Mūsdienu aktualitātes kiberdrošībā

E-pasta šifrēšana

Mg.sc.ing. Nauris Pauliņš

e-pasts: nauris.paulins@zpr.gov.lv

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 aktualitāte

Drošības nodrošināšanā iesaistīti visi uzņēmuma darbinieki. Kāpēc?

- Darbiniekiem ir pieejama informācija:
  - Grāmatvedim – finanšu informācija
  - Juristam – līgumi, iepirkumi
  - IT darbiniekiem – paroles, tīkla konfigurācija,
  - Ierindas darbinieks – piekļuves parole, iestādes iekšējā informācija

Darbiniekus bieži izmanto kā vieno no ķēdes posmiem uzbrukumā

Svarīgi ir ne tikai kā lieto IT resursus ne tikai iestādē, bet arī ārpus tās

Internetā ielikto nav tik viegli izņemt: https://web-beta.archive.org/web/

Informācijas aizsardzība:

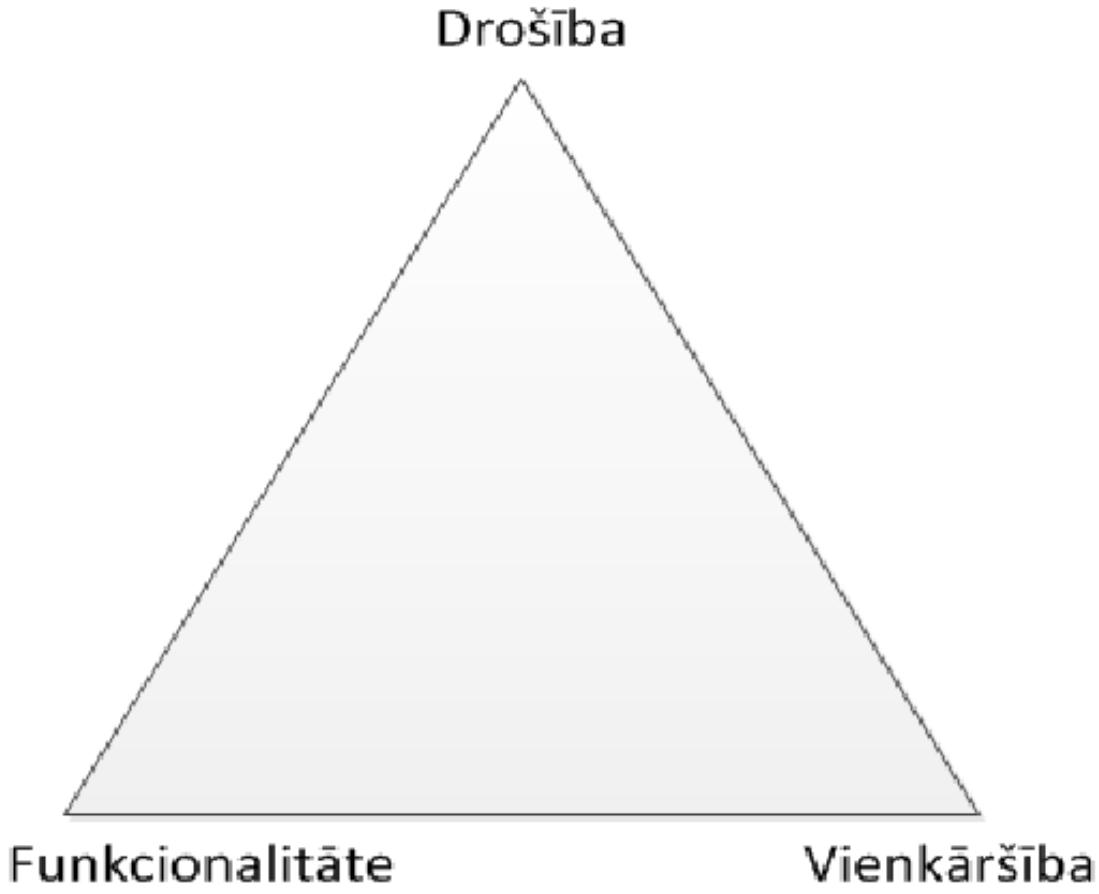
Informācija - ir ziņa vai ziņu kopums jebkurā tehniski iespējamā fiksēšanas, uzglabāšanas vai nodošanas veidā".

Dati - informācija, kas materializēta uz tāda datu nesēja, ko spēj apstrādāt dators vai cita datortehnika"

Informācijas aizsardzība:

Pārvaldības procedūras un tehnoloģiju kopums, kas nodrošina korektas informācijas pieejamību **īstajai personai, īstajā laikā un īstajā vietā**

Vienmēr pastāvošā dilemma



Pamatprincipi:

Mēs pieņemam lēmumus un veicam darbības vadoties pēc tās informācijas, kas mums ir pieejama un zināma. Tāpēc mums ir jārūpējas, lai informācija būtu patiesa un kvalitatīva.

Konfidencialitāte	**Informācijas piederības nodrošināšana tās īpašniekam un slepenības nodrošināšana pret nesankcionētu atklāšanu**
Integritāte	**Informācijas veseluma, precizitātes un pareizuma nodrošināšana atbilstoši biznesa vajadzībām**
Pieejamība	**Informācijas saglabāšana un uzturēšana, lai tā būtu pieejama īstajā laikā un īstajā vietā**

Aizsardzības metodes:

