CERT.LV

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

E-pastu uzturēšanas labā prakse

"Esi Drošs", 2019. gada 28. novembris
Andrejs Konstantinovs, andrejs@cert.lv

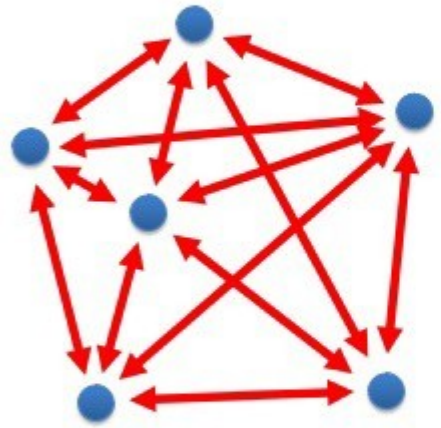
Epasti kā valsts nozīmes infrastruktūra

Salīdzinājums	Ceļi	Epasti
Īstermiņā var iztikt ar zemākas kvalitātes risinājumu?	Jā	Jā
Tehniski, varētu pat iztikt vispār bez X?	Jā	Jā
Iedzīvotāji, uzņēmumi un organizācijas paļaujas uz X?	Jā	Jā
Drošāks X veicina ekonomikas attīstību?	Jā	Jā
Patiesās izmaksas augstākas nekā varētu sagaidīt?	Jā	Jā

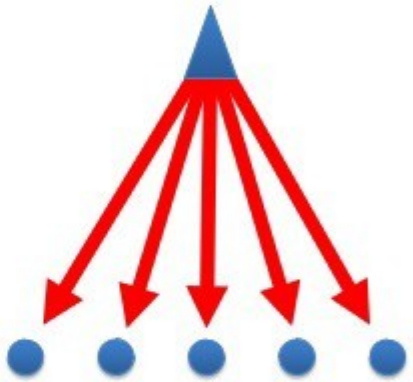
Epasti kā valsts nozīmes infrastruktūra

Salīdzinājums	Ceļi	Epasti
Īstermiņā var iztikt ar zemākas kvalitātes risinājumu?	Jā	Jā
Tehniski, varētu pat iztikt vispār bez X?	Jā	Jā
Iedzīvotāji, uzņēmumi un organizācijas paļaujas uz X?	Jā	Jā
Drošāks X veicina ekonomikas attīstību?	Jā	Jā
Patiesās izmaksas augstākas nekā varētu sagaidīt?	Jā	Jā
X iztstrādi / uzturēšanu var apgūt augstskolā?	**Jā**	**Nē**
Iespējams centralizēts risinājums situācijas uzlabošanai?	**Jā**	**Nē**

