



possible.lv

IT drošības risinājumi

Kas katram
uzņēmumam būtu
jāzina par kiberdrošību ?

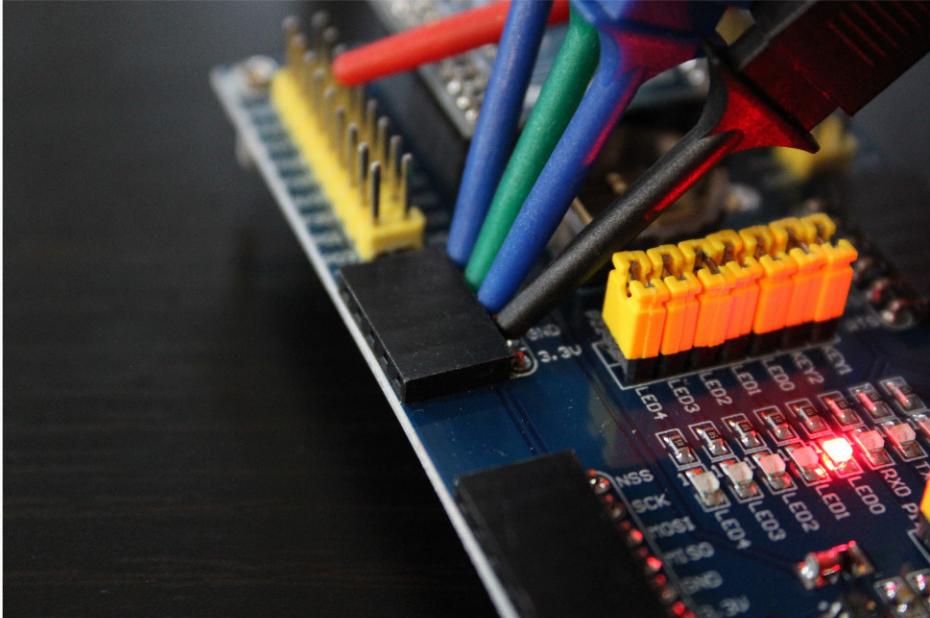
Praktiski padomi un ieteikumi

Kirils Solovjovs



- Mg.sc.comp, Mg.phys
- Possible Security vadītājs
- Iepriekš:
 - Aizsardzības ministrija
 - NATO CCDCOE

Possible Security



- Ielaušanās testi un auditi
- Programmatūras un aparatūras drošība
- Konsultācijas
- Augstākās klases serviss

nejauka situācija



- Ievainojams bezvadu tīkls rūpnīcā
- Netālu no rūpnīcas izvietota iekārtu, kas maskējas par kāda darbinieka iekārtu
- Caur tīklu piekļūts rūpnīcas finanšu sistēmai, veikts pārskaitījums
- Nodarītie zaudējumi: 200 000 €

uzticoties noziedzniekiem



- Saņemts e-pasts „Nozagām jūsu datus. Samaksājet 4 BTC (100 000€), lai nepublicētu”
- Uzņēmums jau iepriekš maksājis izpirkuma maksu, cerot, ka situācija neatkārtosies
- Nodarītie zaudējumi, t.sk. un soda naudas un reputācijas kaitējums: 700 000 €

kārtība mājās



- Reklāmas aģentūra neveidoja rezerves kopijas
- Aparatūras problēmu dēļ neilgu laiku pirms projekta nodošanas visi projekta faili kļuva nepieejami
- Potenciālie zaudējumi: 30 000 €

kiberdrošība



- Konkrētas kibertelpas aizsardzības pasākumi, lai aizsargātu
 - datorus
 - tīklus
 - programmatūru
 - personisko un konfidenciālo informāciju
 - u.tml.