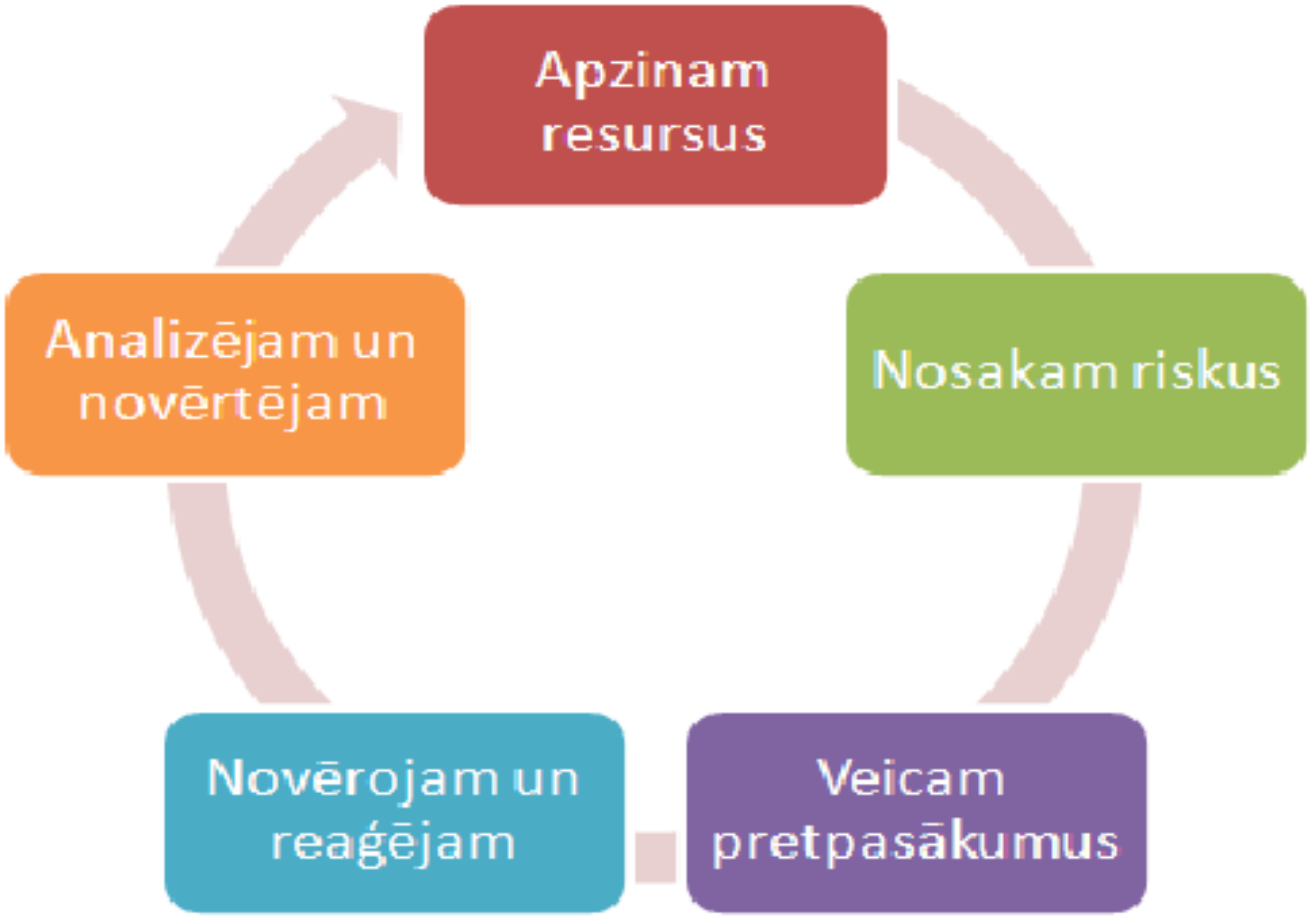
Svarīgi ir zināt kā aizsargāties, bet vēl svarīgāk ir zināt ko aizsargāt!

Tāpēc vienlīdz svarīgas ir:

- Tehniskā aizsardzība: Programmatūras un tehnisko resursu izmantošana, lai aizsargātu savus informācijas resursus un sistēmas

- Loģiskā aizsardzība: Biznesa procesi un procedūras, kas nodrošina korektu informācijas aizsardzības plānošanu un organizēšanu un nodrošināšanu

Tas ir nebeidzams process:

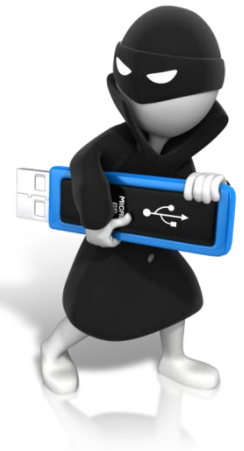


Drošības incidents

- **IT Drošības incidents** ir tāds cilvēka izraisīts notikums, kura rezultātā tiek vai var tikt nodarīts kaitējums (neparedzēts lietojums, servisa atteikums, datu noplūde, uzticamība vai integritātes zudums…) tīklam, datoram, lietojumprogrammai vai datiem.

Informācijas tehnoloģiju drošības likums:

