** (ang. Hacking) v računalniški sistem – klasična oblika hekerskega napada (izkorišča ranljivost programa ali slabo geslo)

• **RAZOBLIČENJE** (ang. Defacement) spletnih strani.

• **KRAJA IDENTITETE** je pogosto zgolj posredni cilj, kako priti do ostalih podatkov (emailov, bančnih kartic, službenih podatkov,...) POMEN OSEBNIH PODATKOV!

TEST INFORMACIJSKEGA POOBLAŠČENCA:

https://www.ip-rs.si/kraja-identitete/test/index.html

2. VARNOSTNE GROŽNJE

POMEN (DIGITALNE) ZASEBNOSTI

- Zasebnost je širok pojem, nima univerzalne definicije (zasebnost komuniciranja, stanovanjska zasebnost, duševna zasebnost, lastništvo, intima...). **Zasebnost = svoboda misli, odločanja, ravnanja...**
- Po vseh listinah je **osnovna človekova pravica**! (EU konvencija o človekovih pravicah – 8.člen: Pravica do spoštovanja zasebnega in družinskega življenja)
- **Pravica pa ni absolutna!** Pravica do zasebnosti se konča tam, kjer se začne pravica drugega posameznika, družbe, podjetja... Samo natančno določeni, nearbitrarni in sorazmerni pogoj dajejo legitimnost vdoru v zasebnost – razlika med sodobno, odprto družbo in diktaturo.
- Bistvema razlika med ZDA (bolj ščiti prostorsko zasebnost) in EU (večji pomen informacijske zasebnosti) pravnim redom

Kaj je huje z vidika informacij? Vdor v stanovanje (analogno) ali vdor računalnik, mobilni telefon – poplava digitalnih sledi- informacij?

2. VARNOSTNE GROŽNJE

Koga zanima moja zasebnost?

Državo (represivne organe), kabelskega operaterja, multinacionalke, soseda, hekerja...FURS?

Primer nesorazmernega posega!

Motivi “Kiberkriminalcev”:

- **Osebni**: okoriščanje**,** zabava, maščevanje, samodokazovanje, zabava,...
- **Profesionalni**: kraja intelektualne lastnine, pogodbenih skrivnosti, poslovnih partnerjev, onemogočanje konkurence, denar...
- **(Kiber)terorizem**: napadi na posamezno državo, povzročanje ekonomske škode ali celo ogrožanje življenj. (diplomatska špijonaža, poškodbe infrastrukture,...) **Tarče so infrastrukturna podjetja!**
- **Hacktivizem** (legalni ali ilegalni): podpora: političnim aktivistom, družbeno/socialnim spremembam, svobodi interneta,

  (Anonymous, Afriška pomlad, ACTA, Okupirajmo Wall Street)


2. VARNOSTNE GROŽNJE

Leto 2014 je bilo slabo a postaja vse slabše !

Kibernetski kriminal je rastoča industijska panoga, z ogromnimi dobički in majhnimi tveganji!

- **400-600 mrd €** znašajo svetovne (direktne+indirektne) izgube ali 0,5% BDP v razvitih in 0,2% v manj razvitih državah, vir McAfee 2014
- **400 mil** žrtev letno, ali **1 mil/dan**, 12/sek, vir Norton report 2013
- Elektronska pošta v 2012 (138.000-Yahoo, 107.000-Gmail, 55.000-Hotmail, 26.000-AOL,...) – 1 hackerska skupina D33DS
- Kibernetska vojna: **15% svetovnega internet prometa predstavljajo napadi!** vir: futerzone.at, 6.11.2012
- Igube EU plačilnih sistemov- kartic zaradi kibernetskega kriminala v 2012 znašajo **1,5 mrd €** , vir: EC3 2013

Kiberkriminal nam je bližje kot si mislimo!

2. VARNOSTNE GROŽNJE

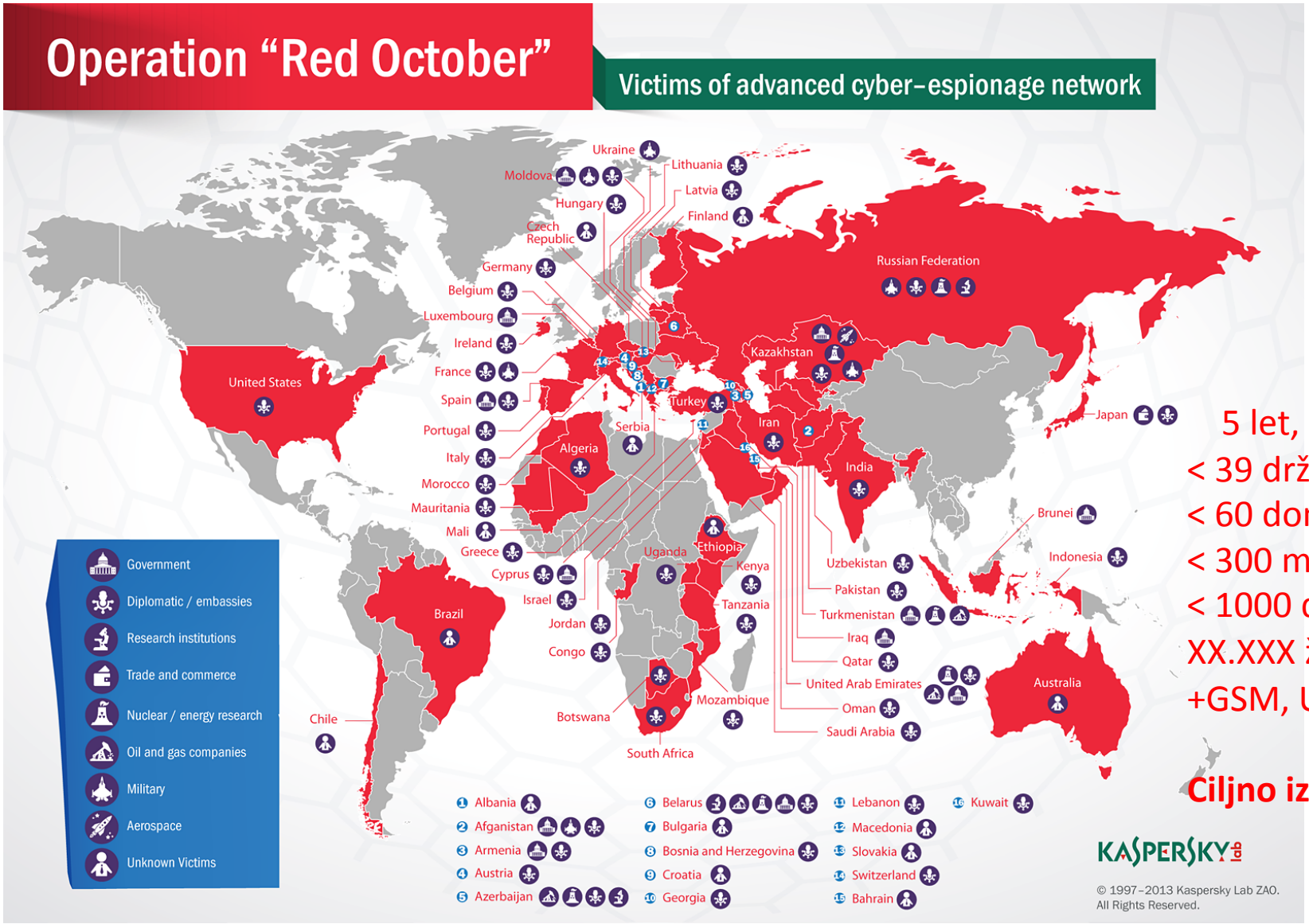
Juli 2015: 37 mio up., osebni podatki, kreditne kartice, zasebna sporočila, vse podatki podjetja… MOTIV: 20$?

