“Informācijas drošības izpratnes programma” darbinieku vispārējā apmācība

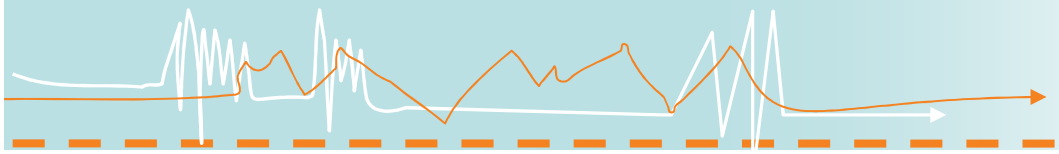
Latvijas Republikas satiksmes ministrija, Rīga, 2014.gada 8.aprīlis.

Egils Stūrmanis

Prezentācija izveidota sadarbojoties DEG un CERT.LV.

Saturs

- Ievads
- Tiesiskais regulējums
- Internets skaitļos
- Drošības jēdziens un teorija
- Informācijas aizsardzība ikdienā
- Datoru ētika
- Biroja ētika
- Sociālā inženierija
- Sabiedrības izglītošana
- Rīcība drošības incidenta un pārkāpumu gadījumos



CERT.LV

Ievads

Informācijas sabiedrības veidošanās

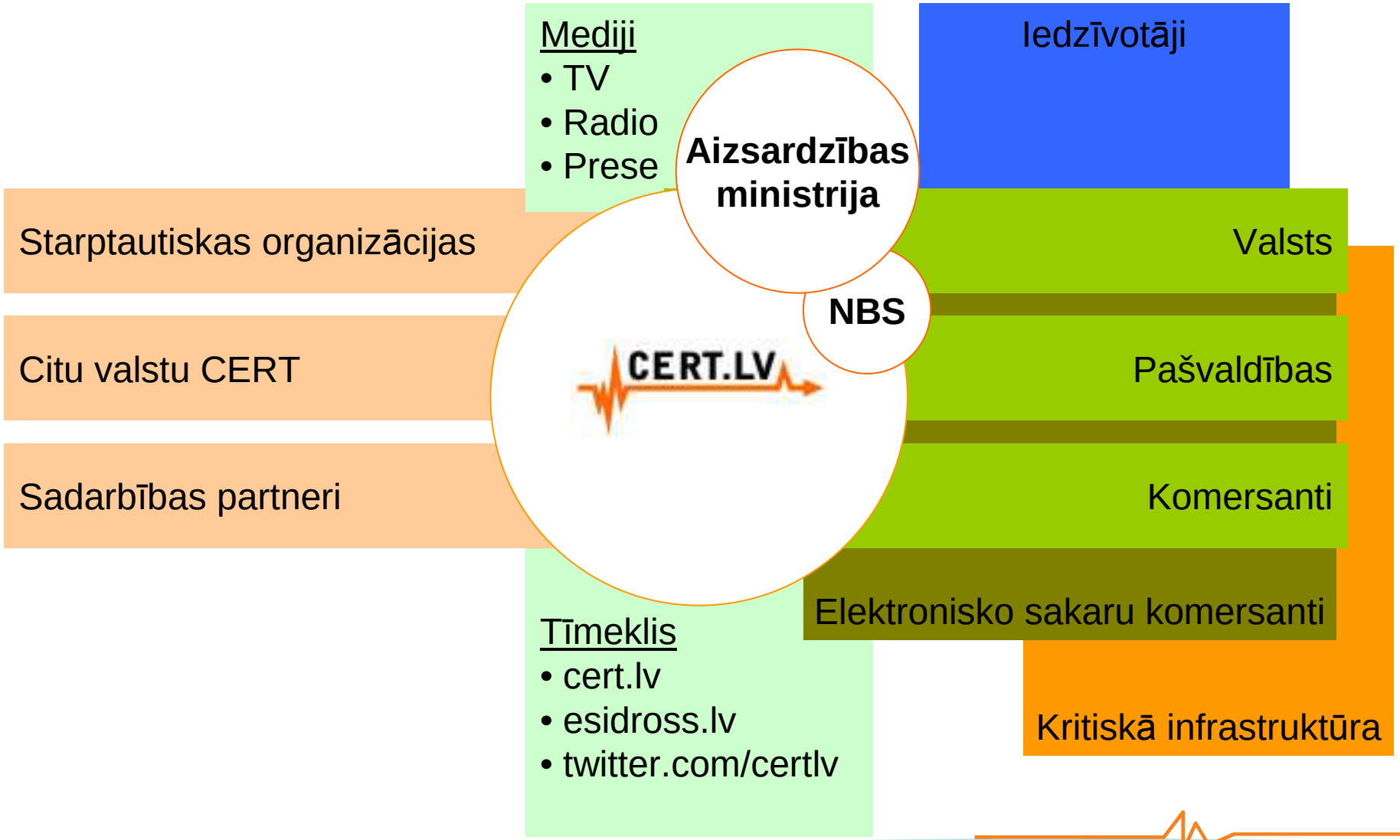
- Sabiedrības “internetizācija”.
- Indivīds informācijas sabiedrībā.
- Privātuma apdraudējums – arvien būtiskāks drauds personīgajai drošībai.
- Zināšanas par to, kā aizsargāt informāciju par sevi, veicina personīgo drošību.
- Darbinieku zināšanas par to, kā aizsargāt iestādes informāciju, veicina iestādes drošību.

Tiesiskais regulējums

CERT.LV

- Darbojas saskaņā ar “Informācijas tehnoloģiju drošības likumu” kopš 2011.gada 1.februāra.
- Darbības uzdevumi un tiesības tiek deleģētas Latvijas Universitātes aģentūrai “Latvijas Universitātes Matemātikas un informātikas institūts”.
- Finansēta no valsts budžeta.
- Visi pakalpojumi ir bezmaksas.
- **Misija: “Veicināt IT drošību Latvijā”.**
- **Virzība: “IT drošības kompetences centrs Latvijā”**

CERT.LV sadarbības partneri



Tiesiskais regulējums Latvijas Republikā

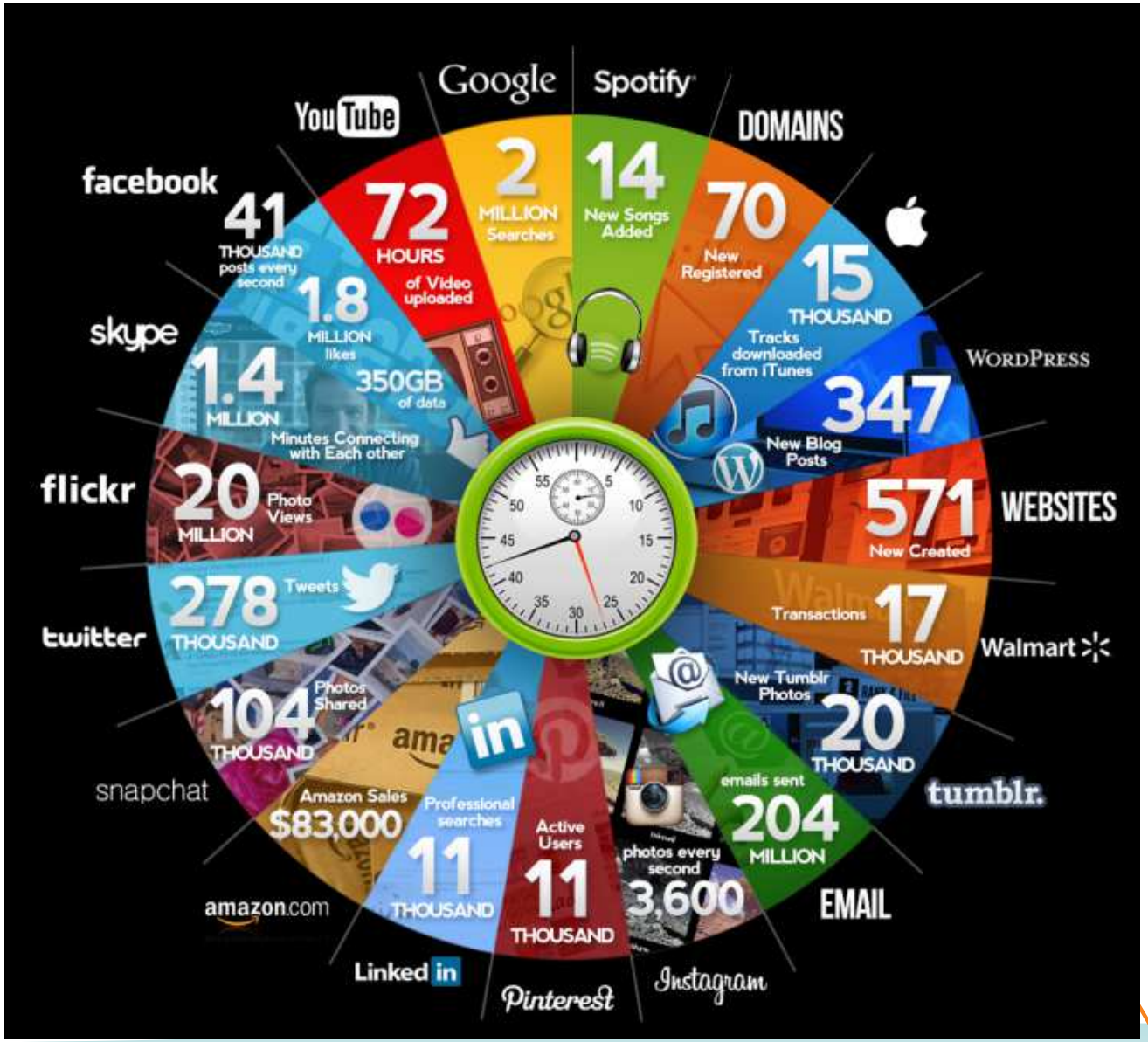
- Latvijas Republikas Satversmes 96.pants;
  - "Ikvienam ir tiesības uz privātās dzīves, mājokļa un korespondences neaizskaramību."
- Likumi
  - Fizisko personu datu aizsardzības likums;
  - Valsts informācijas sistēmu likums;
  - Informācijas atklātības likums;
  - Informācijas sabiedrības pakalpojumu likums;
  - **Informācijas tehnoloģiju drošības likums.**