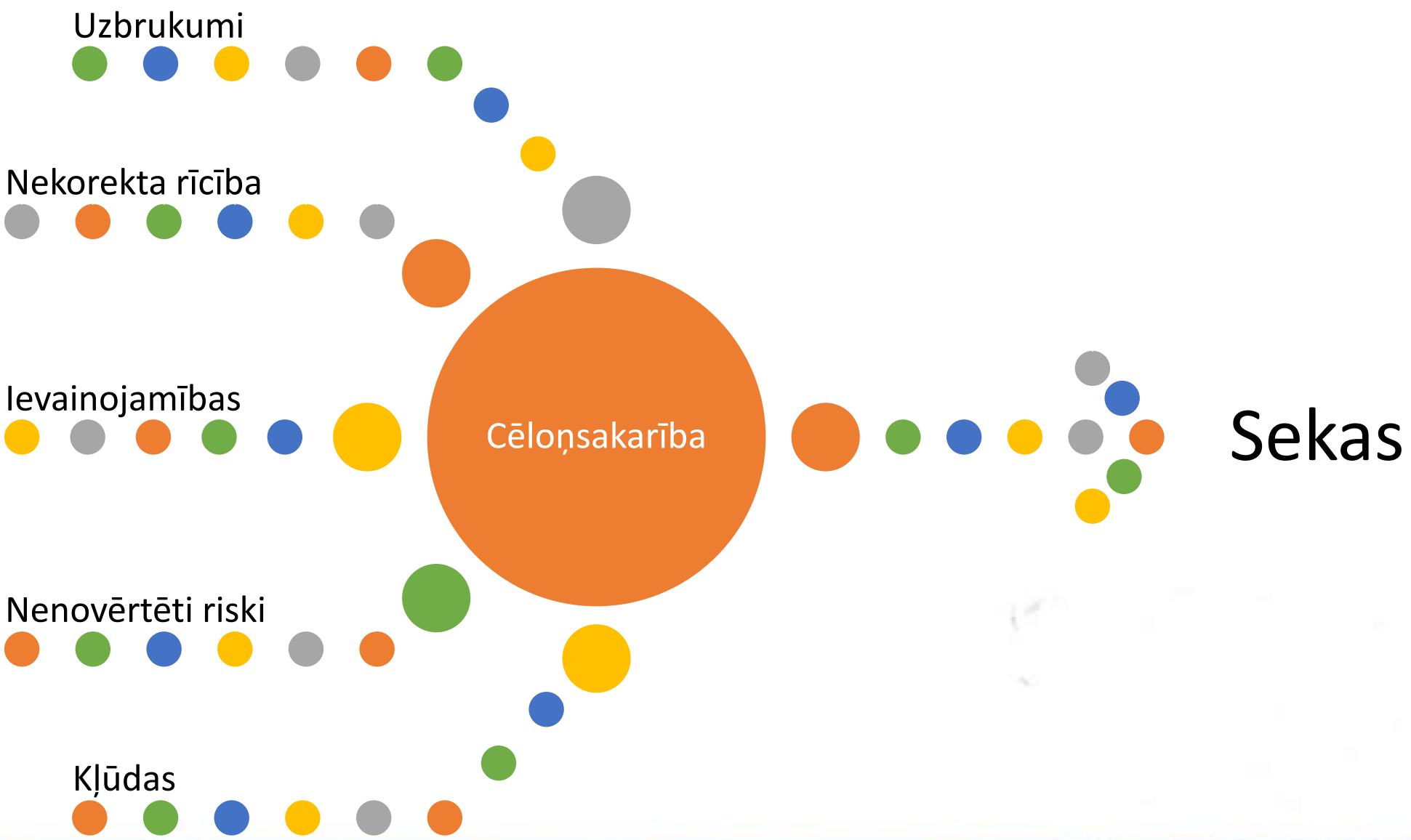
- Informācijas tehnoloģiju drošības incidents (turpmāk – drošības incidents) ir kaitīgs notikums vai nodarījums, kura rezultātā tiek apdraudēta informācijas tehnoloģiju integritāte, pieejamība vai konfidencialitāte



Sodi, ja netiek uzturēta drošība

- Sadalīts atbildības un noteiktas prasības uzņēmuma darbiniekiem;
- Tiek apzināta organizācijas resursi un tiem attiecināmie riski, izvērtēta to ietekme uz organizācijas darbu (mums vēl jādara)
- IS gadījumā var piemērot KL 318 vai 319. pantu, kas paredz amatpersonu atbildību, jo atbildīgais par iestādes drošības stāvokli ir Iestādes, institūcijas vadītājs un drošības pārvaldnieks.
- Fizisko personu datu apstrādē ir paredzēti arī naudas sodi, kur maksimālais sods paredzēts līdz 14 000 EUR (pēc jaunās regulas līdz 20milj. vai 4% no iepriekšējā gada apgrozījuma)

Draudi var būt dažādi



Iekšējie draudi

Uzņēmuma darbinieki*:

- 70% plāno kaut ko paņemt līdzi, kad mainīs darba devēju
- 62% paņēma līdzi datus, kad pameta uzņēmumu
- 56% atzinuši «internal hacking» - apzinātu mēģināšanu piekļūt iekšējiem resursiem, bez leģitīma pamatojuma

Iekšējie draudi – kaitnieciska darbība ar informāciju, kuras avots ir organizācijas iekšienē

- Piekļuve datiem, kuri neietilpst personas piekļuves apgabalā
- Uzņēmuma informācijas nopludināšana, nozagšana
- Uzbrukumu veikšana, izmantojot zināmo informāciju un tiesības

- Riska grupas:
  - Darbinieki
  - Līgumdarbinieki, ārpakalpojuma sniedzēji
  - Citas uzticības personas ar pieeju organizācijas resursiem

*Avots: Imperva pētījums «The Insider's Guide to the Insider Threat» (2012, ielu aptauja Londonā un Šanhajā)

Kibernoziegumus nav tik vienkārši pierādīt

- ISD jēdziens (pieejamība, integritāte, konfidencialitāte). **Krimināltiesiskā aizsardzība piemērojama tikai tām ADAS, kur sistēmas īpašnieks vai tiesiskais valdītājs ir izstrādājis IS drošības politiku**, nosakot lietotāju piekļuves kārtību, informācijas klasifikāciju sistēmā, aprīkojis sistēmu ar attiecīgiem aizsardzības līdzekļiem utml..
- Darbībai nodarījuma brīdī jābūt aizliegtai ar KL (*non lege sine poena*)
- Darbībai ir jābūt reālai, aktīvai un vērstai uz konkrētu negatīvu rezultātu- pret vienu vai vairākiem ISD elementiem
- Personai ir jāapzinās, ka tā veic aktīvu darbību un vēlas konkrēta negatīva rezultāta iestāšanos.

Tas viss mūs skar ikdienā:

Internetā iepazīts varmāka Rīgā aplaupa un izvaro sievieti (91)

Foto: valsts policija

Rīgas policisti pr[illegible] ...gā ...ēd... 26. gad...s vecu vīrieti, kuru likuma sarg[illegible]tur aizdomās par laupīšanu un izvarošanu, kas pastrādāta

Papildināts - *Tella Latvija* uzbrukuši hakeri un «nobrucis» LIX, radot problēmas interneta vietnēm

Latvijas Sargs, 2012. gada 4. aprīlis 10:30

Uzņēmums *Tella Latvija* cietis no hakeru uzbrukuma un, visticamāk, cilvēciskas kļūdas dēļ problēmas radušas

Hakeri sabojā ziņu aģentūras LETA mājas lapu

Jau vēstījām, ka IT eksperti valsts datu aizsardzību novērtē kā nepietiekamu. "Uzlabojumi ir, taču ar to ir par maz. Ja steidzīgi nenotiks visaugstākā līmeņa auditi, tad mēs vēl dzirdēsim par caurumiem, noplūdēm un kļūdām valsts datu sistēmās," TVNET pastāstīja Latvijā un citās valstīs strādājošās IT&T kompānijas "Latnet" Pārdošanas departamenta vadītājs Vladislavs Gurmans.