Okt 2015: 4 mio up., osebni podatki, bančni podatki, 40mio€, MOTIV:ideologija!

MARIBORSKI VODOVOD

2. VARNOSTNE GROŽNJE

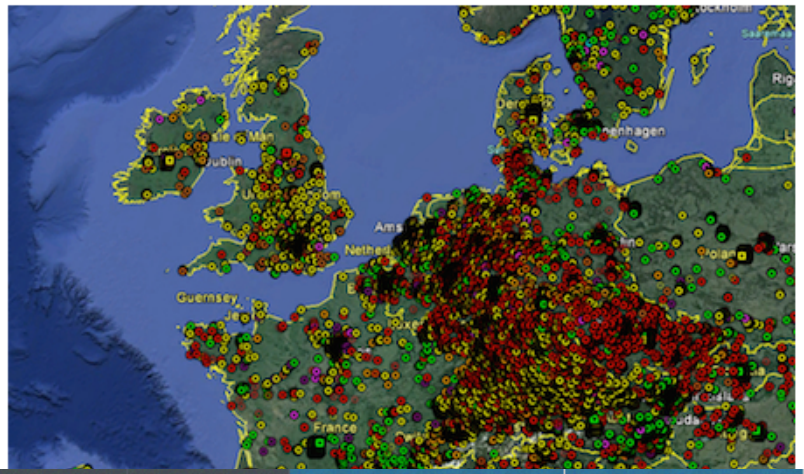
14.1.2013, Kaspersky



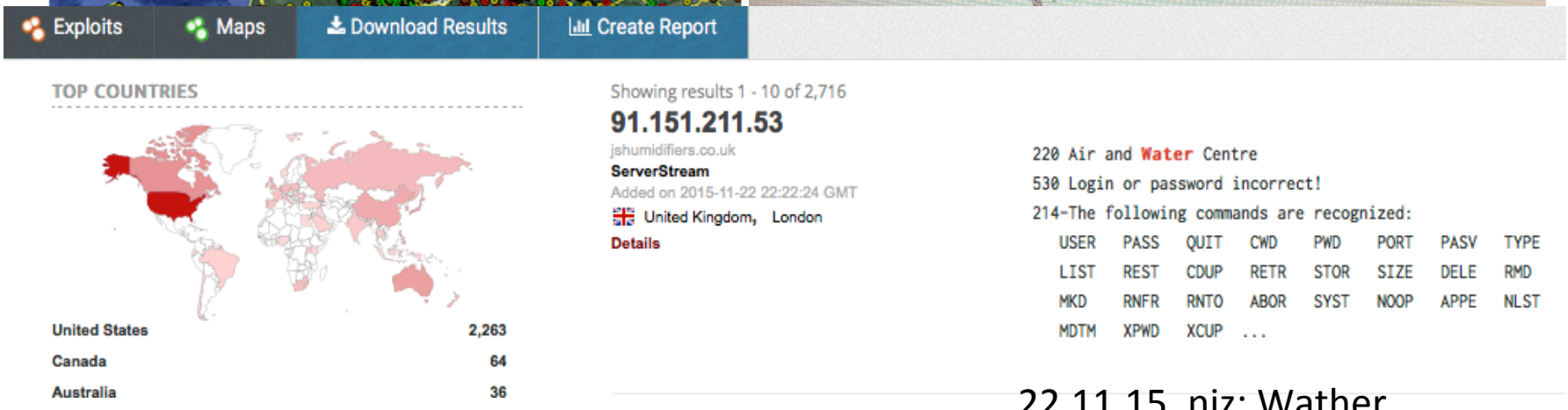
5 let,
< 39 držav,
< 60 domen,
< 300 modulov,
< 1000 datotek,
XX.XXX žrtev,
+GSM, USB…

Ciljno izbrane!

Industrijska informatika! (SCADA, PLC, BUS,…)