Decentralizācijas plusi un mīnusi



Decentralized
Peer-to-Peer

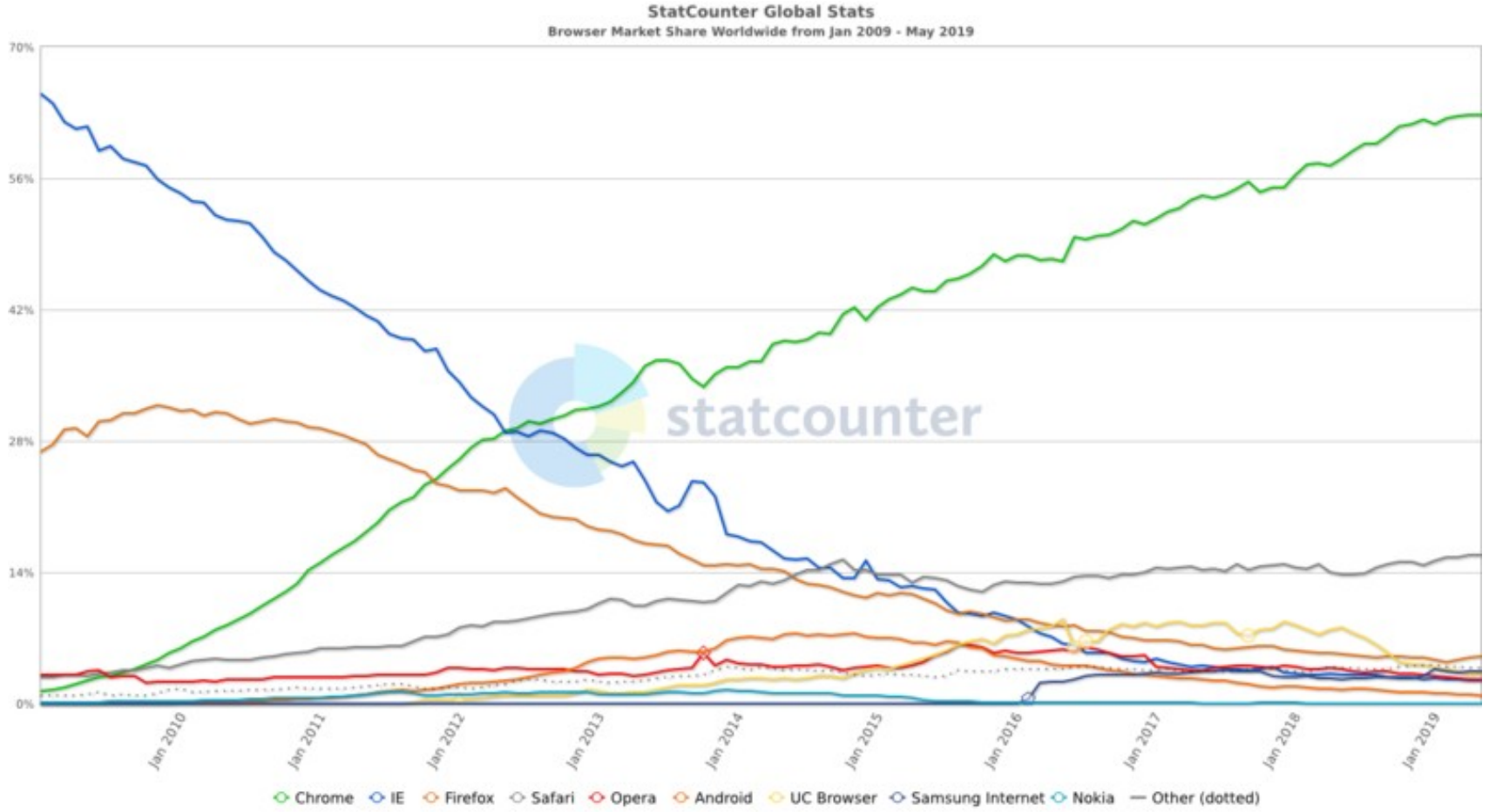


Centralized
Command & Control

- Plusi:
  - Pieejamība
  - Izturība
  - Neatkarība
  - Kļūdu tolerance
- Mīnusi
  - Heterogenitāte
  - Uzlabojumu opcionālitāte
  - Atpakaļsavietojamība
  - Inerce

https://medium.com/postcards-from-2035/centralised-and-decentralised-societies-compared-1336162fbe67

Epastu sistēmas atšķirības no WWW



https://gs.statcounter.com/browser-market-share#monthly-200901-201905

Paroļu politika

- Jābūt formalizētai, MK 442 noteikumu 15. pants ir labs sākums
- Nevar atstāt lietotāju pārziņā – jāvalidē servera pusē!
- Nozagto kredenciāļu datubāzes:
  - Have I Been Pwnd – var pieteikties paziņojumiem par visu domēnu
  - Firefox Monitor – labāks ieteikums gala lietotājiem
- Multifaktoru autentifikācija – web interfeisā
- Per-application tokens – epastu klientā

Paroļu politika (turp.)

"Mums konti tiek bloķēti pēc 3 login mēģinājumiem – kā kredītkartes"

- *Password spray attack* – pārbauda 1 paroli pret visiem epastiem
- Ar laika sprīdi, teiksim 3 login / 1 h:
  - 2 * 24 – mēģinājumi dienā bez bloķēšanas
  - 2 * 24 * 30 – **1500** mēģinājumi mēnesī bez bloķēšanas
- Bez laika sprīža (konts bloķēts pēc 3 secīgām kļūdām jebkurā laikā):
  - Lietotāji (vai viņu ierīces) logojas darba kontos vismaz reizi dienā == **laika sprīdis ir 24 h**
  - 2 * 5 – mēģinājumi nedē'ļā bez bloķēšanas
  - 2 * 5 * 52 – **500** mēģinājumi gadā bez bloķēšanas
- Ja kļūdas tiek skaitītas atsevišķi par IMAP/POP/SMTP – x3!

TLS politika

- Modifikācijas ar TLS pieejamas visiem protokoliem:
  - POP3 -> POP3S
  - IMAP4 -> IMAP4S
  - SMTP -> SMTPS, STARTTLS
- Pašparakstīti sertifikāti jāatstāj pagātnē!
  - Jāpievērš uzmanība, ka atšķirībā no web, epastu softs neatbalsta SNI
- Jābūt iespējai pārliecināties, ka lietotāji tiešām izmanto TLS!
  a) Aizliegt plaintext autentifikāciju (vis-2019'ākais risinājums)
  b) Sekot līdzi pieslēgumu veidiem caur žurnālfailiem/monitoringu
  c) Izplatīt konfigurācijas iestatījumus caur Autoconfig/Autodiscover mehānismiem

Žurnālfaili

- Jābūt pieejai (arī ja ārpakalpojums)
- Vismaz jābūt iespējai atbildēt uz jautājumiem:
  - Kas vēl sāņēma šo pikšķerēšanas epastu?
  - Pie kuriem epastiem vēl ir notikuši no X ip adreses vai Y valsts?
  - Pret kuriem lietotājiem šobrīd notiek vai iepriekš tika veikti brute-force uzbrukumi?
- Ideāli ir iespējams izveidot automatizāciju ar web-callback'iem:
  - Saņemt paziņojumus par svarīgiem notikumiem Slack/MM/Skype grupas chat'ā
  - Automātiski izveidot tiketu Jira vai citā uzņēmumā lietotajā sistēmā