IT drošības likums

- Pieņemts Saeimā 2010.gada 28.oktobrī,
- Stājas spēkā 2011.gada 1.februārī,
- Nosaka CERT.LV izveides kārtību,
- Nosaka kārtību kā valsts un pašvaldību institūcijās jāorganizē IT drošības pārvaldība,
- Pamatojoties uz likumu izstrādāti MK noteikumi par:
  - Kritiskās infrastruktūras drošības pasākumu plānošanu (spēkā no 2011.gada 1.februāra),
  - Elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanu (spēkā no 2011.gada 1.maija).
- Nosaka Nacionālās informācijas tehnoloģiju drošības padomes izveidi.

Internets skaitļos

Mūsdienu pasaule 60 sekundēs



Interesanta statistika 2012.gads

Pasaulē saskaņā ar Pingdom datiem

- 2,4 miljardi interneta lietotāju
- 4,3 miljardi e-pasta adrešu, 2,2 miljardi lietotāji
- 68% datu plūsmas – mēstules
- 0,22% e-pastu – ļaundabīgi
- 634 miljoni tīmekļa vietņu
- 2,4 miljardi sociālo tīklu kontu, 1 miljards aktīvu Facebook lietotāju
- 6,7 miljardi mobilo telefonu numuru, 1,1miljards - viedtālruņi

Eiropā

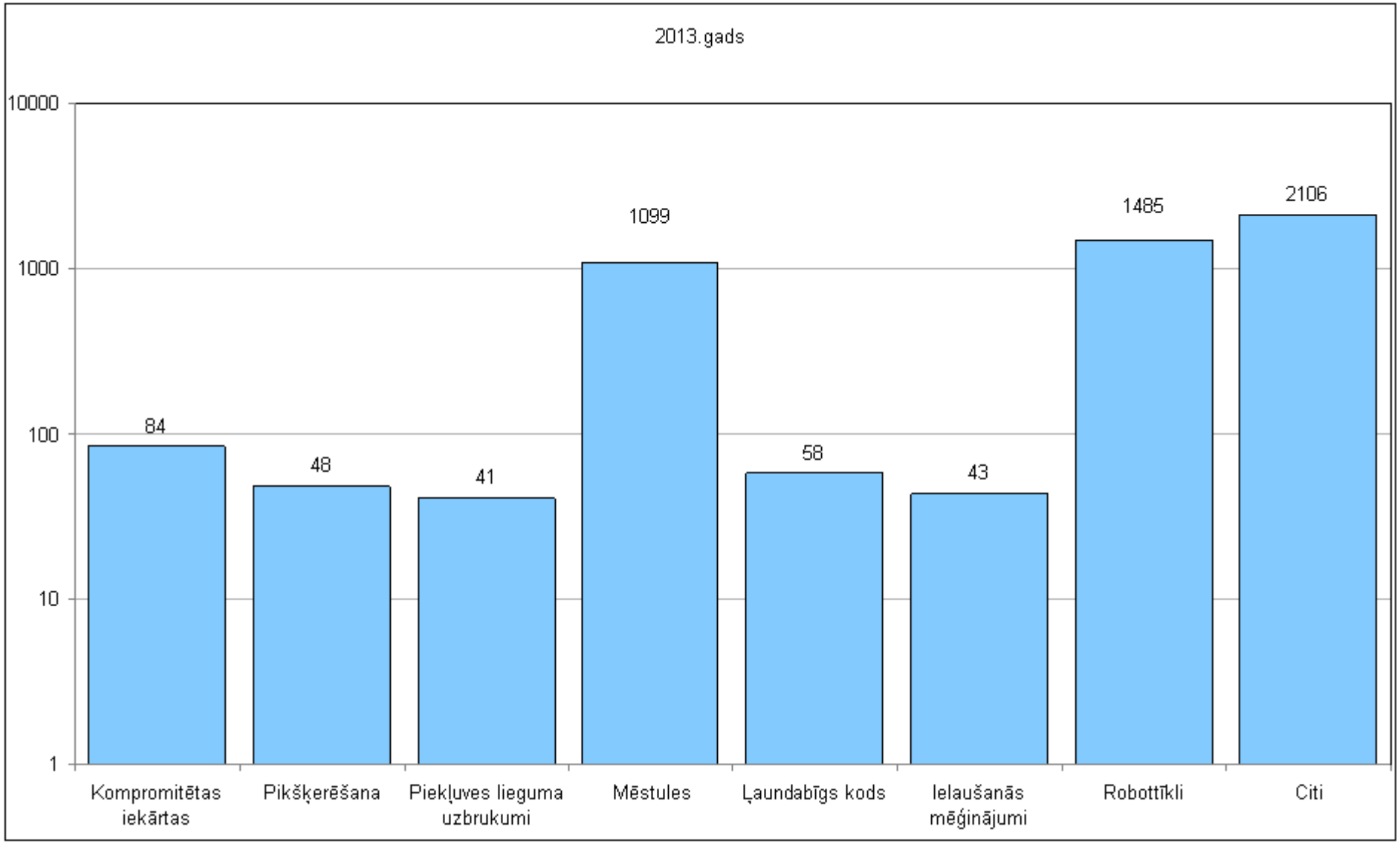
- 518 miljoni (~63%) cilvēku lieto Internetu