Datu drošības jautājums šodien aktuāls kļuva arī ziņu aģentūrā LETA.

Kāda Latvijas ministrija piedzīvojusi mērķtiecīgu hakeru uzbrukumu 4

Kādai Latvijas ministrijai uzbrukuši hakeri, apstiprināja informācijas tehnoloģiju (IT) drošības incidentu novēršanas institūcijā *CERT.LV*. Netiek atklāts, kurai ministrijai uzbrukts, bet publiskota informācija par hakeru...

Notikuši mērķēti kiberuzbrukumi valsts iestādes darbiniekiem

Kādā valsts iestādē vairāki darbinieki saņēma savu kolēģu vārdā nosūtītus e-pastus ar virsrakstu "Latvijas Stabilitātes programma 2016.-2019.gadam", kas tika izsūtīti no inbox.lv servera. To pielikums saturēja Microsoft Office formāta dokumentu ar makro funkciju, kas lejupielādēja un izpildīja datorvīrusu. Datoru inficēšana iestādē nav konstatēta.
Ir pamats domāt, ka uzbrucēji bijuši no Korejas.

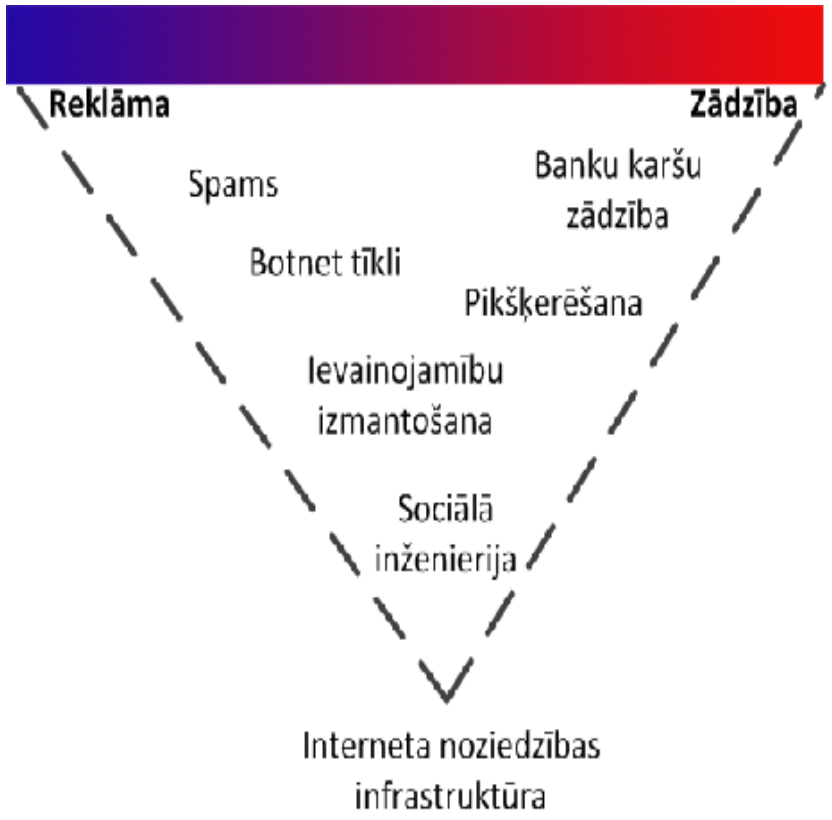
Skolnieks labo atzīmes e-klase.lv portālā

Tika konstatēts, ka kāds vidusskolas skolnieks labojis savas un klasesbiedru atzīmes e-klase.lv portālā, izmantojot skolotājas paroli. Parole tika iegūta no LinkedIn kompromitēto paroļu datiem, kas ir brīvi pieejami internetā. Nodarījums netieši atgādina, ka parolēm dažādās vietnēs ir jābūt atšķirīgām, citādi tās var viegli piemeklēt.

