



CERT.LV ieteikumi attālinātā darba organizēšanai

"Esi drošs", 24.03.2020

Andrejs Konstantinovs

CERT.LV raksts



English

Meklēt ...



Ziņas Par mums Incidenti Kontakti Arhīvs

Valsts un pašvaldību iestādēm

Likumi un MK noteikumi

IT drošības pārvaldība

Kad ziņot par incidentu vai drošības nepilnību?

Interneta pakalpojumu sniedzējiem

Normatīvais regulējums

Rīcības plāns

Atbildīgs IPS

Kritiskās infrastruktūras uzturētājiem

Jaunumi

COVID-19 negatīvi ietekmē arī kibertelpas drošību

COVID-19 pandēmijas ietekme jūtama ne vien fiziskajā pasaulē, bet arī kibertelpā. Ļaudari valdošo krīzes situāciju un organizāciju pāriešanu attālinātā darba režīmā nekautrējas izmantot savā labā - gan peļņas gūšanai, gan spiegošanai. Tādēļ aicinām šajā periodā būt īpaši piesardzīgiem un rūpēties arī par savu kiberhigiēnu.

[2020-03-20] **Aktualitātes**

CERT.LV ieteikumi attālinātam darbam ārkārtas situācijas apstākļos

Ieteikumi attālinātā darba organizēšanai, informācijas aprītei un glabāšanai ārkārtas situācijas apstākļos.

[2020-03-17] **Ieteikumi lietotājiem**

Kiberlaikapstākļi

Februāris 2020

- Krāpšana
- Ļaunatūra & ievainojamības
- Ielaušanās un datu noplūde
- Pakalpojuma pieejamība
- Lietu internets

Kalendārs

- 24. marts
[Seminārs "Esi drošs"](#)
- 26. marts

- <https://cert.lv/lv/2020/03/cert-lv-ieteikumi-attalinatam-darbam-arkartas-situacijas-apstaklos>

Kas nepieciešams attālinātajam darbam?

Komunikācija:

- Videokonferences
- Epasti
- Čati
- Telekonferences

Darba procesu pielāgošana:

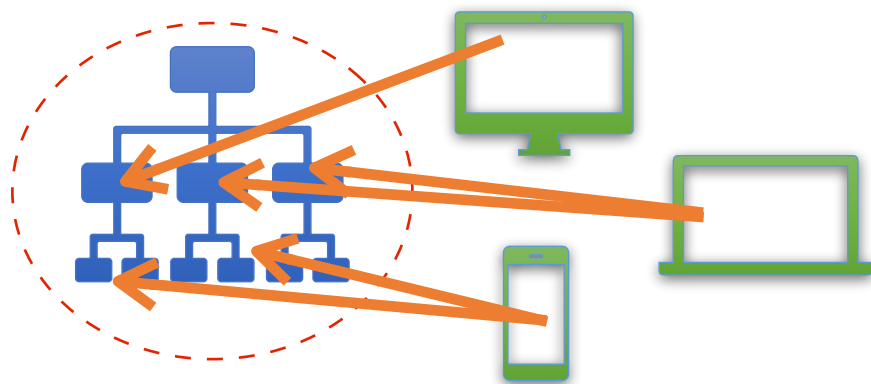
- Printēšana
- Paraksti

Iekšējie servisi:

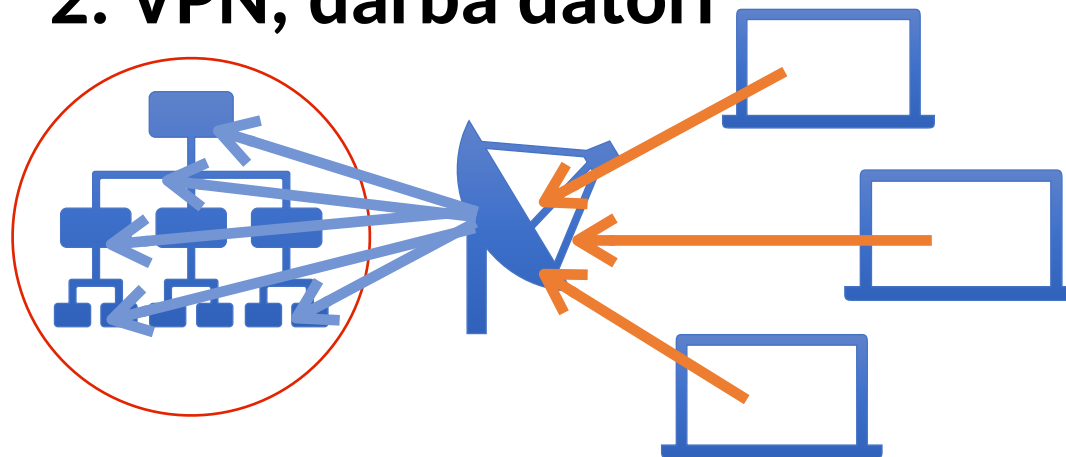
- Sharepoint
- Confluence
- ERP
- CRM
- Legacy
- Pašu izstrādāti risinājumi
- Telefoni