Latvijā

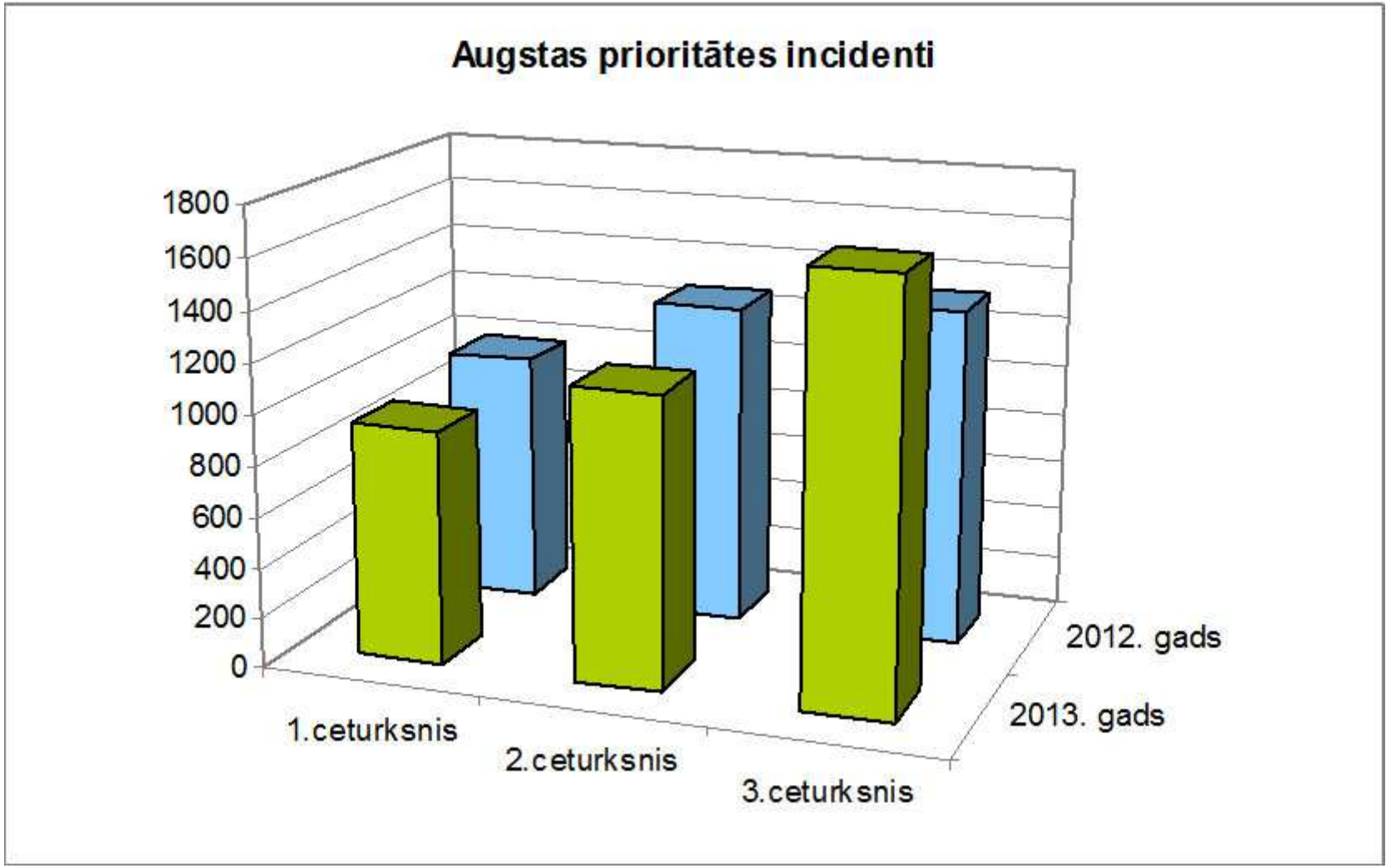
- 71 % iedzīvotāju lieto Internetu
- 1,2 miljoniem (~58%) iedzīvotājiem ir konts draugiem.lv
- 350 tūkstošiem (~17%) iedzīvotājiem ir konts facebook

http://royal.pingdom.com/2012/01/17/internet-2011-in-numbers/

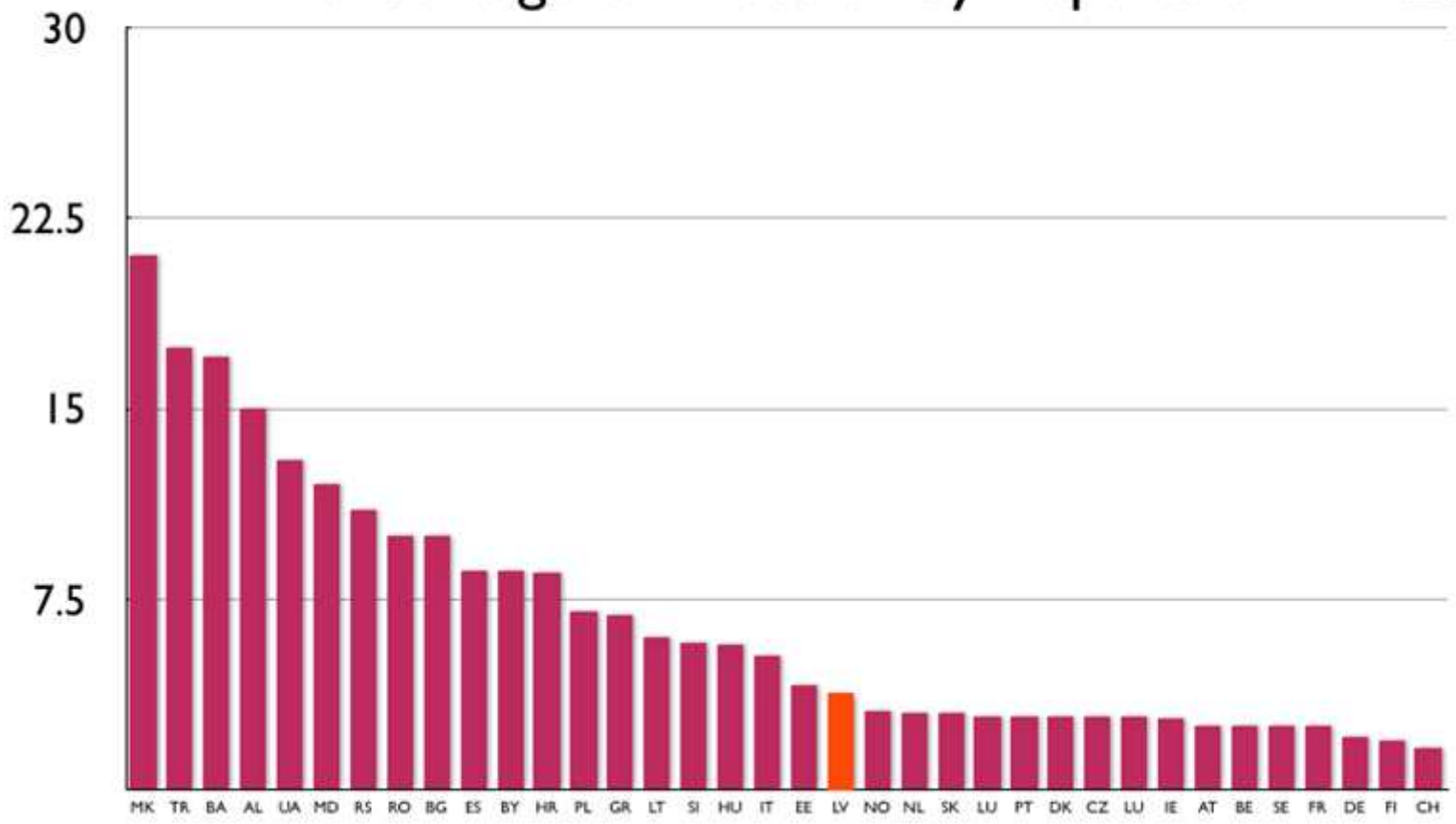
Datorvīrusi un ļaunprātīga koda programmas



Augstas prioritātes incidentu dinamika



Team CYMRU pētījums



Drošības jēdziens un teorija

Drošības jēdziens

- **Drošība:**
  - Apstākļi, kuros kaut kas (vai kāds) nav apdraudēts, pakļauts briesmām;
  - Kaut kas (vai kāds) ir aizsargāts pret nejaušībām, kļūmēm, bojājumiem;
  - Kāds, kurš ir uzticams, drošs un uz ko var paļauties.

- **Drošība** - psihoemocionāls (subjektīvs) stāvoklis, kurā eksistē drošības sajūta, ka nekas mūs neapdraud.

- Parasti **drošība** ir iespējama, pastāvot zināmiem nosacījumiem:
  - Ir apzināti iespējamie draudi un drošības riski;
  - Ir novērtēti drošības riski un to potenciālā ietekme;
  - Ir veikti drošības pasākumi (konkrētas darbības draudu un/vai risku mazināšanai).

Informācijas jēdziens

- **Informācija** = dati + zināšanas;
- **Informācija** - iestādes īpašums - tās nemateriālie aktīvi;
- **Informācija** ir tāds iestādei piederošo nemateriālo aktīvu veids, kuru sagrozīšana, sabojāšana vai iznīcināšana var radīt zaudējumus ne tikai pašai iestādei, bet arī informācijas sniedzējam un saņēmējam.