Spam/Karantīna/Tegi/Filtri

- Jābūt ne-binārai iespējai starp “atmest” un “pieņemt”:
  - Mapes “spam” vai “karantīna”
  - Filtri/Label/Krāsu marķējums vai kāds cits funkcionāli līdzīgs mehānisms
  - Vismaz pievienot attiecīgos [Tegus] nosaukumā
- Lieliski, ja ir iespēja pievienot dažādus “tegus” ar atšķirīgu semantiku
  - Vismaz atšķirt “spam” no (potenciāliem) viltojumiem
- Ideāli, ja ir iespēja mainīt tegus (vai pārcelt epastus) retroaktīvi

SMTP Authentication & Open relays

- SMTP Relay – epastu serveris piedāvā pārsūtīt epastus caur sevi
- Visvienkāršākais veids, kā nodrošināt epastu izsūtīšanu no:
  - Mājaslapām
  - Automatizētiem servisiem, botiem
  - IoT ierīcēm (piem. printeriem)
- **Nav droši**, bez autentifikācijas jebkurš serviss / iekārta var izsūtīt epastus arī no neeksistējošām vai kādam citam piederošām adresēm
- Pilnīgi *Open relays* vairs nav palikuši, bet pati *smtp relay* tipa konfigurācija joprojām ļoti populāra, tikai ar IP ierobežojumiem

Client security

- A/V vai Endpoint Security – labi, bet nav pietiekami
- Savlaicīgi atjauninājumi – kritistki svarīgi
  - MS Outlook ievainojamības ar publiski pieejamiem RCE efekta eksploitiem:
    - CVE-2017-11774
    - CVE-2018-0950
  - Mozilla Thunderbird:
    - Nav zināmi eksploiti, bet ievainojamības arī ir: CVE-2018-12376, CVE-2018-18501
    - Jāņem vērā, ka tas ir bāzēts uz novecojuša Firefox dziņa un netiek aktīvi atjaunots
    - Zerodium cenas par Thunderbird exploitiem ir zemāka salīdzinot ar Outlook
- AD domēnos jāpārliecinās, ka SMB trafiks ārpus domēna tiek bloķēts

Pikšķerēšana (phishing)

- Daudziem asociējas ar primitīvām spam kampaņām
  - Svešvalodā vai latviešu valodā, bet ar acīmredzamām “Google Translate” sekām
  - Bezpersonisks vēstījums
  - Jokaini pielikumi, šausmīgs dizains, neticams vēstījums, URL neatbilst minētajiem servisiem
- Bet tās nav obligātās pazīmes! Rezultatīvākās pikšķerēšanas kampaņas neatbilst nevienam no šiem punktiem.
- Arī klasiskais padoms – vērīgi pārbaudīt sūtītāja epasta adresi un salīdzināt to ar kādu iepriekšējo epastu – nav pietiekams dēļ:
  1) BEC (Business Email Compromise)
  2) Epastu viltošanas

Epastu viltošana

Epastu vēstule cilvēku redzējumā ->

<- Epastu vēstule adminu skatījumā

Aizsardzības mehānismi

Hronoloģiskā kārtībā:

- SPF (2006) – šobrīd visbiežāk sastopamais
  - Nepieciešams komunikācijai ar Gmail, Outlook365 vai citiem “interneta milžiem”
  - Ieviešanai pietiek ar viena DNS ieraksta izveidi (validācijai gan nepieciešams atbalsts serverī)
  - Lietojot bez DMARC - pārbauda tikai ārējo adresātu, ne to kuru redz cilvēks
- DKIM (2011) – nepieciešams atbalsts no servera puses
  - Izmanto kriptogrāfiju, lai droši parakstītu visus domēna izejošos epastus
  - Lietojot bez DMARC – pasargā pret modifikāciju, bet ne pret pilnīgi jauna epasta izsūtīšanu
- DMARC (2015) – ielāps abām iepriekš minētajām tehnoloģijām

Aizsardzības mehānismi (turp.)

- DMARC – noteikti jāievieš (arī ja domēnam epasti netiek lietoti!)
- Ja epasti tiek lietoti, jāievieš arī viens no:
  - DKIM (vēlams, bet nepieciešams serveru atbalsts gan izsūtītājiem, gan saņēmējiem)
  - SPF (visplašāk atbalstīts un vienkāršāk ieviešams, bet sniedz vājākas garantijas)
- Ja pie DMARC klāt pieslēgti abi DKIM un SPF, tad epasti tiks pieņemti, ja nostrādā vismaz viens no viņiem!
- Visas minētās tehnoloģijas var strādāt pagaidu/testēšanas režīmā:
  - SPF - “Softfail” (~ALL)
  - DMARC - “p=none”
  - DKIM - “o=~” vai “t=y”

Thank you!

http://www.cert.lv

baiba.kaskina@cert.lv