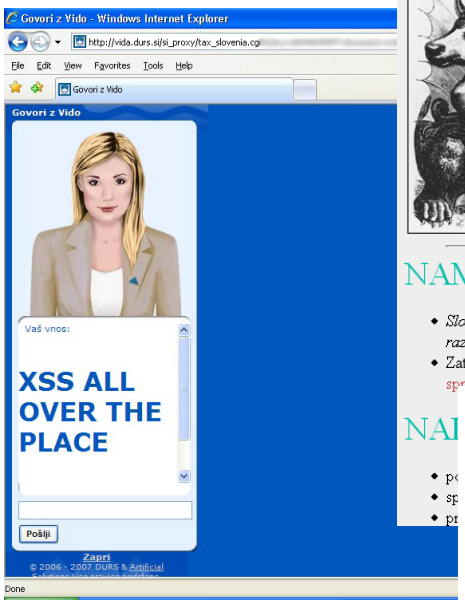


22.11.15, niz: Siemes



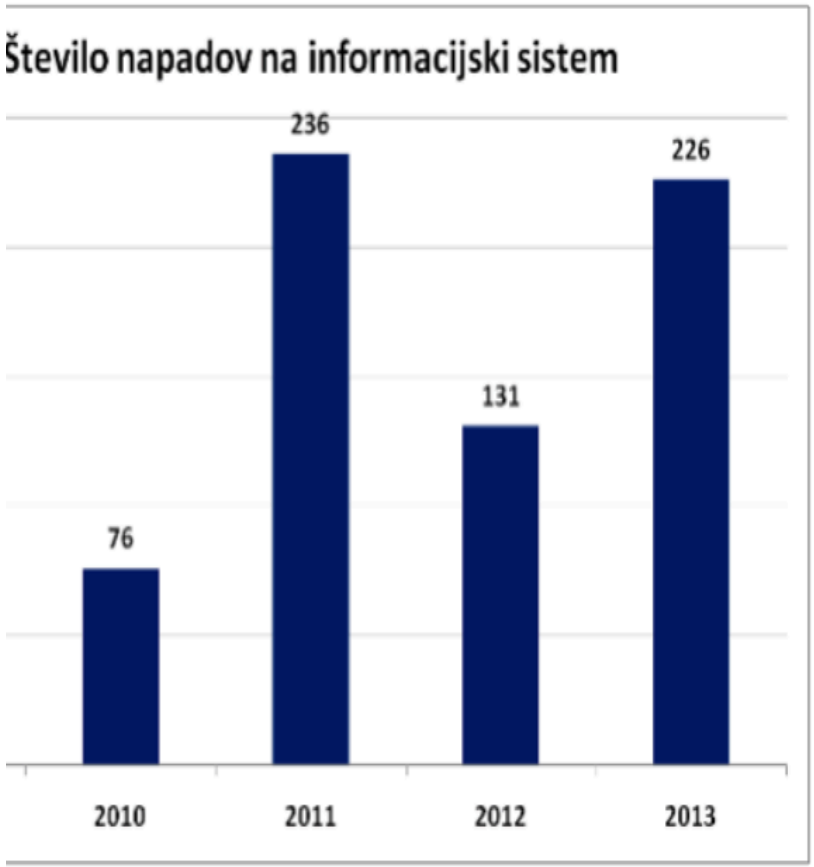
22.11.15, niz: Wather

2. VARNOSTNE GROŽNJE



2. VARNOSTNE GROŽNJE

Število prijav goljufij, ki jih je dobil SI-CERT. Vir: SI-CERT



Vir: policija

SLO: evidentirana direktna škoda nekaj 100.000 €

Socialni inženiring

"pomeni po svoji naravi pridobivanje nekih koristi z zlorabo oz. manipulacijo zaupanja posameznika" tako **z tehničnimi**, kakor **netehničnimi** sredstvi.

- Socialni inžinering preko telefona: lažno predstavljanje (primer Luke Koper).
- Neposredni pristop: anketar, študent, raziskovalec, hierarhično višji...
- Gledanje čez ramo: pogosto v trgovinah (sledi gibom tipkanja gesla, pin kode).
- Brskanje po smeteh (pravilno uničevanje podatkov).
- E-mail phishing: vljudno opozarja na osvežitev podatkov.
- Lažne spletne strani: pozor na pravien URL naslov! (pogosto spletne banke).
- Nosilci podatkov: Lažni USB ključek z zlonamerno kodo.
- Lažno Brezžično omrežje: lahko spremljajo vse kaj vtipkamo.
- **Družabna omrežja:** so polna naših osebni podatkov, lažno predstavljanje...

Družabna omrežja ? DA, ampak....

Larry Wall

Richard Stallman

Razkritih 6,5 mio gesel

45.000 računov

Brigite?

Marchello?

Kdo bo vaši novi prijatelji, poslovni partner...? NAČELO PREVIDNOSTI!

Družabna omrežja so del poslovanja, vendar...

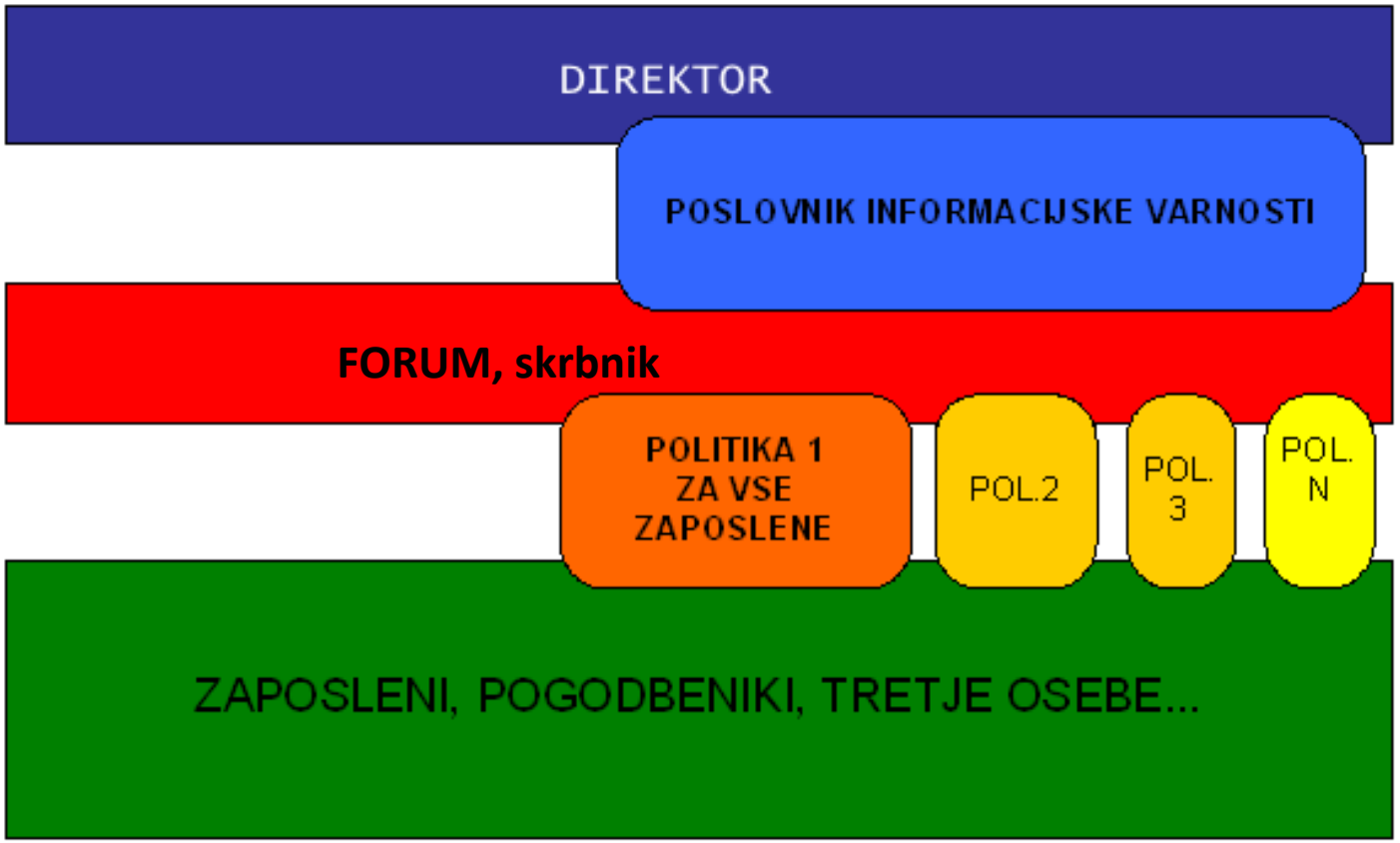
predstavljajo tveganja za podjetje:

- Prepletanje zasebnosti in podatkov o podjetju
- Možna objava zaupnih podatkov
- Zaradi objave podjetja(delovnega mesta), posameznik lahko postane **prehodna tarča ali sredstvo**.... Končni cilj je podjetje!
- Iz objavljenih osebnih podatkov, družinskih članov, hišnih ljubljenčkov, naljubših pisateljev, knjig, filmov... je z veliko verjetnostjo **možno generirati geslo** za dostop do zasebnih ali službenih računov.
- Z mailom in geslom do službenega e-maila (OWA) ali daljinskega dostopa je možen dostop do zaupnih podatkov podjetja, ali....