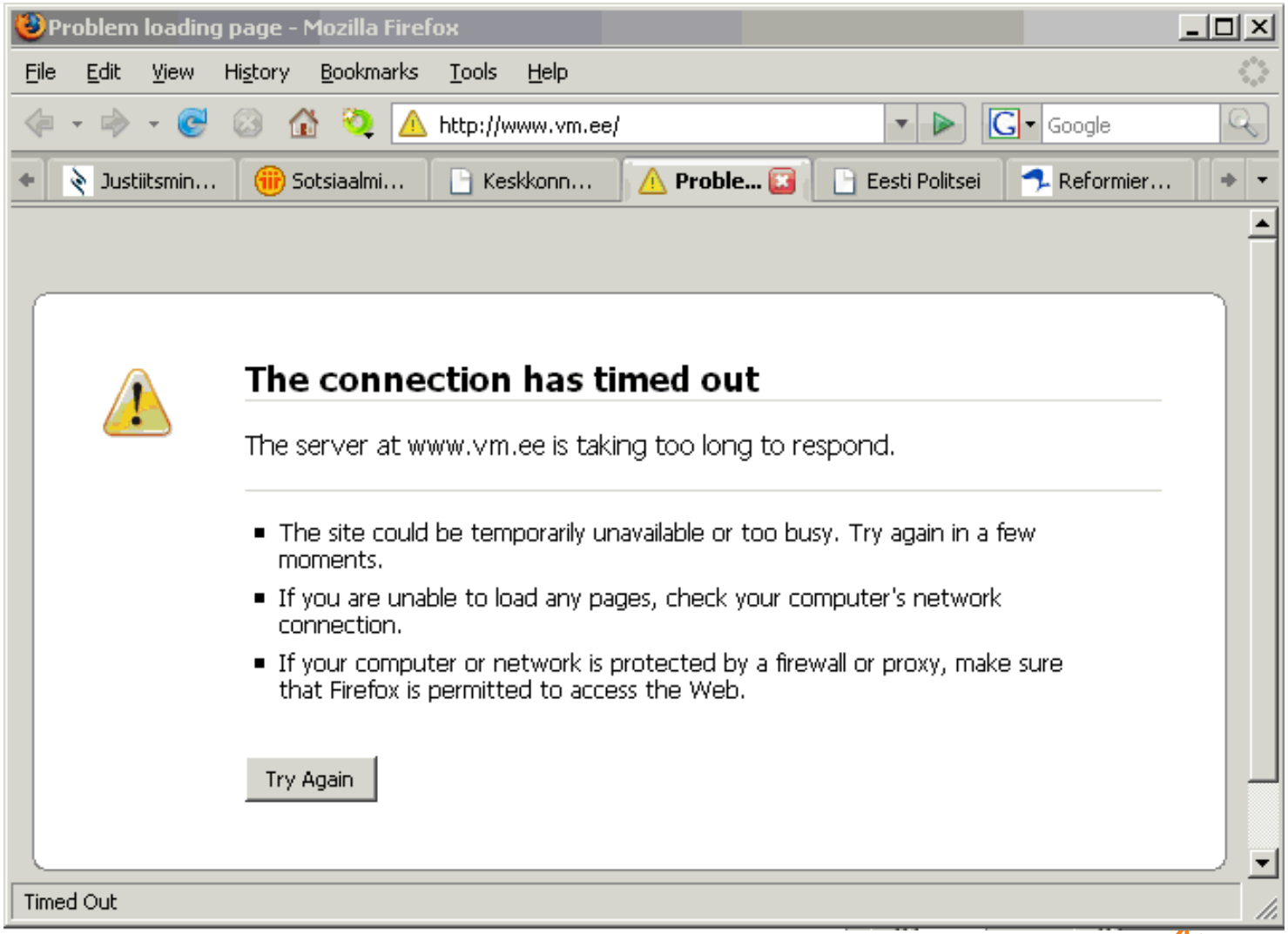
Informācijas drošība

- Informācijas drošība nozīmē informācijas un informācijas sistēmu aizsargāšanu no **neautorizētas piekļuves, izmantošanas, publiskošanas, tās pieejamības traucēšanas, pārveidošanas vai iznīcināšanas.**
- Informācijas drošības galvenais mērķis: aizsargāt un nodrošināt informācijas konfidencialitāti, integritāti un pieejamību.
  - Informācijas integritāte – raksturo, cik lielā mērā informācija ir pilnīga, patiesa, precīza un aktuāla;
  - Informācijas pieejamība – raksturo to, vai lietotāji var piekļūt nepieciešamajai informācijai ne vēlāk kā noteiktā laikā pēc informācijas pieprasīšanas brīža;
  - Informācijas konfidencialitāte– raksturo to, cik lielā mērā informācija ir pieejama tikai šīs informācijas saņemšanai paredzētajiem lietotājiem.
- Informācijas drošība ir iespējama, vienīgi pastāvot noteiktiem nosacījumiem un tās aizsardzības nodrošināšanai izvēlētai metodikai.

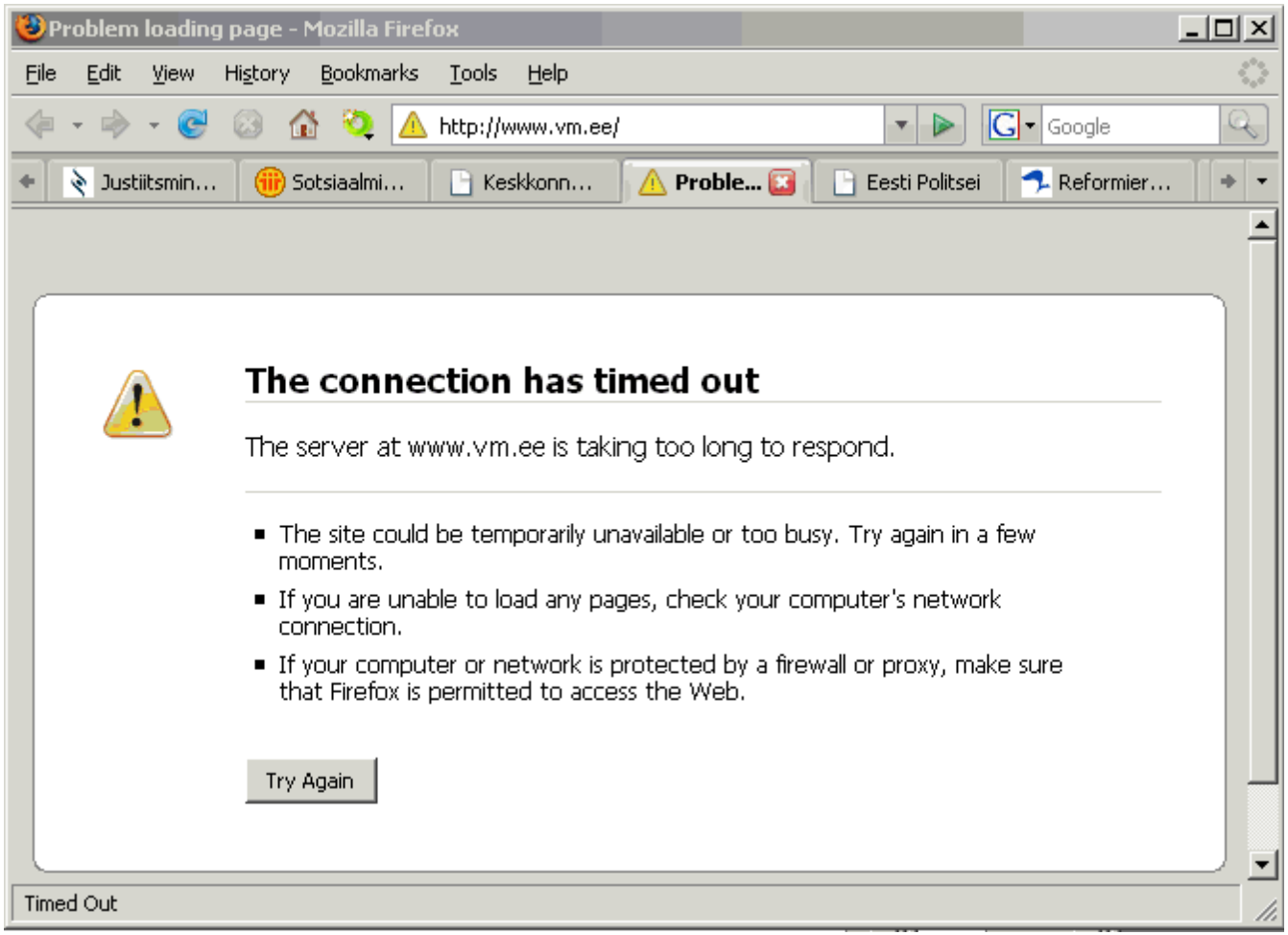
Integritātes izjaukšana - dezinformācija