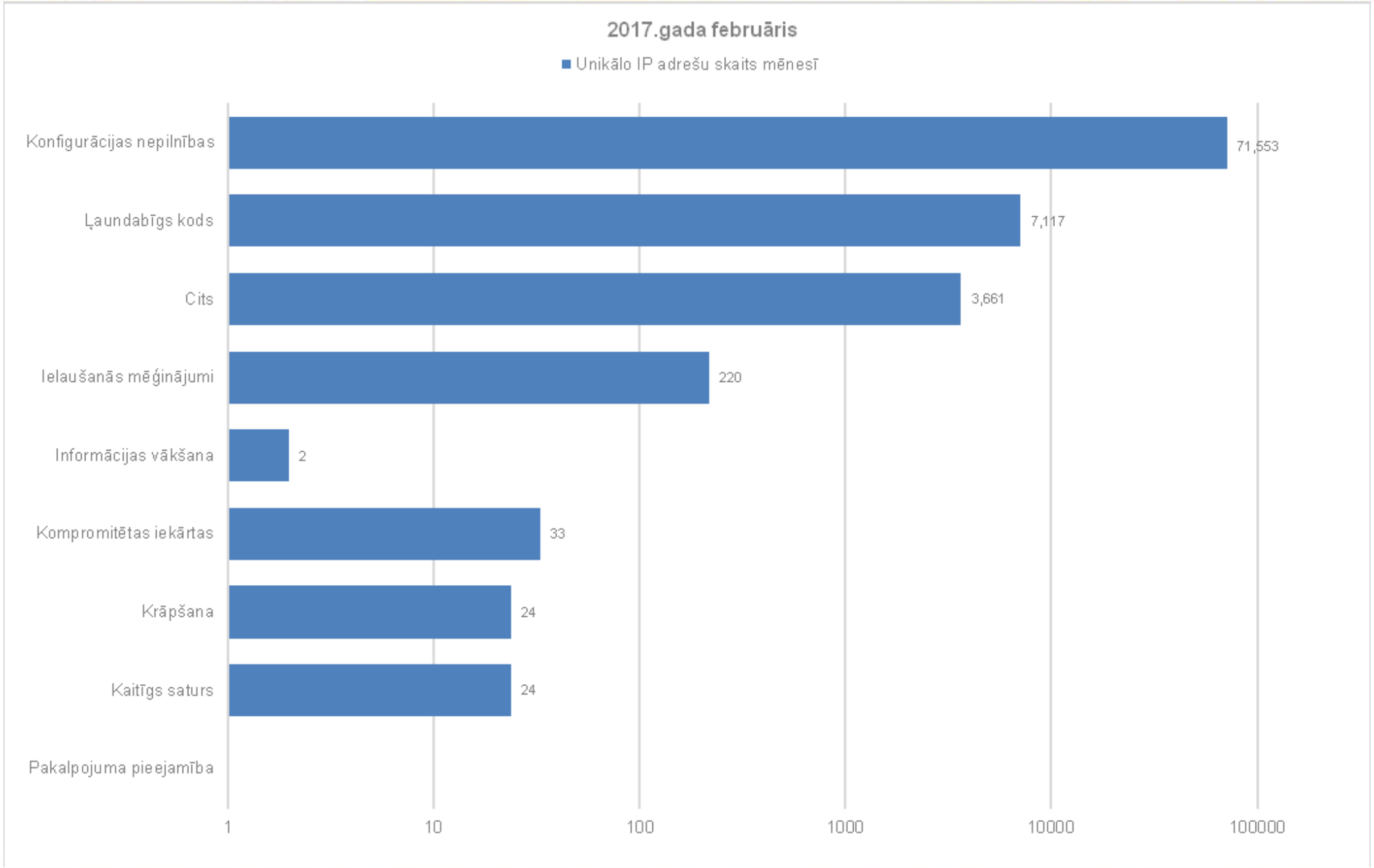
Izķēmots pašvaldības iestādes portāls

21.09. tika konstatēts, ka izķēmots pašvaldības iestādes portāls. Pēc CERT.LV brīdinājuma iestāde veica pārbaudi, kurā atklāja izķēmošanas cēloni - CMS TikiWiki 14.0 ievainojamību. Portāls tika salabots un tā darbība atjaunota.

Mūsdienu aktuālie draudi:



- Naudas, identitātes vai datu zādzība
- Jūsu resursu zādzība, lai apkrāptu citus
- Krāpniecība, lai izkrāptu Jums naudu
- Datu zādzība ar mērķi tos izmantot savtīgos nolūkos vai vienkārši pārdot
- Pakalpojumu atteices izraisīšana, lai traucētu veiksmīgu pakalpojumu nodrošināšanu


2017.gada februāris
Unikālo IP adrešu skaits mēnesī
Konfigurācijas nepilnības
71,553
Ļaundabīgs kods
7,117
Cits
3,661
Ielaušanās mēģinājumi
220
Informācijas vākšana
2
Kompromitētas iekārtas
33
Krāpšana
24
Kaitīgs saturs
24
Pakalpojuma pieejamība
1
10
100
1000
10000
100000

Uzbrukumu principi:

Neviens «uz aklo» neuzbrūk un arī cietumā nevienam nepatīk

https://www.exploit-db.com/google-hacking-database/

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 atpazīšanu u.c.)

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

Labas paroles izveide

Piemērs:

1. izvēlamies teksta rindiņu – piemēram: **mans draugs nenopietns cilvēks**
2. izvēlamies katra vārda pirmo un trešo burtu – iegūstam paroli: mndanncl
3. vajag ciparu – l burtu nomainām uz 1 – iegūstam paroli: mndannc1
4. vajag lielo burtu – m burtu nomainām uz M – iegūstam paroli: Mndannc1
5. vajag simbolu – a burtu nomainām uz & – iegūstam paroli: Mnd&nnc1
6. katrai vietnei atšķirīga parole – pievienojam vietnes sev zināmu saīsinājumu:
   - Mnd&nnc1dr – parole draugiem.lv;
   - Mnd&nnc1ek – parole e-klase;
   - Mnd&nnctw – parole twitter.com

Sociālā inženierija

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

- **Aizsardzības stratēģija iestādē:**
  - darbojošies iestādes IT drošības noteikumi;
  - stingra piekļuves procedūra IT resursiem ar lietotājvārdu un paroli;
  - procedūra, kā un kam paziņot par incidentu.

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

"Date: Tue, 03 Feb 2015 14:23:16 +0300
From: anete kurzeme <anete.kurzeme@mail.ru>
To: anete.kurzeme@mail.ru

Labdien,
Šo rēķinu mēs jums izrakstijām pirms 3 mēnešiem un esam konstatējuši, ka maksājums par šo rēķinu nav saņemts. Vai jūs lūdzu varētu pārbaudīt to?
Elektroniskais rēķins
http://dokumenti.su/klienti/rekini/pdf.php?id=a5a663f6a29ctests

Ar cieņu,
galvenā grāmatvede
+371 29704926
A/S "Manotrans"

Ar cieņu,
Mārtiņš Kuzmanis

[redacted]

From: gov.lv [lookup host] [mailto:roo.violenciafamiliar@tj.mt.gov.br [lookup email] [lookup "tj.mt.gov.br"]]
Sent: Saturday, April 4, 2015 4:05 PM
To: undisclosed-recipients:
Subject: anti/virus

Mēs vēlamies Jūs informēt, ka mēs pašlaik veic plānotā tehniskā apkope un uzlabot mūsu tīmekļa pasta pakalpojumu un kā rezultātā šī ir HTK4S vīruss nav konstatēts konta mapes, un jūsu konts ir jāatjauno uz mūsu jauno F-Secure HTK4S anti-vīrus / anti-spam versija 2015. līdz novērstu kaitējumu jūsu svarīgi failus. Aizpildiet zemāk kolonnas un sūtīt atpakaļ vai e-pasta konts uz laiku tiks apturēta no mūsu pakalpojumiem.

********** **********

Lietotāja vārds: .....
Parole: .....
Dzimšanas datums: .....

hm !!! ?