Tudi z zasebnim ravnanjem vplivamo na varnost podjetja!

3. ORGANIZACIJA VI V PODJETJU

MV je vpeljal sistem vodenja varovanja informacij po smernicah **ISO/IEC 27001**. Namenjen je tako zaščita zaposlenih kakor tudi podjetja samega.



3. ORGANIZACIJA VI

DIREKTOR - POSLOVNIK INFORMACIJSKE VARNOSTI:

- opredeljuje zavezanost vodstva varovanju informacij,
- vpeljuje organiziranost varovanja – **vlogo foruma** in zadolžitve,
- strukturo in organiziranost dokumentov.

SKRBNIK VI – administrativna vloga, dokumentacija, sklicuje srečanja

FORUM VI

Je interdisciplinarni organ, ki obravnava vse v zvezi s tematiko VI (organizacija, vzpostavitev, izvedba, izvajanje nadzora, izboljševanje...)

Stalni člani so **vsi vodje** podjetja MV, po potrebi pa tudi drugi, nestalni člani

3. ORGANIZACIJA VI

VARNOSTNE POLITIKE:

- so drugonivojski dokumenti, ki jih sprejema direktor MV na predlog forum-a
- namenjene so vsem ali posameznim skupinam uporabnikov,
- vsebujejo pravila, ki se nanašajo na rokovanje, uporabo in upravljanje z informacijskimi viri,
- so neodvisne od tehnologije in opredeljujejo način, kako doseči ustrezen nivo varovanja in zaščite informacijskih virov, z opredelitvijo in predpisano uporabo varnostnih mehanizmov,
- opredeljuje pravilno uporabo informacijskih virov, ter **odgovornosti zaposlenih** – PRAVNO OBVESTILO,
- vsaka politika je natančno strukturirana, opremljena: IME, VERZIJO, DATUM SPREJEMA, SLEDENJE SPREMEMB.

Politike spoštujejo zasebnost uporabnika in pravico do omejene komunikacijske svobode!

4. UPORABNIŠKE VARNOSTNE POLITIKE

"Oh, can't complain."

- Politike vsebujejo pravila za rokovanje z informacijskimi sredstvi
- Minimizirajo konflikt pravic in zagotavljajo zasebnost! (direktiva EU 2002/58/ES – Zasebnost elektronskih komunikacij)
- **V podjetju MV je izrecno je opredeljena PRIČAKOVANA PRAVICA do ZASEBNOSTI a tudi način!**

4. UPORABNIŠKE VARNOSTNE POLITIKE

“Uporabniške” politike so namenjene slehernemu zaposlenemu, ki uporabljaja IT sredstva podjetja:

VP_01_01 Poslovnik varovanja informacij

VP_03_01 Politika primerne rabe informacijske tehnologije

VP_04-01 Politika varovanja človeških virov

VP_04_02 Politika uporabe interneta

VP_04_03 Politika uporabe elektronske pošte

VP_06_01 Politika zaščite pred zlonamerno programsko opremo

VP_07_01 Politika uporabe gesel

VP_07_03 Politika mobilnih naprav

VP_07_04 Politika oddaljenega dostopa

VP-03-01 Primerna raba informacijske tehnologije

Vsebuje splošne napotke glede varne uporabe**. Za vzdrževanje opreme se obrnite na podporo uporabnikom tel.261 na elektronski naslov it.podpora @mb-vodovod.si**.

Strogo prepovedane aktivnosti:

- Priključevanje v omrežje brez odobritve službe informatike
- Odnašanje podatkov izven MV, ki ni v skladu z politikami... brez odobritve
- Posredovanje osebnih podatkov (ZVOP) ali podatkov o MV brez pooblastila?
- Nameščanje nelegalne programske opreme
- Razkritje gesla uporabniškega računa (vključno sodelavcem, družinskim članom...)
- Vse ostale oblike nadlegovanja...

4. UPORABNIŠKE VARNOSTNE POLITIKE

- Uporaba službenih tiskalnikov za zasebne namene
- Pošiljanje ali posredovanje neželene elektronske pošte ali reklamnega materiala, verižnih e-sporočil ali piramidnih oz. podobnih shem kakršnekoli vrste
- Posredovanja službene elektronske pošte na drug (zaseben) elektronski naslov

Dovoljena je omejena zasebna raba, ki je v skladu z določili politik!

Brskanje po spletnih straneh, prejemanje in pošiljanje zasebnih elektronskih sporočil je omejeno dovoljeno, vendar le v kolikor to ne ogroža delovnega procesa ali informacijske infrastrukture, ter v kolikor ne posega v pravice ostalih uporabnikov oz. zaposlenih!

Uporaba mape "ZASEBNO" < 4GB podatkov

4. UPORABNIŠKE VARNOSTNE POLITIKE

Varovanje opreme zunaj prostorov podjetja

•Oprema (Notebook, Pametni GSM) ne sme biti nenadzorovana v javnih prostorih

•posebno pozornost posvetite pri priključevanju preko WI-FI dostopnih točk, uporabljajte **le poznane** (operateji, občina LJ, MB...). Predlagam LTE !

•Varno logiranje obvezno! Primer**:** https://www.facebook.com ali https://mail.google.com **,** torej **http**s – "secure"

•Službena OWA je varen način povezovanja z službeno e-pošto

Varno uničenje in ponovna uporaba sredstev

Fizično uničenje magnetnih medijev CD,DVD – sami, za trde diske poskrbi informatika! Papirna dokumentacija – rezalnik!

USB ključi: nikoli ne vtikajte najdenih USB ključev – možno, da je podtaknjen! Na USB medije ne kopirajte zaupnih podatkov! Če že, jih zaščitite-kriptirajte.