Konfidencialitātes izjaukšana – informācijas noplūde

Pieejamības izjaukšana – nav pakalpojuma



Informācijas tehnoloģiju uzbrukumu ieroči - Igaunijas gadījums

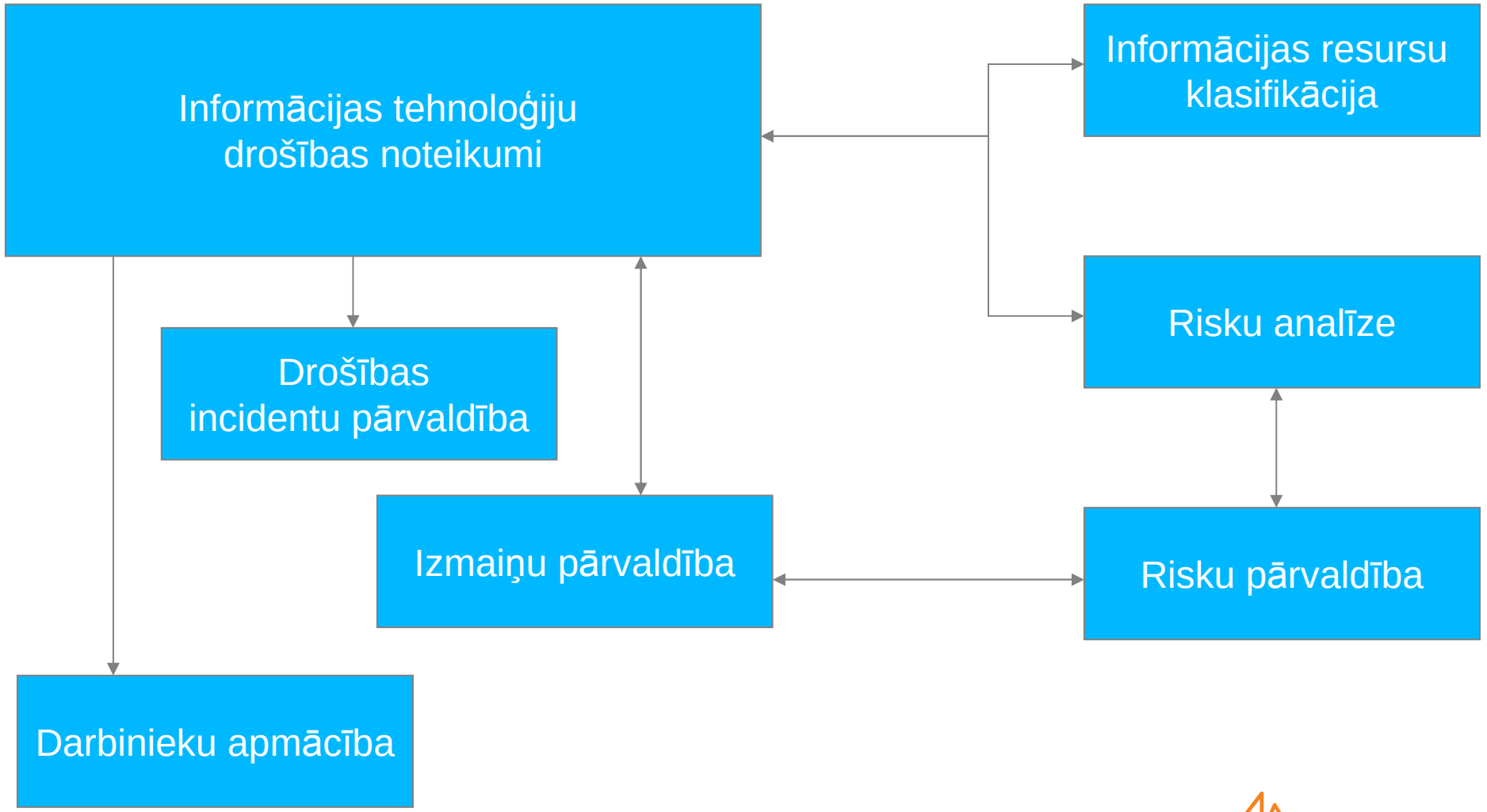


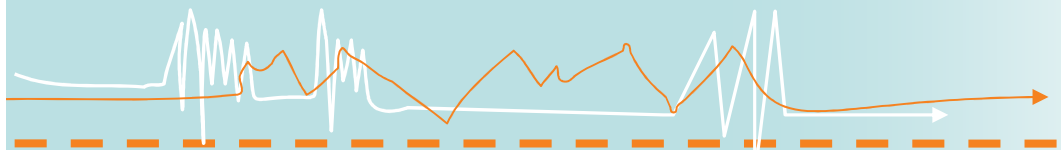
Avots: F-Secure http://www.f-secure.com/weblog/archives/archive-042007.html

Informācijas drošības noteikumu mērķi

- Apliecināt iestādes vadības apņemšanos nodrošināt iestādē resursu drošību, lai nodrošinātu to integritāti, pieejamību un konfidencialitāti;
- Nodrošināt iestādē vienādu un sistemātisku pieeju informācijas tehnoloģiju drošības jautājumu risināšanā;
- Panākt iestādes darbinieku izpratni par nepieciešamajiem informācijas tehnoloģiju drošības jautājumiem;
- Būt par pamatu nepieciešamo procedūru, instrukciju un citu nepieciešamo drošības dokumentu izstrādē un ieviešanā.

Informācijas tehnoloģiju drošības pārvaldība iestādē





CERT.LV

Informācijas aizsardzība ikdienā

Autentifikācija

- Autentifikācija ir process, kurā veic lietotāja identitātes pārbaudi datorsistēmā.

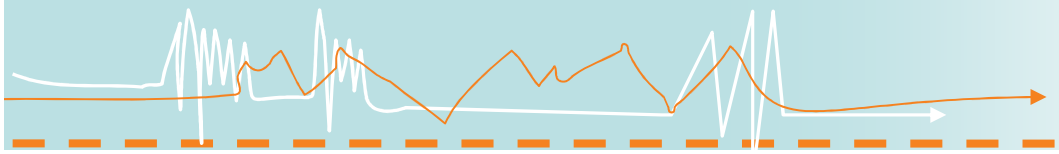
- Autentifikācijas veidus var iedalīt vairākās kategorijās:
  - Lietotājs kaut ko zina (piem., paroli vai personālo identifikācijas numuru - PIN);
  - Lietotājam kaut kas pieder (piem., magnētiskā karte, viedkarte u.c.);
  - Lietotājam kaut kas ir - pamatojoties uz lietotāja biometriskajām īpašībām (piem., balss, pirkstu nospiedumiem, paraksta atpazīšanas u.c.)

- Pēc autentifikācijas parasti notiek autorizācija - lietotāja piekļuves (sistēmas resursiem, informācijai) tiesību piešķiršana.

Pareiza paroles izvēle

- **Labā prakse:**
  - lietotāja parole sastāv no lielo un mazo latīņu alfabēta burtu un ciparu kombinācijas, un tās garums nedrīkst būt īsāks par astoņiem simboliem. Kā paroli nedrīkst izmantot personu identificējošus datus (piemēram, lietotāja vārdu, uzvārdu, automašīnas numuru) un vārdus, kas saistīti ar organizāciju vai kas bieži tiek lietoti ikdienas darbā,
  - mainīt paroli reizi X mēnešos,
  - neizmantot iepriekšējās 2 paroles,
  - dažādiem resursiem lietot atšķirīgas paroles

- **Piemērs:**
  - sliktas paroles – Kaarlis2 Sanita09 CERT2011g
  - ieteicamas paroles – 3Kotaz@s HL36b87m p3y6trEY



CERT.LV

Datoru ētika

Datoru tiesiska lietošana

- **Labā prakse – lietotājam nav atļauts:**
  - Veikt darbības, kas nevajadzīgi noslogo informācijas resursus, neņemot vērā citu lietotāju vajadzības (piemēram, saglabāt un drukāt nevajadzīgi daudz dokumentu kopiju, atstāt atvērtas datortīkla koplietošanas resursos glabājamās datnes, kuras tobrīd darbam nav nepieciešamas, u.c.);
  - Veikt internetā pieejamo datorprogrammu lejupielādi un instalāciju, nesaskaņojot ar IT administratoru;
  - Veikt internetā pieejamu, liela izmēra multimediju datņu (piemēram, mūzika, filmas, attēli, datorspēles) lejupielādi;
  - Patvaļīgi instalēt datorprogrammas vai mainīt programmu uzstādījumus;
  - Nesaskaņojot ar vadību, pieslēgt organizācijas lokālajam datortīklam vai tā informācijas resursiem personīgo datortehniku (piemēram, darbstacijas, konsoles, portatīvos vai plaukstdatorus, mobilās ierīces, bezvadu maršrutētājus, skenerus, drukātājus, u.c.).