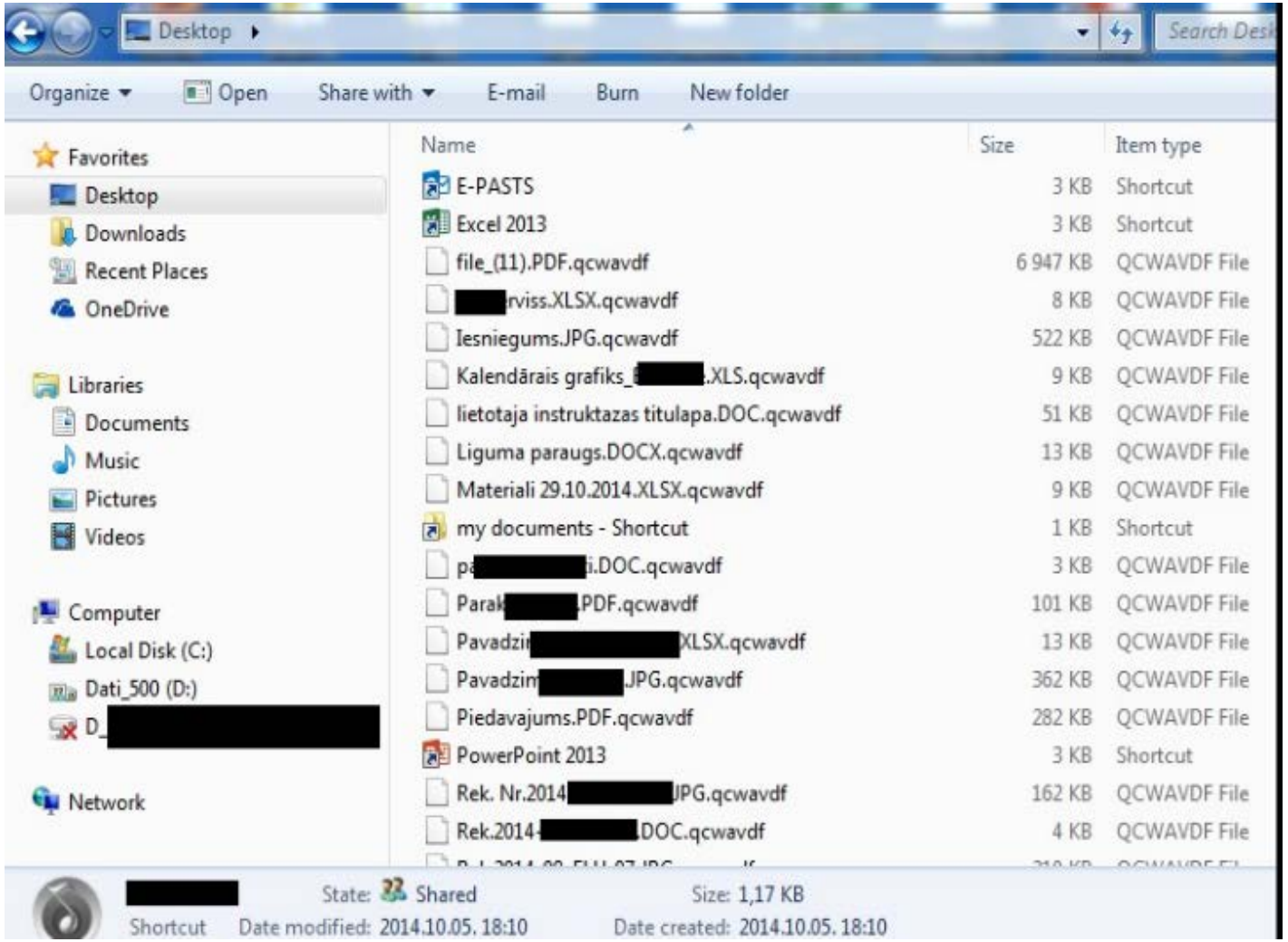
********** ********** *

Nespēja to darīt, 24 stundu laikā nekavējoties padarīt jūsu e-pasta konts deaktivizēts no mūsu datu bāzes gov.lv [lookup host]

Rīkojamies saprātīgi

- Pārdomājiet, pirms atvērt nezināmas saites
- Ja rodas šaubas, pārbaudām, vai tīmekļa vietne ir īsta
- Bez vajadzības neveram saites portālu komentāros
- Pārbaudām e-pastu sūtītāju un adresātu
- Neatveram šaubīgus e-pasta pielikumus
- Noteikumus izpildām mājās un darbā!

Jaunākā tendence



Zibatmiņas

- plaši pieejama un ērti lietojama;
- izmanto datu apmaiņai starp daudziem datoriem;
- viegli pazaudējama;
- viegli inficējama 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;
- 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 svarīgu un aizsargājamu informāciju.

Elektroniskais pasts

Privātais elektroniskais pasts – svarīgākais Jūsu interneta resurss.

Darba elektroniskais pasts – sarakste darba vajadzībām.

Labā prakse:

- pārbauīt e-pasta sūtītāju un adresātu;
- padomāt pirms atvērt e-pastā atsūtītu saiti interneta pārlūkā;
- neatvērt šaubīgus e-pasta pielikumus;
- izmantot filtrus, lai atdalītu vēlamu e-pastu no mēstulēm;
- šos ieteikumus ievērot gan darbā, gan mājās.

Svarīgi atcerēties:

- Par aizdomīga e-pasta sūtījuma neatvēršanu nav paredzēta atbildība! Toties par datora inficēšanu un konfidenciālas informācijas publiskošanu - ir.