kiberuzbrukumi



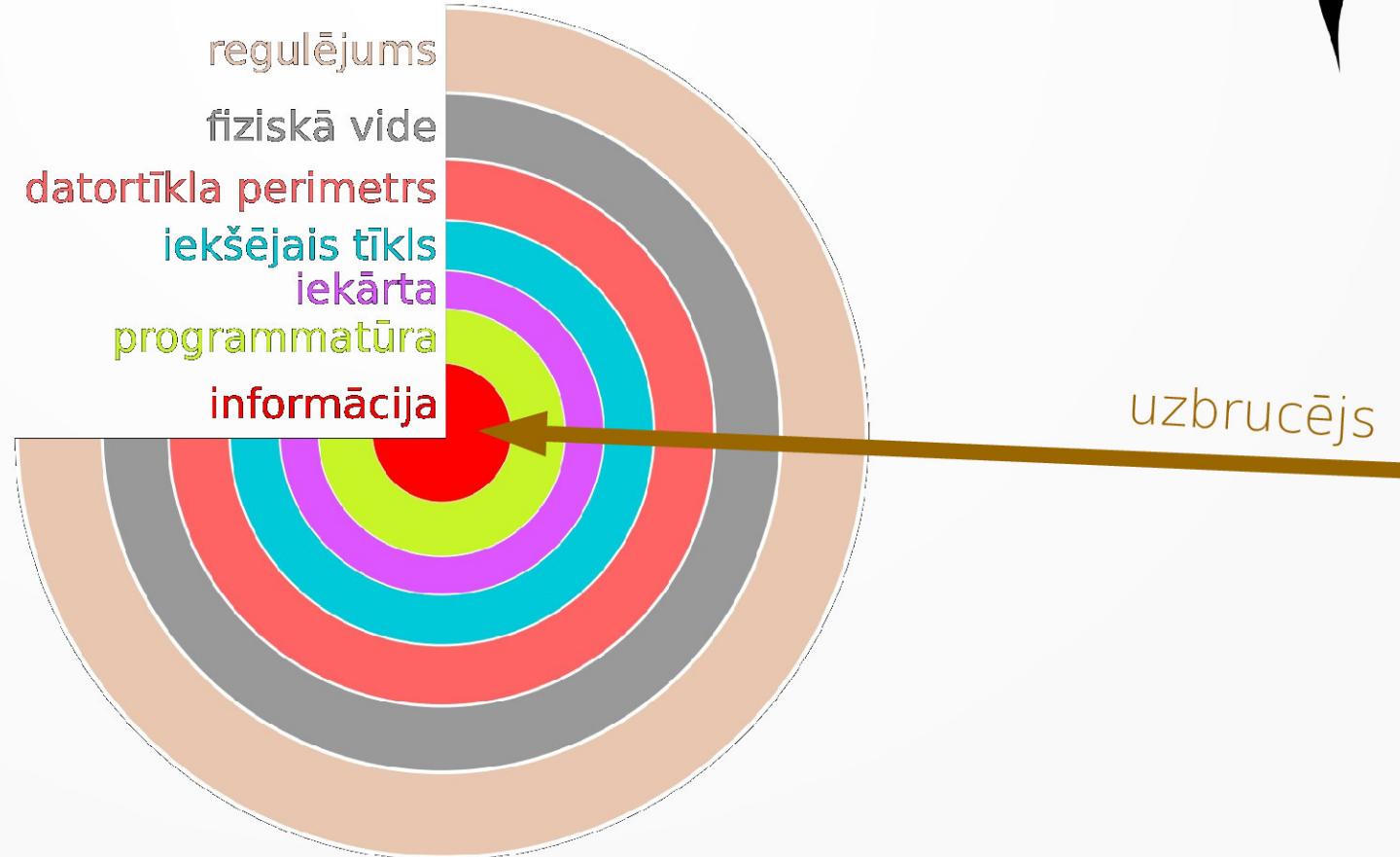
- informācijas noplūde
- ļaundabīgs kods
(ļaunatūra)
- paroļu uzbrukumi
- *backdoors*
- tīkla uzbrukumi
- ļaundabīgas ierīces
- fiziskie apdraudējumi
- sociālā inženierija
(cilvēka uzbrukumi)

„kāpēc es?”



- nejauša izvēle
 - “bērnelī”, jokdari
- augsta vērtība
 - konkurenti, organizētā noziedzība
- papildu kaitējums
 - valstu sponsorētie uzbrucēji u.c.

aizsardzība dzīlumā



kiberhigiēna



- paroles
- ugunsmūris
- antivīrus
- šifrēšana, glabājot datus
- šifrēšana, pārsūtot datus
- fiziskā drošība un modrība
- nē – nepazīstamām iekārtām
- nē – neatļautām iekārtām organizācijas tīklā
- ziņošana
- drošība visā informācijas dzīves ciklā
- sekošana jaunumiem

telefoni



- Telefona šifrēšana
- Drošs kods, otrs faktors
- Find My Device / Find My iPhone
- Izslēgt analītiku
- Ierobežot, ko var darīt neatbloķējot telefonu
- Nevērt valā negaidītus pielikumus
- Atjauninājumi
- Nepievienot neatļautas lietas pie citām sistēmām

droša programmatūras lietošana



- Instalē tikai to programmatūru, kas nepieciešama
 - darba iekārtās – saskaņo programmatūras instalēšanu ar IT dienestu
- Neatklāj programmatūrai pārāk daudz datu, ja neesi drošs, vai Tevis ievadītie dati nenonāk internetā!

attālinātais darbs



- Perimetra modelis vs galiekārtu modelis
- Savu iekārtu lietošana
- Videokonferences
- Savi tīkli
- Rezerves kopijas un šifrēšana
- Ziņo par šaubām!

komandējums



- Iekārta jānēsā līdzī
- Jāizvairās no savu paroļu ievades svešās ierīcēs
 - Ja tomēr tas nepieciešams, tad
 - jāatrod “logout” un
 - atgriežoties pie savas ierīces, jānomaina parole.
- Daudzfaktoru autentifikācija apgrūtinās īaundarim iespēju piekļūt kontam ar paroli vien

kā veidot paroli



- ļoti gara parole ir labāka par ļoti sarežģītu paroli
- To ir vieglāk atcerēties un vismaz tik pat grūti uzminēt
- Nebaidies no atstarpēm!
 - **rL@!xnN%/**
~ 5 000 000 000 000 000 minējumi
 - **Sniegav-ri malku c3rt, labi**
~ 100 000 000 000 000 000 000 minējumi, 20000x drošāka

kā lietot paroli



- Tava parole ir Tava parole.
- Nedalies ar citiem!
 - Arī ar priekšnieku nē.
 - Parole ir Tavs digitālais paraksts. Kā pēc tam pierādīsi, ka tas nebiji Tu?
- Un neprasi citu paroles.



possible.lv

IT drošības risinājumi

possible@possible.lv