4. UPORABNIŠKE VARNOSTNE POLITIKE

Nadzor

•nadzor je namenjen predvsem ugotavljanju varnostnih lukenj in pomanjkljivosti informacijskega in povezanih sistemov

•je omejen na nadzor uporabe ter delovanja računalnikov in druge informacijske opreme – ne pa nadzoru (vsebine) uporabnika

•Podjetje je zavezano spoštovanju zasebnosti na delovnem mestu. Do vsebine lahko dostopa zgolj v izrednih primerih pod posebnimi pogoji skladno z določili politike – vnaprejšnje obvestilo uporabnika.

•Podjetje upošteva načela sorazmernosti, zakonitosti in ustavne dopustnosti.

Uveljavljanje politike – velja za vse politike!

Vsi zaposleni ste odgovorni za izvajanje določil te (ostalih) politik(e)!

Kršitev določil politike je lahko predmet disciplinskih postopkov!

4. UPORABNIŠKE VARNOSTNE POLITIKE

VP-04-02 Politika uporabe elektronske pošte

Primerna raba

- Službeni naslov ime.priimek@mb-vodovod.si je namenjen izvrševanju nalog delovnega mesta
- Zahteva se **natančnost** pri pisanju pravilnih elektronskih naslovov
- Sporočila naj bodo primerne vsebine in oblike, napisana v **spoštljivem** tonu
- Uporabniki za pošiljanje elektronskih sporočil službene narave v razmerju do naslovnikov **ne** smejo uporabljati lastnih e-poštnih računov (gmail, yahoo...)
- elektronska pošta mora biti podpisana z imenom in priimkom pošiljatelja (avtomatsko)
- Vsako elektronsko sporočilo, ki zapusti omrežje MV, naj bo opremljeno z nogo ki vsebuje pravno obvestilo – izjavo o omejitvi odgovornosti (avtomatsko)

4. UPORABNIŠKE VARNOSTNE POLITIKE

Vse informacije o strankah in poslovanju MV smatrajte zaupne narave. Tako se od uporabnika pričakuje enako ravnanje z zaupnimi informacijami v elektronski obliki

Pri prenosu **zaupnih** podatkov preko elektronske pošte, mora uporabnik uporabljati mehanizme šifriranja, ki omogočajo prebiranje sporočila samo želenim prejemnikom. *Uporabniki elektronske pošte se morajo zavedati, da je kljub skrbi za varnost skrbnikov sistema, elektronska sporočila možno, glede na tehnologijo, posredovati drugim, jo prestrezati, shranjevati in tiskati.*

Priponke

•Priponke se pred prejemom in/ ali pošiljanjem avtomatsko preverjajo s t.i. protivirusnim programom

•Velikost priponke je omejena. Priponke z določenimi končnicami se varnostnih razlogov lahko filtrirajo

4. UPORABNIŠKE VARNOSTNE POLITIKE

Prepovedana uporaba

- Kakršenkoli napad na osebnost naslovnika
- Izmenjavo pornografskih vsebin
- Posredovanje verižnih sporočil (Socialni inžinering – ignoriraj sporočila!)
- Podpiranje rasne, spolne, nacionalne, verske, starostne diskriminacije
- Versko ali politično propagando
- Oglaševanje izdelkov ali storitev v osebnem interesu
- Sodelovanje v igrah na srečo
- Nepooblaščeno posredovanje poslovno občutljivih-zaupnih podatkov
- ....
- Neetične aktivnosti ali vsebine, ki lahko očrnijo profesionalni ugled podjetja

4. UPORABNIŠKE VARNOSTNE POLITIKE

Omejena zasebna raba

- MV dovoljuje omejeno zasebno rabo, vendar le v kolikor to ne ogroža delovnega procesa ali informacijske infrastrukture ter v kolikor ne posega v pravice ostalih uporabnikov
- Zasebna sporočila (domene @mb-vodovod.si) in vse datoteke, povezane z njimi, morajo biti shranjene v mapi "ZASEBNO", ločeno od sporočil, povezanih z izpolnjevanjem delovnih obveznosti
- Velikost zasebne mape v sistemu elektronske pošte ne sme presegati dogovorjenih 5%
- Dovoljena je raba zasebnih elektronskih računov komercialnih ponudnikov (npr. gmail, yahoo, hotmail).

Mapa ZASEBNO < 100MB podatkov!

4. UPORABNIŠKE VARNOSTNE POLITIKE

Zaščita

Na poštnem strežniku se elektronska pošta pregleduje izključno s programsko opremo za odkrivanje zlonamerne programske opreme, prav tako pa se izvaja odstranjevanje izvršljivih in ostalih nevarnih datotek, ki so bile del sporočila (npr. v obliki priponk).

Izvaja se zaščita pred neželenimi elektronskimi sporočili (antispam), ki omejuje pretok (označevanje, filtracija in blokiranje) takšnih sporočil do uporabnikov elektronske pošte.

Vsak uporabnik elektronskega poštnega nabiralnika je dolžan sproti urejati svojo poštno korespondenco. Briše nepotrebne emaile, zasebne premakne v mapo ZASEBNO!

4. UPORABNIŠKE VARNOSTNE POLITIKE

Nadzor

•MV si pridržuje pravico, da v **izjemnih primerih, po vnaprejšnjem obvestilu** uporabnikov, dostopa do, bere, preverja, nadzoruje in kopira vsa elektronska sporočila in datoteke (priponke), ki se nahajajo v informacijskem sistemu družbe.

•MV v nobenem primeru ne bo nadzorovala vsebine elektronskih sporočil in datotek (priponk), ki so **zasebne** narave (mapa ZASEBNO) in jih posamezni uporabniki službene strojne opreme in interneta skladno s to politiko in v omejenem obsegu prejemajo in/ ali pošiljajo v delovnem času prek svojih elektronskih naslovov komercialnih ponudnikov (npr. gmail, yahoo, hotmail, idr.).

4. UPORABNIŠKE VARNOSTNE POLITIKE

Zavedanje: Elektronski naslov je v svetu (Amerika, Azija) tržno blago!

Elektronska pošta je pogosto zlorabljena – trženje, metoda socialnega inženiringa:

•verižna pisma imajo namen doseči čim večjo bazo e-naslovov, za kar vplivajo na naša čustva (otroci, živali, bolni....) – **enostavno jih ignorirajte!**

•Nigerijsko pismo – v polomljenem jeziku (bogat sorodnik, nakazilo na TRR, prijatelj z zadregi,....) **– brišite!**

•Lažna (phising) pošta spletnih storitev, ki od vas zahteva določeno akcijo – klik na link (Amazon, Facebook, Ebay, Paypal, Gmail, Banke...) **– brišite!**

•Oglaševanje izdelkov in vabilo k nakupu (spam) aktualnih izdelkov – **razmislite, kako ste znašli na listi oglaševalca?**

- **Ne naročajte se z službenim e-mailom na tržne storitve (Megabon, Popusti.si, 1nadan... še manj tujih...)!**
- **Ne odpirajte elektronske pošte "sumljivih" pošiljateljev!**

4. UPORABNIŠKE VARNOSTNE POLITIKE

Primeri "Nigerijskih" pisem:

•Spoštovani, res je moje veselje, da napišem to pismo, ki verjamem bo presenečenje za vas,...