Interneta lietošana

Labā prakse mājās:

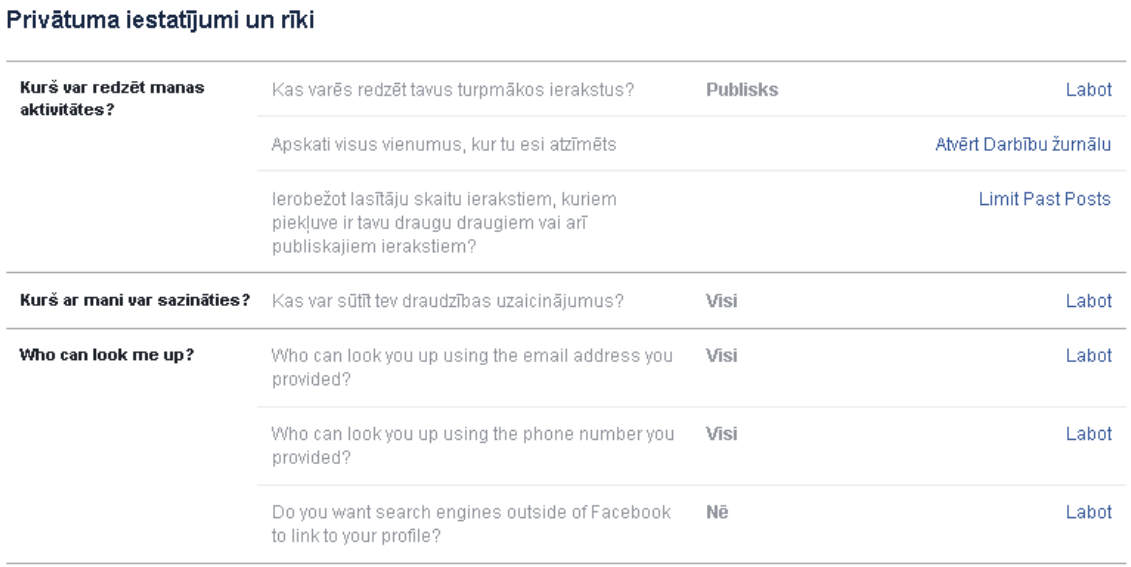
- uzstādīt ‘ugunsmūri’ (*firewall*);
- lietot antivīrusu programmas (regulāri atjaunināt);
- pārbaudīt ar antivīrusu programmu zibatmiņas, CD, DVD diskus;
- bezvadu tīkla iekārtas pieejai uzstādīt drošu paroli;
- lietot licencētu programmatūru;
- nestrādāt ar konfidenciālu informāciju;
- lūgt ievērot noteikumus arī pārējiem datora lietotājiem.

Svarīgi atcerēties:

- internets mājās ir izmantojams bez ierobežojumiem, bet tas palielina drošības riskus;
- jūsu darbības internetā nav anonīmas!

Sociālie tīkli

- Domāt ko mēs publicējam un par ko mēs publicējam
- Pārskatām privātuma un drošības iestatījums
- Regulēt, kāda auditorija var skatīt jūsu sociālā tīkla ziņas
- Izmantot bloķēšanas iespējas
- Pārskatīt laika joslas opcijas



Privātuma iestatījumi un rīki

Kurš var redzēt manas aktivitātes?	Kas varēs redzēt tavus turpmākos ierakstus?	**Publisks**	Labot
	Apskati visus vienumus, kur tu esi atzīmēts		Atvērt Darbību žurnālu
	Ierobežot lasītāju skaitu ierakstiem, kuriem piekļuve ir tavu draugu draugiem vai arī publiskajiem ierakstiem?		Limit Past Posts
Kurš ar mani var sazināties?	Kas var sūtīt tev draudzības uzaicinājumus?	**Visi**	Labot
Who can look me up?	Who can look you up using the email address you provided?	**Visi**	Labot
	Who can look you up using the phone number you provided?	**Visi**	Labot
	Do you want search engines outside of Facebook to link to your profile?	**Nē**	Labot

Rīcība drošības incidentu un pārkāpumu gadījumos

Labā prakse darba vietā:

- sazināties ar atbildīgo IT administratoru un risināt radušos problēmu;
- nepieciešamības gadījumā IT administrators sazinās ar CERT.LV.

Mājās:

- pats atbildīgs par sava datora drošību;
- jānovērtē kaitējums, un, ja nepieciešams, jāraksta iesniegums drošību sargājošām iestādēm;
- portālā www.esidross.lv var meklēt padomus, kā atrisināt radušos problēmu.

Fizisko personu datu aizsardzība

Personas dati:

- Jebkāda informācija, kas attiecas uz identificētu vai identificējamu fizisko personu
- Nav nozīme datu formātam, gan elektroniska, gan papīra formāta ietverta, gan skaņas, gan attēla formātā
- Jābūt adekvātiem, precīziem, tie pienācīgi jāaizsargā
- Jāapstrādā tikai saskaņā ar mērķiem, godīgi un likumīgi

Sodi:

Administratīvo pārkāpumu kodekss, 204.7 pants. Nelikumīgas darbības ar fiziskās personas datiem

Krimināllikums, 145. pants. Nelikumīgas darbības ar fiziskās personas datiem.

Noteikumu mērķis

Noteikt organizatorisko pasākumu un nepieciešamo tehnisko līdzekļu kopumu, kas nodrošina godprātīgu un likumīgu personas datu apstrādi un lietošanu tikai paredzētajiem mērķiem, to glabāšanas, atjaunošanas, labošanas un dzēšanas veidu, nodrošinot ikvienas fiziskas personas tiesības uz savu personas datu aizsardzību.

- **Pārzinis** –kas nosaka datu apstrādes mērķus un atbild par personas datu apstrādi.
- **Datu subjekts** – fiziska persona, kuru var tieši vai netieši identificēt;
- **Personas datu operators** – pārziņa pilnvarota persona, kas veic personas datu apstrādi pārziņa uzdevumā.
- **Sensitīvi personas dati** – personas dati, kas norāda personas rasi, etnisko izcelsmi, reliģisko, filozofisko un politisko pārliecību, dalību arodbiedrībās, kā arī sniedz informāciju par personas veselību vai seksuālo dzīvi.

Pamatprincipi, kas jāievēro

- Godprātīga un likumīga datu apstrāde
- Datu apstrāde tiek veikta atbilstoši paredzētajam mērķim un tikai saskaņā ar to;
- Dati ir adekvāti (ne pārmērīgi);
- Dati ir precīzi;
- Dati netiek glabāti ilgāk kā nepieciešams;
- Dati tiek apstrādāti saskaņā ar datu subjekta tiesībām;
- Dati ir drošībā;
- Netiek pārsūti citiem bez drošas un adekvātas aizsardzības;

Pārziņa pienākums

- Rūpēties par personas datu apstrādes sistēmas darbību, nodrošinot pilnvaroto personu drošu piekļuvi tai, kā arī iespēju datu subjektam iepazīties ar saviem personas datiem.