- **Svarīgi atcerēties:**
  - Dators darbā ir ‘darba instruments’ un paredzēts darba pienākumu veikšanai.

Uzbrucēji virtuālajā vidē (1)

- **Mērķi - iestādes:**
  - Klientu informācija,
  - Finansiālā, maksājumu informācija,
  - Informācija par darbiniekiem
  - Ar valsts pārvaldi saistītie, ierobežotas pieejamības un slepeni dokumenti.
- **Uzbrucēju komunikāciju veidi:**
  - Personīgi kontakti,
  - Telefons,
  - Elektroniskais pasts,
  - Ļaundabīgas programmas.
- **Minimālā aizsardzības stratēģija:**
  - Labākā aizsardzība – saprātīga rīcība,
  - Datu kriptēšana (šifrēšana).
  - Darbinieku personīgo ierīču (BYOD) lietošanas regulējums,
  - Gatavība mērķētiem uzbrukumiem,
  - Darbinieku izglītošana.

Uzbrucēji virtuālajā vidē (2)

- **Mērķi - privātpersonas:**
  - Finansiālās informācija,
  - Identitātes zādzība,
  - Datoru resursu iegūšana,
  - Informācijas zagšana un viltošana,
  - Šantāža, nomelnošana.
- **Uzbrucēju komunikāciju veidi:**
  - Personīgi kontakti,
  - Telefons,
  - Elektroniskais pasts,
  - Ļaundabīgas programmas.
- **Minimālā aizsardzības stratēģija:**
  - Labākā aizsardzība – saprātīga rīcība,
  - Stingra paroļu izveidošanas un glabāšanas kārtība,
  - Zināšanas, kā un kam paziņot, ja noticis kas slikts.

Zibatmiņas

- **Zibatmiņa:**
  - Plaši pieejama un ērti lietojama,
  - Izmanto datu apmaiņai starp daudziem datoriem,
  - Viegli pazaudējama,
  - Viegli inficēt ar ļaundabīgu kodu (vīrusiem utt.).

- **Labā prakse:**
  - Pievienojot datoram ārējo datu nesēju to noskanēt ar antivīrusu programmu,
  - Ar īpašu piesardzību lietot ārējos datu nesējus, kurus iedevuši draugi un paziņas,
  - Neglabāt, bez vajadzības, svarīgu un aizsargājumu informāciju.

Viedtālruņi

- **Viedtālrunis** - miniatūrs dators, kurš spēj:
  - pieslēgties bezvadu internetam,
    - aplūkot tīmekļa vietnes, tajā skaitā sociālos tīklus,
    - apmainīties ar elektronisko pastu,
    - fotografēt un filmēt,
    - automātiski apmainīties ar datiem ar pakalpojuma sniedzēju.
  - noteikt atrašanās vietu,
  - kalpot kā datu nesējs,
  - būt radiouztvērējs un mūzikas/video atskaņotājs,
  - ... un visbeidzot spēj pildīt arī telefona funkcijas.

- **Labā prakse:**
  - izmantot tikai tās iespējas, kuras dotajā brīdī nepieciešamas,
  - neinstalēt apšaubāmas izcelsmes programmas,
  - neglabāt tālrunī banku karšu numurus un pin kodus, citu svarīgu un aizsargājamu informāciju.

Droša elektroniskā pasta lietošana (1)

- **Kad jākļūst uzmanīgam?**
  - Jūs saņemat sensacionāla rakstura paziņojums ar uzaicinājumu veikt zināmas darbības;
  - Interneta pārlūkprogramma rāda pieprasījumu nezināmas lietojumprogrammas palaišanai;
  - Saņemts uzaicinājums apmeklēt nezināmu tīmekļa vietni;
  - Jūs saņemat ziņojumu valodā, kuru ikdienas sarakstē nelietojat;
  - Jūs sākat saņemt dīvainas ziņas no draugiem un paziņām;
  - Draugi un paziņas sāk saņemt dīvainas ziņas no Jums.

- **Labā prakse:**
  - Izdzēst nevajadzīgu/ nelūgtu reklāmu – piedāvājumus,
  - Nevērt vaļā saites, kuras satur elektroniskais pasts no nezināmu/apšaubāma sūtītāja,
  - Lietot filtrus lai atdalītu uzticamus saņemtos elektroniskā pasta sūtītījumus.

Droša elektroniskā pasta lietošana (2)

- **Labā prakse:**
  - Lietotājam aizliegts lietot iestādes piešķirto individuālo e-pasta adresi reklāmas un cita veida komerciālu paziņojumu sūtīšanai un pārsūtīšanai, kā arī norādīt iestādes e-pasta adreses šāda veida ziņojumu saņemšanai;
  - Aizliegts atvērt neskaidras izcelsmes e-pasta ziņojuma pielikumus (piemēram, īpatnēji norādīts ziņojuma temats laukā "Subject", ziņojumam pievienota nezināma formāta vai izpildāmā datne, hipersaite uz nepazīstamu interneta mājas lapu), it īpaši, ja par bīstamo datņu veidiem vai nosaukumiem saņemts brīdinājums no IT administratora;
  - Neizmantot iestādes e-pastu personiskajai sarakstei – šim mērķim izmantot savu personīgo e-pastu (gmail, inbox, tvnet, apollo u.c.).
- **Svarīgi atcerēties:**
  - Par aizdomīga e-pasta sūtījuma neatvēršanu nav paredzēta atbildība! Toties par datora inficēšanu un konfidenciālas informācijas publiskošanu - ir.

Droša elektroniskā pasta lietošana (3)

Droša Interneta lietošana darba vietā

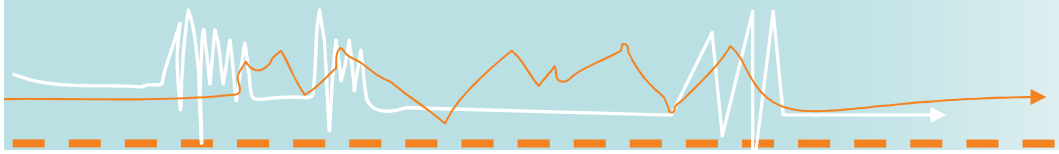
- **Labā prakse darba vietā:**
  - Lietotājam savu darba pienākumu pildīšanai un kvalifikācijas celšanai ir pieejams internets;
  - Lietotājam ir aizliegts patvaļīgi mainīt interneta pārlūkprogrammas drošības uzstādījumus vai veikt darbības, kas vērstas uz iestādes interneta pieslēguma nodrošinājuma servera (*firewall*) apiešanu;
  - Informācijas drošības pārvaldības ietvaros, organizācija ir tiesīga kontrolēt, ierobežot vai aizliegt lietotājam izmantot internetu izklaidei, vai jebkuriem citiem ar tiešo darba pienākumu veikšanu nesaistītiem mērķiem.
- **Svarīgi atcerēties:**
  - Internets darba vietā ir pieejams darba vajadzībām!
  - Jūsu darbības Internetā nav anonīmas!

Droša Interneta lietošana mājās

- **Labā prakse mājās:**
  - Uzstādīt (*firewall*);
  - Lietot antivīrusu programmas (regulāri atjaunināt);
  - Pārbaudīt ar antivīrusu programmu zibatmiņas, CD, DVD diskus;
  - Bezvadu tīkla iekārtas pieejai uzstādīt drošu paroli;
  - Lietot licenzētu programmatūru;
  - Nestrādāt ar konfidenciālu informāciju;
  - Lūgt ievērot noteikumus arī pārējiem datora lietotājiem.

- **Svarīgi atcerēties:**
  - Internets mājās ir izmantojams bez ierobežojumiem, bet tas palielina drošības riskus;
  - Jūsu darbības Internetā nav anonīmas!

Policijas vīruss



CERT.LV

Biroja ētika

Disciplīna darba telpās

- **Labā prakse:**
  - Ievērot iekšējās kārtības noteikumus nozīmē ievērot informācijas fiziskās drošības prasības;
  - Informācijas apstrādes un glabāšanas principi:
  - “Zina tikai tas, kam jāzina”;
  - “Tīra darba virsma”, jeb darba dokumenti uz rakstāmgalda atrodas tikai darba laikā.