•Jaz sem ...,London, tukaj v Angliji. Delam z Santander Bank plc Londonu. Z vsem spoštovanjem ter pri tem upoštevajo, pišem vam iz moje pisarne...

•Jaz sem osebno računovodja do konca gospod Ron Bramlage poslovnež, ameriški državljan, ki na žalost izgubil življenje, so bili njegova žena in štirje otroci ubili...

•Pojav "Phising" emailov slovenskih bank v 2015!

VP 09-03 Politika uporabe interneta

Internet je lahko **učinkovito** poslovno orodje. Informacije na spletu, komunikacije z drugimi podjetji, organi, izobraževanje, ...

Vendar ima tudi **stranske učinke**:

- Pretirana raba interneta zmanjšuje produktivnost
- Neprimerna raba lahko povzroči negativno reklamo ali zakonsko odgovornost
- Povzroča podjetju realne stroške (operater)
- **"Odprtost v svet"** predstavlja informacijsko varnostno tveganje!

4. UPORABNIŠKE VARNOSTNE POLITIKE

Prepovedana uporaba:

- Izmenjava pornografskih , terorističnih, vohunskih vsebin
- Podpiranje kakršnekoli diskriminacije (rasne, spolne, nacionalne, verske, starostne)
- Oglaševanje produktov o osebnem interesu
- Sodelovanje v igrah na srečo
- Osebno okoriščanje
- Razpošiljanje avtorsko zaščitenih vsebin (programskih, multimedijalnih,,.)
- Aktivnosti ki omalovažujejo ugled podjetja MV
- Ostale nezakonite dejavnosti
- ....

4. UPORABNIŠKE VARNOSTNE POLITIKE

Zasebna raba interneta

Internetni dostop, ki ga MV zagotavlja svojim zaposlenim na delovnem mestu, je **namenjen prvenstveno službeni uporabi**.

"Občasna uporaba interneta za zasebne namene je dovoljena v omejenem obsegu, v razumnih mejah in če ni moteča pri izvajanju delovnih nalog in odgovornosti posameznega zaposlenega in njegovih sodelavcev."

Odgovornost uporabnikov

- Upoštevati določila politike
- Minimiziranje nepotrebnega omrežnega prometa
- Ne smejo preobremenjevati omrežja s prenosom velike količine podatkov, za kar so primernejši drugi mediji...

4. UPORABNIŠKE VARNOSTNE POLITIKE

Nadzor

- Vsi dostopi do internetnih strani se beležijo na požarnem zidu in zagotavljajo revizijsko sled. Na požarnem zidu je konfigurirana lista dovoljenih oziroma prepovedanih naslovov spletnih strani....
- V kolikor bo MV ugotovila dostope do interneta za namene, ki so s to politiko prepovedani, bo s tehničnimi sredstvi preprečila dostop do teh strani oz. preprečila kakršnokoli drugačno prepovedano aktivnost...
- MV je zavezan spoštovanju zasebnosti na delovnem mestu. Do vsebine lahko dostopa zgolj v izrednih primerih pod posebnimi pogoji skladno z določili politike – vnaprejšnje obvestilo uporabnika....
- MV upoštevala načela sorazmernosti, zakonitosti in ustavne dopustnosti....

4. UPORABNIŠKE VARNOSTNE POLITIKE

Primer nevarne uporabe: lovljenje (phishing) osebnih podatkov:

•Pri brskanju naletite na linke za spletne storitve (Facebook, Twitter, Dropbox, Google mail-drive, Youtube...), ki zahtevajo vnos osebnih podatkov ali uporabniškega imena in gesla – **NE KLIKNI!**

•Takšni linki so pogosto priponke elektronski pošti, ki jo lahko dobite na službeni ali zasebni poštni predal.

Koristite ročni vpis https://naslov !

Zavedajte se, da vsako stran, ki jo obiščete pustite za seboj digitalno sled (IP, domeno – MB-vodovod.si, tip računalnika in operacijskega sistema, vrsta brskljalnika,....) ... S tem odkrijete od kod ste tudi georafsko, možne ranljivosti sistema, lahko pa odkrijete celo svoje osebne podatke shranjene v medpomnilniku...

4. UPORABNIŠKE VARNOSTNE POLITIKE

Facebook <update+jcifslrlygdh@excite.it>
To:
Reply-To: noreply <noreply@excite.it>
Confirm your account on Facebook

facebook

Hi [redacted]@gmail.com,

You joined Facebook, but you still haven't confirmed your accou

To confirm, simply follow this link:
http://www.facebook.com/n/?confirmemail.php&e=rado.infolog%40gmail.com&c=9796686&r1bab9C1A0AB7bfe8Dc8120033A2D&code=9796686&n_m=rad%40gmail.com

And that's it! Once you do this, you'll have access to all of Faceb features.

Important: After today, you'll be unable to log in to your Facebo account until you complete this step.

You may be asked to enter this confirmation code: 9796686

Again, welcome!

Thanks,
The Facebook Team

This message was sent to [redacted]@gmail.com. If you don't want to receive these emails from Facebook in the future, please click: unsubscribe.
Facebook, Inc. Attention: Department 415 P.O Box 10005 Palo Alto CA 94303

YouTube

YouTube Safety Center has sent you a message

You can reply to this message by visiting your inbox.

To: [redacted]@gmail.com

We need your participation in representing your information correctly and completely.
Get more details

Help center Email options Report spam Unsubscribe

©2012 YouTube, LLC 901 Cherry Ave, San Bruno, CA 94066

VP-05-02 Politika uporabe gesel

Pomen gesla

Uporniško ime/geslo – identifikacija/avtentifikacija – osebna izk./fotografija

Geslo je edini način, da nas računalnik (sistem, storitev...) prepozna!

✓ Uporabniško ime se generira po nekem ključu – je lahko delno javno

✓ **Geslo – storogo zaupno, namenjeno zgolj lastniku računa!**

“Study: 73% Use Bank Password Everywhere” !

Posebno pozornost namenimo izbiri gesla!

Različna gesla za različne račune, službene, zasebne...!

4. UPORABNIŠKE VARNOSTNE POLITIKE

Statistika najslabših gesel:

1) password
2) 123456
3) 12345678
4) qwertz
5) abc123
6) ...imena, priimki, ljubljenčki, hobiji**, zaposlitev**, naj knjige-filmi...

...**podatki, ki jih pogosto razkrivamo o sebi na družabnih omrežjih**

Sistemi (os.rač.) za avtomatsko generiranje "Brut force" so sposobni zadeti 8 znakovno geslo v manj kot 30 min, ob pomoči osebnih podatkov pa je slabo geslo stvar minute!