- Personas datu obligāto tehnisko aizsardzību īsteno ar fiziskiem un loģiskiem aizsardzības līdzekļiem, nodrošinot aizsardzību pret drošības incidentu radītu personas datu apdraudējumu.

Apstrāde ir atļauta, ja:

- Normatīvajos aktos nav noteikts citādi un ja ir vismaz viens no šādiem nosacījumiem:
  - Saņemta personas datu subjekta piekrišana;
  - Datu apstrāde izriet no datu subjekta līgumsaistībām vai, ievērojot datu subjekta lūgumu, datu apstrāde nepieciešama, lai noslēgtu attiecīgu līgumu;
  - Datu apstrāde nepieciešama Pārziņa likumā noteikto funkciju veikšanai;
  - Datu apstrāde nepieciešama, lai aizsargātu datu subjekta vitāli svarīgas intereses, tai skaitā dzīvību un veselību;
  - Datu apstrāde nepieciešama, lai nodrošinātu sabiedrības interešu ievērošanu vai realizētu publiskās varas uzdevumus…
  - Datu apstrāde ir nepieciešama, lai ievērojot datu subjekta pamattiesības…

Informācijas tehnoloģiju drošības likums:

- **Nosaka:**
  - Valsts un pašvaldību institūcijām izstrādāt IT drošības noteikumus.
- **Paredz:**
  - Rakstiski norīkot atbildīgo personu par IT drošības pārvaldību.
  - Dokumentētus IT drošības noteikumus.

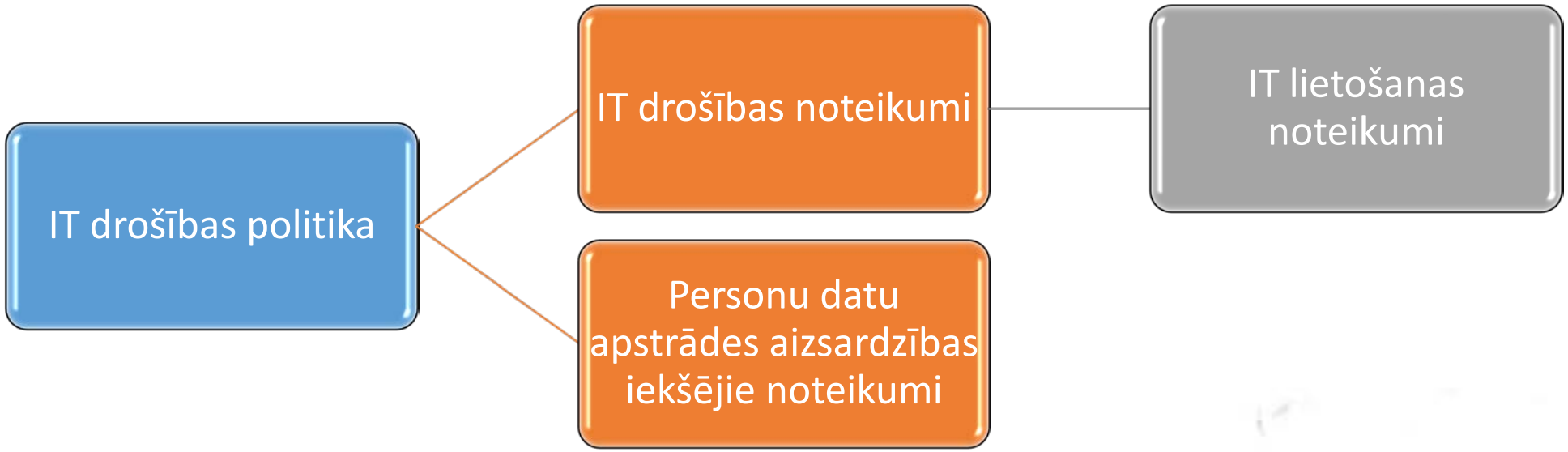
IT drošības speciālists

Galvenie pienākumi:

- Organizēt IT drošības pārvaldību.
- Veikt IT drošības pārbaudes (ne retāk kā reizi gadā).
- Celt savu kvalifikāciju, apmeklējot kursus (vismaz reizi gadā).
- Veikt darbinieku instruktāžu / apmācības (ne retāk kā reizi gadā).

Atbildīgajai personai netiek izvirzītas nekādas prasības attiecībā uz izglītības līmeni vai kompetenci

IT un personu datu aizsardzības dokumenti



"Personas datu aizsardzības obligātās tehniskās un organizatoriskās prasības"

- Personas datu obligāto tehnisko aizsardzību īsteno ar fiziskiem un loģiskiem aizsardzības līdzekļiem, nodrošinot:
  - 3.1. aizsardzību pret fiziskās iedarbības radītu personas datu apdraudējumu;
  - 3.2. aizsardzību, kuru realizē ar programmatūras līdzekļiem, parolēm, šifrēšanu, kriptēšanu un citiem loģiskās aizsardzības līdzekļiem

- **Kāpēc nevar visu vienkārši sūtīt man uz e-pastu?**
  Uz e-pastu drīks nosūtīt personas datus saturošus dokumentus tikai tos šifrējot.

E-pastu šifrēšanas piemērs

- https://www.gpg4win.org/

- Izveidojam privātās un publiskās atslēgas pāri
- Publisko atslēgu nosūtam citiem, lai viņi var šifrēt ziņas
- Otra šo atslēgu importē savā datorā, jāapliecina tam uzticība un jāsertificē atslēga
- Tad otrā puse brīvi šifrēt dokumentus ar šo atslēgu un sūta mums
- Mēs ar savu privāto atslēgu varam atšifrēt sūtīto ziņu.
- Programma arī integrējas tādos klientos kā – Outlook, Thunderbird, Claws Mail, KMail

E-adrese


Valsts iestādes + rezerves karavīri
01.06.2018
Tiesas, ZTI, MNA
01.01.2020
Fiziskas personas, VID nod. maksātāju reģ. reģistrētie
01.06.2018
Komersanti + UR reģistros reģistrētie
01.01.2019
01.01.2020
Izmanto brīvprātīgi
Izmanto obligāti