- **Svarīgi atcerēties:**
  - Kabineta durvju atslēga nav greznumlieta!

Komunikācija ar trešajām personām

- **Labā prakse:**
  - Pieņemt apmeklētāju nenozīmē viņam atļaut brīvas “pastaigas” pa iestādes darba telpām!
  - Ierobežotas pieejamības informācijai ir jāpaliek iestādes iekšējā lietošanā!
  - Konfidencialitātes pienākums ir saistošs ne tikai organizācijas darba telpās, bet arī ārpus tām!
  - Nav ieteicams apspriest darba informāciju ar radiem, draugiem, paziņām.

Sociālā inženierija

Sociālā inženierija (1)

- **Sociālā inženierija** – manipulēšana ar cilvēku, lai tas veiktu zināmas darbības vai izpaustu konfidenciālu informāciju, tehniski nepiekļūstot informācijas sistēmai.

- Sociālās inženierijas paņēmieni tiek īstenoti, pamatojoties uz īpašiem atribūtiem cilvēka lēmumu pieņemšanas mehānismos.

- **Svarīgi atcerēties:**
  - Šķietami visnenozīmīgākā komunikācija ar nepazīstamu cilvēku nedrīkst sevī informāciju par darbu, dzīves vietu, radiniekiem utt.

Sociālās inženierijas piemērs – banku vīruss (1)

FROM: janis.berzins@dell.com
Subject: Re:dokuments

Čau,

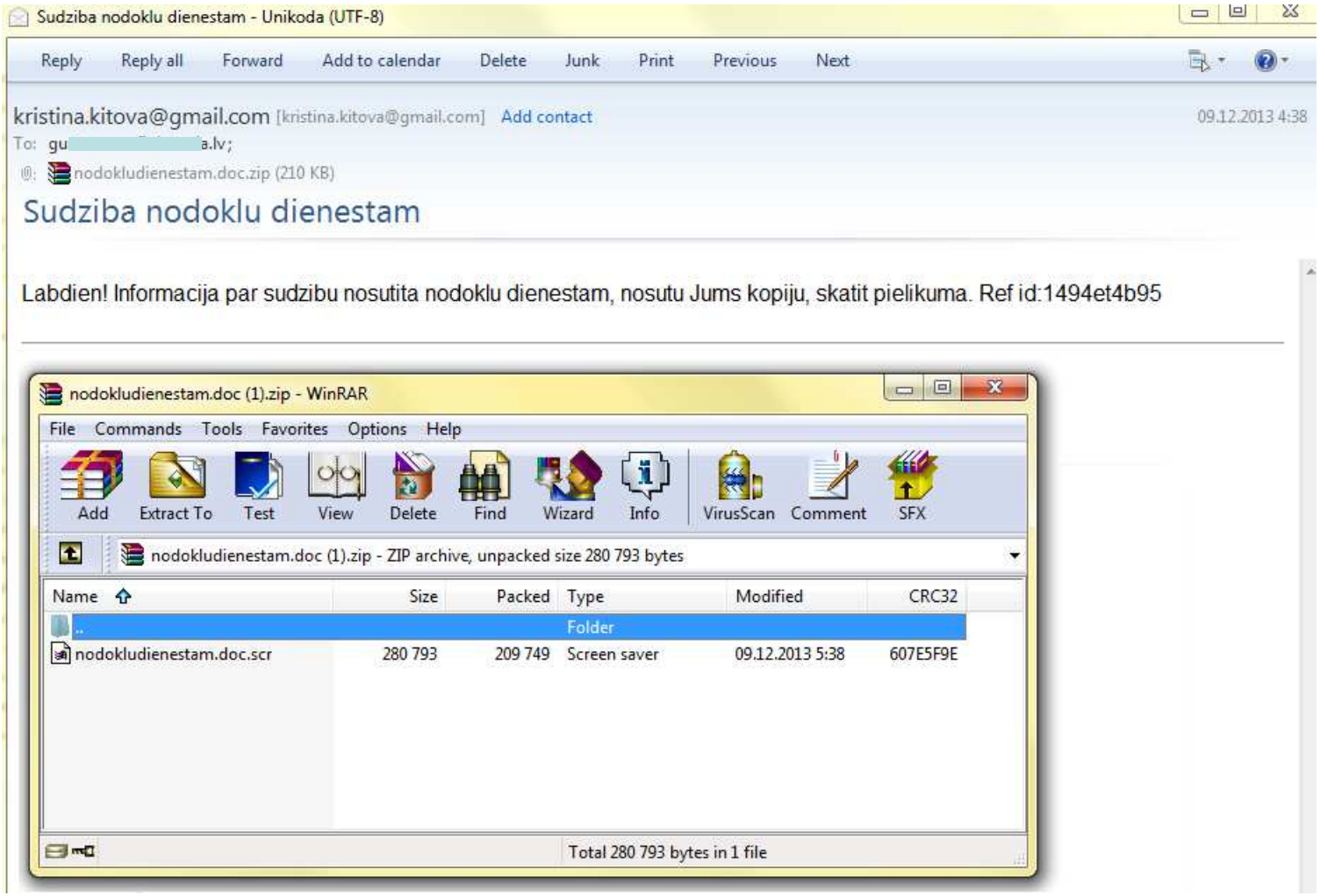
Steidzami apskaties failu un dod ziņu! ...mums jārisina tā lieta steidzami!

http://files.inbox.lv/ticket/<unikāla_simbolu_virkne>/
Jānis

Svarīgi atcerēties:

- Šāda veida e-pasta vēstules var tikt izmantotas lai inficētu darba datoru ar mērķi iegūt informāciju.
- Par aizdomīga e-pasta sūtījuma neatvēršanu nav paredzēta atbildība! Toties par datora inficēšanu, kā rezultātā tiek publiskota konfidenciāla informācija - ir.

Sociālās inženierijas piemērs – banku vīruss (2)



Sociālā inženierija (2)

- Mērķa sasniegšanai sociālais inženieris var manipulēt ar darbinieku motivāciju:
  - bailes pazaudēt darbu;
  - vēlme tikt novērtētam;
  - nogurums vai pārstrādāšanās;
  - mobings, bosings darba vietā.

- Mērķa sasniegšanai tiek izmantota arī cilvēku sociālo vērtības akceptēšanas paradumi:
  - cilvēki pieņem uzvedību, kura viņuprāt piemīt lielākajai daļai citu cilvēku;
  - cilvēki ir tendēti sadarboties ar cilvēkiem kuri izraisa viņos simpātijas.

Sociālā inženierija (3)

- Sociālās inženierijas uzbrukuma posmi:
  - informācijas savākšana;
  - attiecību izveidošana;
  - attiecību izmantošana;
  - mērķa sasniegšana.

- Sociālās inženierijas uzbrukumu veidi:
  - autoritātes tēlošana;
  - Iežēlināšana;
  - atbalsts un aprūpe;
  - ļaundabīgas programmas;
  - pētniecība.

Sociālā inženierija (4)

- Uzbrucēju komunikāciju veidi:
  - personīgi kontakti;
  - telefons;
  - elektroniskais pasts;
  - ļaundabīga programma.

- Aizsardzības stratēģija iestādē:
  - darbojošies iestādes IT drošības noteikumi;
  - stingra piekļuves procedūra IT resursiem ar lietotājvārdu un paroli;
  - stingra paroļu izveidošanas procedūra;
  - lojālas un draudzīgas darba vides izveidošana;
  - procedūra, kā un kam paziņot par incidentu.

Sabiedrības izglītošana

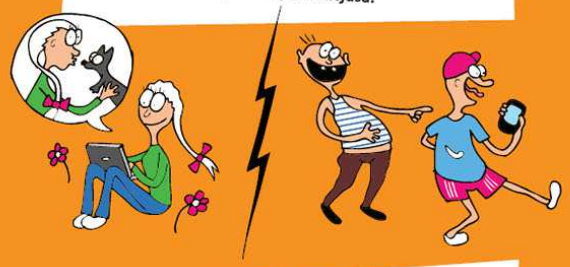
Sabiedrības izglītošana

- Tehniskie un teorētiskie semināri;
- Informācijas drošības izglītības programma (IDIP);
- IT drošības mācības;
- Plakāti pieaugušajiem un bērniem;
- Portāls Esidrošs – www.esidross.lv ;
- Datorologs.

Vai esi Interneta profiņš?

Apdomā pirms publisko attēlus internetā!