Nikoli ne uporabljajmo istih gesel za zasebne in službene račune (domena, OWA)!

4. UPORABNIŠKE VARNOSTNE POLITIKE

Izbira uporabniškega gesla

1) Pravilo v Mariborskem vodovodu:

2) vsaj 8 znakov

- velike in male črke
- številke in posebne znake (. , ! ? « # $ & (/) = * + , ipd),

2) Nikoli naj ne vsebuje:

- izpeljank uporabniškega imena
- logičnih številk (telefonska, registrska,..)
- nizov znakov (123456..,qwertz.., asdfgh..)
- imena, priimka, družinskih članov, rojstnih datumov...
- enakih številk ali črk (11111111, zzzzzzzzz,...).

Nikoli ga ne zapisujmo na listek! Telefon? Kako si sedaj takšno zahtevno geslo zapomniti? Težko?

4. UPORABNIŠKE VARNOSTNE POLITIKE

Primeri dobrega gesla

...naj temelji na osebni izkušnji, (samo), recimo:

"**N**a **R**oblek **b**om **o**dšel **b**om **l**jubco..." pesem iz l.1998 -> **NRbobl98?**

"**M**oj **n**ajljubši **h**obi **j**e **k**olesarjenje" 20**14** -> **Mnhjk14!**

"**N**ajtežji **i**zpit **n**a **f**axu **j**e **b**il **O**snove **e**lektrotehnike" – 2000 -> **NinfjbOe00!**

"**V s**lužbo **n**a **MV r**es **r**ad **h**odim" -2001 -> **VsnMVrrh01**

Podjetje ima formaliziran-avtomatiziran postopek upravljanja z gesli:

•Izdajanje inicialnega gesla, ki zahteva zamenjavo

•Sprememba gesla - ciklično

•Veljavnost in kvaliteta gesla - pravilo

4. UPORABNIŠKE VARNOSTNE POLITIKE

NE ZAPISUJEMO !

4. UPORABNIŠKE VARNOSTNE POLITIKE

Kvaliteto vašega gesla lahko preverite na:

https://howsecureismypassword.net

Poskušajte z vnašanjem posebnih znakov. Seveda nikoli ne vstavite originalnega gesla, ampak podobno!

VP-06-01 Politika zaščite pred zlonamerno prog.opr.

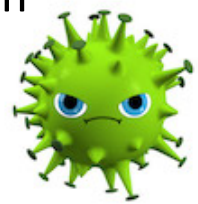
(ponovitev vsega kar smo danes slišali)

Vsi uporabniki informacijskih storitev so seznanjeni s priporočenimi postopki za preprečevanje in odkrivanje zlonamerne programske opreme.

Služba za informatiko skrbi za zaščito tehničnimi sredstvi.

Uporabnikom se priporoča:

- Nikoli ne odpirajo kakršnih koli datotek k elektronski pošti neznanega, sumljivega pošiljatelja ali vira, ki mu ne zaupajo. Ta sporočila naj takoj izbrišejo ter »ponovno« izpraznijo koš.
- Izbrišejo SPAM, verižna in ostala nezaželena sporocila.
- Nikoli naj ne snemajo datotek iz neznanih ali sumljivih virov.
- Izogibajo naj se direktni skupni uporabi diskov z bralno/zapisovalnim dostopom – tudi oblačnim storitvam (Google disk, Dropbox, MS,..)



4. UPORABNIŠKE VARNOSTNE POLITIKE

- Medije (CD, DVD, USB) pred uporabo naj vedno preiščejo s protivirusnim programom.
- Redno naj izdelujejo varnostne kopije pomembnih podatkov ter jih shranjujejo na varna mesta skladno s politiko primerne rabe.

Pomoč:

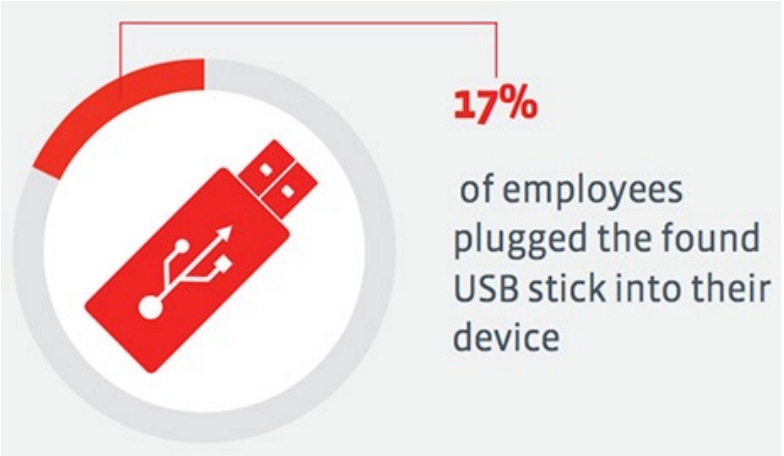
- Nejasnosti- kakršna koli vprašanja vezana na informacijsko varnost
- Poročanje o varnostnih incidentih ali sumljivih okoliščinah (zloraba gesla, sum na virus, vsiljiva e-pošta,...)

na elektronski naslov it.podpora@mb-vodovod.si !

4. UPORABNIŠKE VARNOSTNE POLITIKE

Top 5 virov zlonamerne kode (virusov):