Padomā, vai šie attēli neaizskar un nekaitē Tev, Taviem draugiem, klasesbiedriem, vecākiem vai jebkuram citam cilvēkam, kas attēlots fotogrāfijā. Pēc tam, kad attēls ir „ielikts" internetā, to vairs nevar iznīcināt vai padarīt par nebijušu.

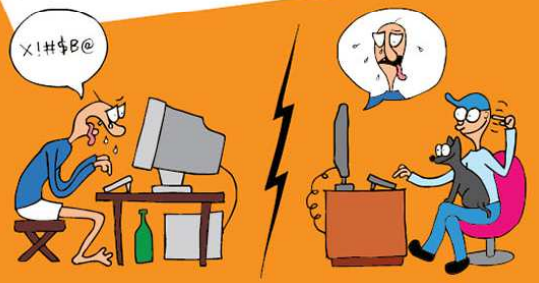


Lieto drošas paroles!

Katram portālam izmanto citādāku paroli. Veido to pietiekami sarežģītu, lai to nevarētu uzminēt pat tie cilvēki, kas Tevi labi pazīst!

Neraksti aizskarošus komentārus!

Cilvēki, kas aizvaino citus, paši jūtas nelaimīgi. Taču, aizvainojot citus, neviens laimīgāks nekļūst. Nesāpini apkārtējos! Esi iecietīgs pret citu viedokli, dzīvesveidu, dzīves uzskatiem.



Nesarunā tikšanās ar tīklā satiktajiem paziņām!

Atceries, ka tīklā satiktie cilvēki ne vienmēr ir tie, par ko izliekas! Sargā sevi, lai neviens nevar nodarīt Tev pāri! Nepiekrīti tikties ar nepazīstamiem cilvēkiem nomaļās vietās, kur nav neviena, kas nepieciešamības gadījumā varētu Tev palīdzēt.

Neatklāj datus par sevi nepazīstamiem cilvēkiem!

Nebūt ne visi, ko Tu satiec virtuālajā vidē, ir tie, par ko uzdodas. Bieži vien ļaundari slēpj savu patieso seju, lai vieglāk piekļūtu Tev, Taviem radiem un draugiem. Jo vairāk Tu par sevi atklāsi, jo vieglāk viņi varēs nodarīt Tev pāri reālajā dzīvē. Neatklāj, kā Tevi sauc, kur Tu dzīvo, kas ir Tavi vecāki vai kādas mantas Tev ir mājās.

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Vai esi Interneta profiņš?

- Par IT drošības incidentiem var ziņot CERT.LV - cert@cert.lv
- IT drošības izglītošanas portāls - www.esidross.lv
- CERT.LV mājas lapa - www.cert.lv

Mēstules nav vēstules!

Ignorē mēstules, ko saņem no nepazīstamiem cilvēkiem. Neatsaucies to „vilinošajiem" piedāvājumiem. Visbiežāk tie ir mēģinājumi izkrāpt Tavu naudu. Mēstules var izfiltrēt, un par tām var sūdzēties.

Neiepērcies internetā bez vecāku ziņas!

Nesniedz internetā savas vai vecāku kredītkartes datus, iepriekš neapspriežoties ar vecākiem. Atceries – izmantojot kredītkartes datus, var nozagt visu naudu, kas pieejama ar šo karti.

Darbības internetā nav anonīmas!

Tavas darbības internetā nav anonīmas! Vajadzības gadījumā tām var izsekot gan skolotāji, gan vecāki, gan likumu sargājošas iestādes.

Rūpējies par datora veselību!

Neinstalē nezināmas izcelsmes programmas datorā, ko Tu lieto. Programma ļoti viegli var "izlikties" par spēli, bet patiesībā būt vīruss, kam Tu pats paver ceļu uz savu datoru.

Ja Tu:

- saņem nepatīkamas, aizvainojošas vēstules internetā,
- esi saskāries ar nepatīkamiem materiāliem internetā,
- esi pamanījis aizdomīgas darbības internetā,
- esi satraukts par savu drošību internetā,

pastāsti par to saviem vecākiem vai kādam citam no pieaugušajiem, kam uzticies! Vari zvanīt Bērnu un jauniešu bezmaksas uzticības tālrunim 116111 vai rakstīt uz: zinojumi@drossinternets.lv vai abuse@cert.lv

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Portāls www.esidross.lv

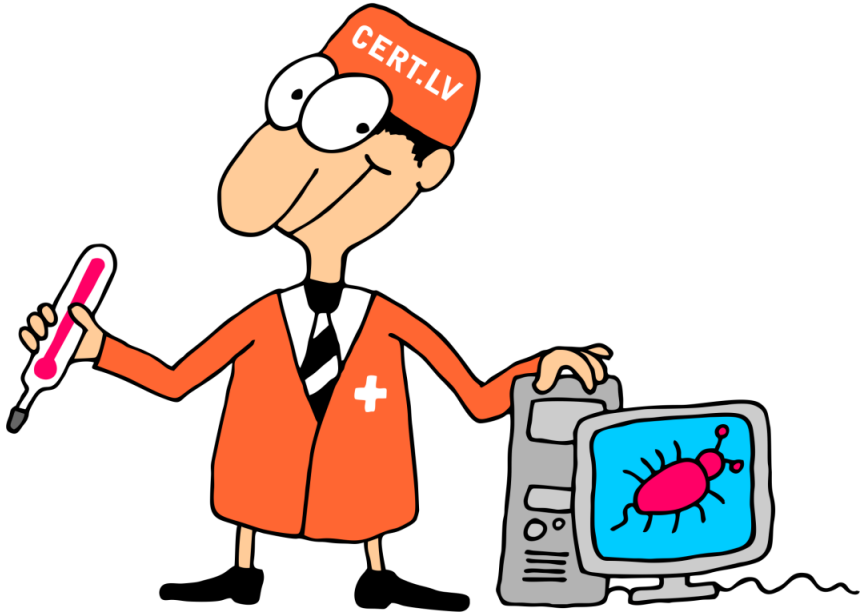
Atbildīgs interneta pakalpojumu sniedzējs

ATBILDĪGS INTERNETA PAKALPOJUMU SNIEDZĒJS ir kvalitātes zīme, kuru var saņemt Elektronisko sakaru pakalpojumu komersants, kurš:

- Sadarbojas ar CERT.LV un informē gala lietotājus par to, ka viņu datori ir inficēti ar kādu no datorvīrusiem un kļuvuši par robotu tīklu sastāvdaļu,
- Sadarbojas ar Net-Safe Latvia Drošāka interneta centru, lai nodrošinātu iespējami ātru nelegālā satura (bērnu pornogrāfijas) izņemšanu no publiskas aprites internetā,
- Pēc klientu pieprasījuma nodrošina bezmaksas interneta satura filtru uzstādīšanu atbilstoši Elektronisko sakaru likumam.

Datorologs

“Datorologs” ir CERT.LV darbinieks, kurš var diagnosticēt un, ja iespējams, novērst e-slimības un ļaunprātības Jūsu datorā, kā arī īsi pastāstīt, kā vari pasargāt savu datoru nākotnē.



CERT.LV

Rīcība drošības incidenta un pārkāpumu gadījumos

Rīcība drošības incidenta un pārkāpumu gadījumos

- **Labā prakse darba vietā:**
  - Sazināties ar atbildīgo IT administratoru un risināt radušos problēmu.
  - Nepieciešamības gadījumā IT administrators sazināsies ar CERT.LV
- **Mājās:**
  - Pats atbildīgs par sava datora drošību,
  - Jānovērtē kaitējums, un ja nepieciešams jāraksta iesniegums drošību sargājošam iestādēm,
  - Portālā www.esidross.lv var meklēt padomus, kā atrisināt radušos problēmu.

Konsultācijām ikdienas darbam informācijas tehnoloģiju drošības un datu aizsardzības jautājumos:

Vārds Uzvārds

IESTĀDE
DEPARTAMENTS
AMATS

Tālrunis: _____
E-pasts: _____

Paldies par uzmanību!

http://www.cert.lv/
cert@cert.lv
baiba.kaskina@cert.lv
egils.sturmanis@cert.lv

Prezentācija izveidota sadarbojoties DEG un CERT.LV.

Prezentācijas saturs sagatavots Latvijā, izmantojot WIkipedia publicētās definīcijas, publikācijas interneta medijos un ņemot vērā autoru - Baibas Kaškinas, Kristapa Miļevska, Egila Stūrmaņa - personīgo izpratni informācijas drošības un datu aizsardzības jautājumos.