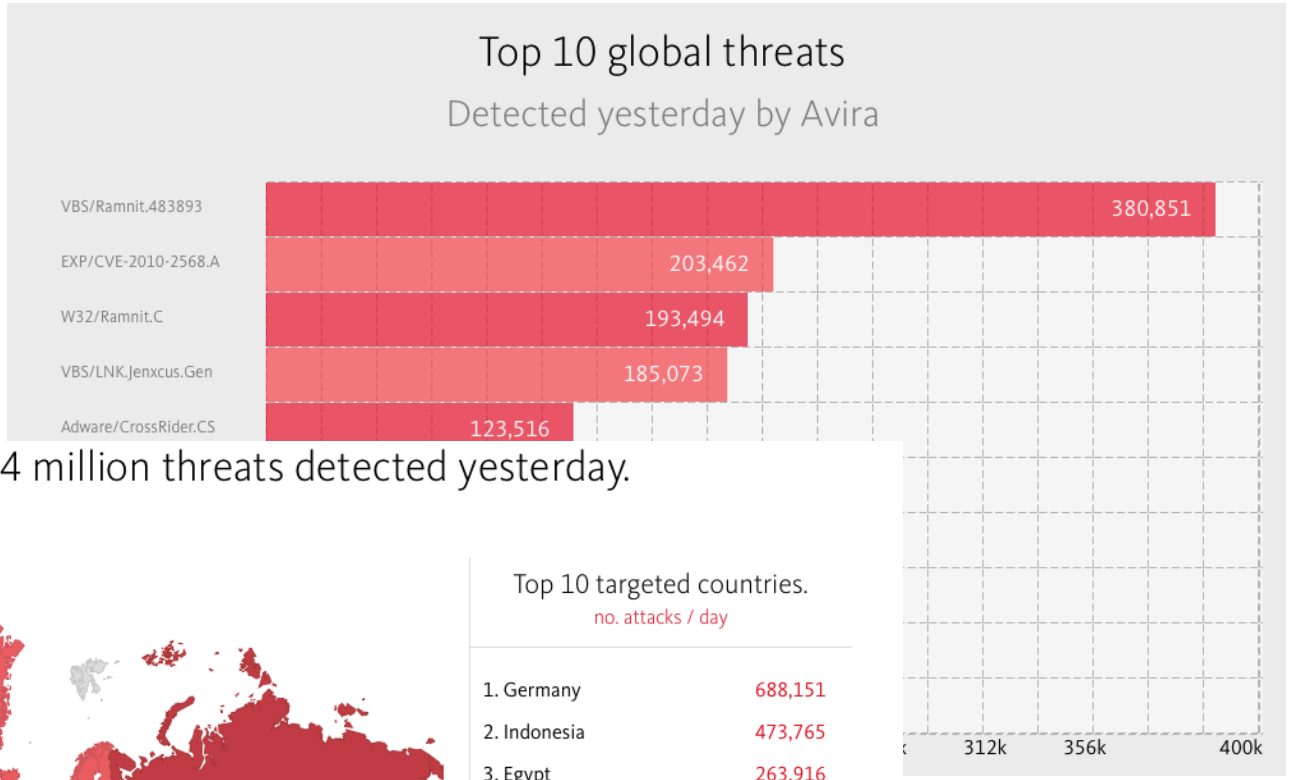
1) Preneseni programi
2) Ne licenčna prog. oprema
3) Email priponke
4) Internet
5) CD, USB



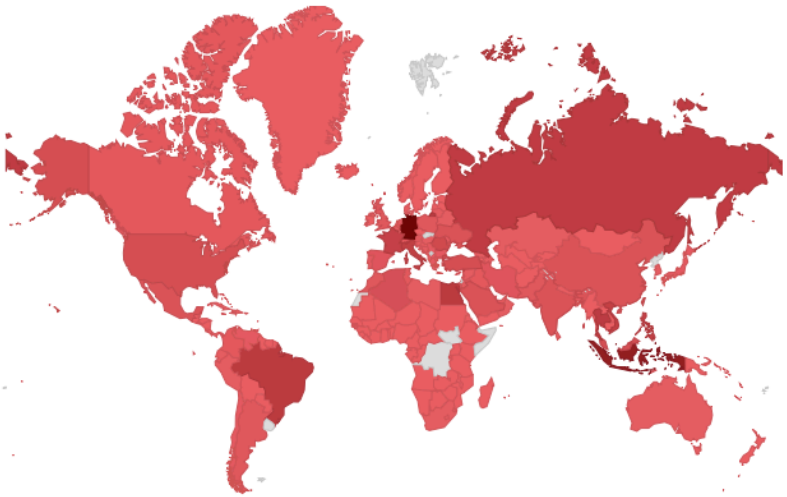
Simptomi:

1) Neodzivnost, počasnost
2) Počasen zagon
3) Ustavljanje oz. sesuvanje
4) Manjkajoče datoteke
5) Nedostopnost diska
6) Neznane datoteke
7) Težave s tiskanjem
8) Neobičajna sporočila - napake

4. UPORABNIŠKE VARNOSTNE POLITIKE



Over 5.4 million threats detected yesterday.



Top 10 targeted countries.
no. attacks / day

1. Germany	688,151
2. Indonesia	473,765
3. Egypt	263,916
4. Brazil	247,119
5. Thailand	238,541
6. Russian Federation	235,132
7. Italy	220,890
8. Vietnam	209,189
9. France	206,395
10. Philippines	196,263

22.11.2015, vir: https://www.avira.com/en/threats-landscape

4. UPORABNIŠKE VARNOSTNE POLITIKE

VP-07-03 Mobilne naprave

Vohun v vašem žepu: "On je vedno z vami. Zjutraj ve, kdaj se zbudite. Zvečer ve, kdaj greste spat. Čez dan ve, s kom se pogovarjate, kam greste, kaj berete, kaj poslušate. Pred njim nimate skrivnosti, pozna vse vaše zmenke, obljube in laži." Ja vaš pametni telefon:

- **GPS** – spremlja vašo lokacijo
- **Photo** – beleži vaša doživetja
- **WWW** – za vas spremlja dnevne novičke, opravlja nakupe
- **Facebook** – pozna vaše prijatelje
- **LinkedIn** – povezuje vas s poslovni partnerji
- **Email** – posreduje službene dokumete

Najlepše: Vse opravljate sami, oglaševalcem sporočate kaj vam je všeč, multinacionalkam kaj vas zanima... Morda še komu tretjemu pošiljate lokacijo, vsebino kratkih sporočil ali pa kar **službene podatke**...

Vedno zaklenjen, kriptirane informacije, pozor pri Wifi povezavah, Aplikacije!

VP 07-04 Politika oddaljenega dostopa

DOMAČI RAČUNALNIK – preteča nevarnost

Vsi, ki ga uporabljate za delo od doma, e-pošta, odpiranje istih datotek na USB ključih, ali preko spletnih servisov Dropbox, google drive, SkyDrive...

Domači računalnik običajno uporablja več družinskih članov, katerih obnašanje je različno tvegano... Nekaj navodil:

- Vedno uporabljajte požarno pregrado tako na usmerjevlniku, kakor tudi računalniku
- Uporabljajte posodobljene antivirusne zaščite (rec. Avira)
- Uporabljajte zgolj licenčno programsko opremo – redne posodobitve
- Ne obiskujte tveganih spletnih strani (**torent, mp3, filmi, xxx**, ...) – izredno agresivne!
- **Gesla!!!** (različna, kompleksna, redna menjava)

Zasebno obnašanje lahko vpliva na varnost informacijskega sistema MV!

Dodatna gradiva:

http://www.cert.si/varnostne-groznje.html

http://www.cert.si/zascita.html

http://www.safe.si/

http://www.e-demokracija.si/cryptoparty/category/cryptonasvet/

ABC varnosti na spletu:

https://www.varninainternetu.si/2011/vse-kar-morate-vedeti-o-spletni-varnosti-na-enem-mestu/

Geslo je kot zobna ščetka:

https://www.varninainternetu.si/2011/geslo-je-kot-zobna-scetka/