Attālinātā darba topoloģijas

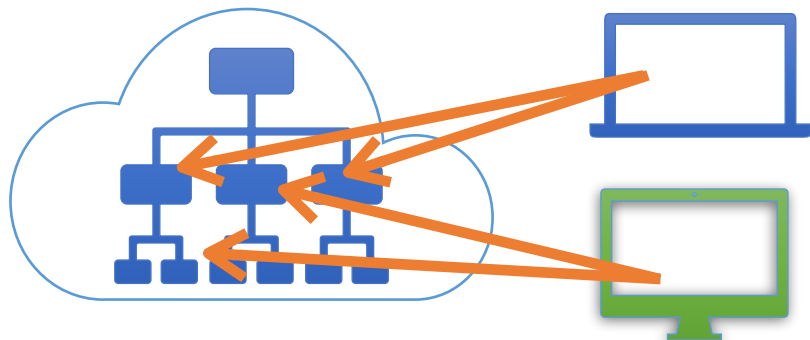
1. Atslēgts ugunsmūris



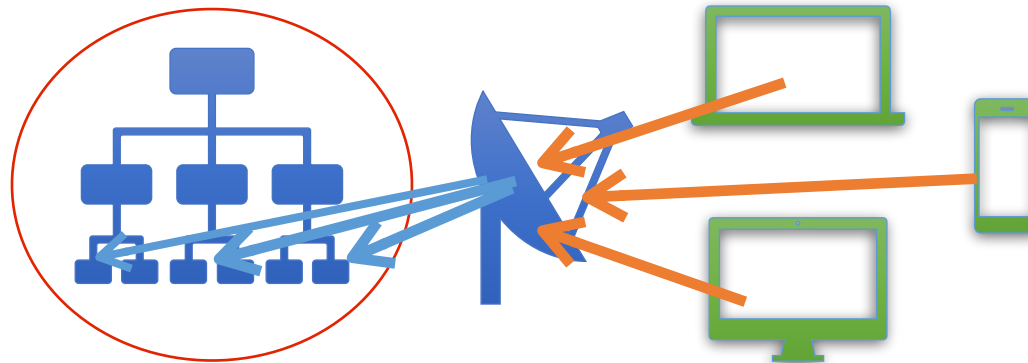
2. VPN, darba datori



3. Mākoņ tehnoloģijas / "Zero trust"

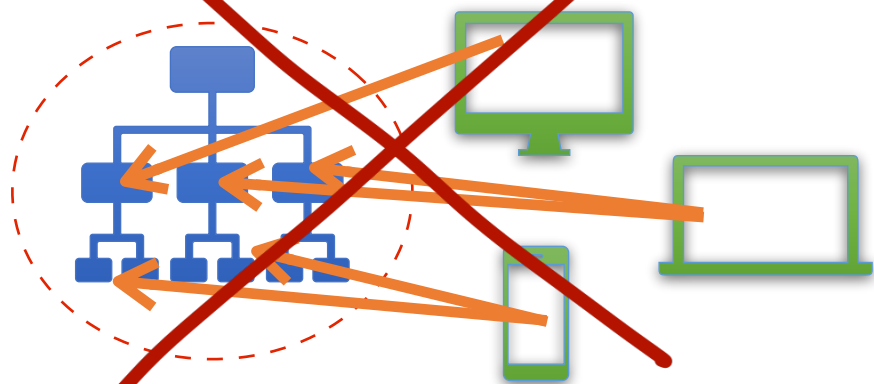


4. VPN -> RDP, lietotāju datori

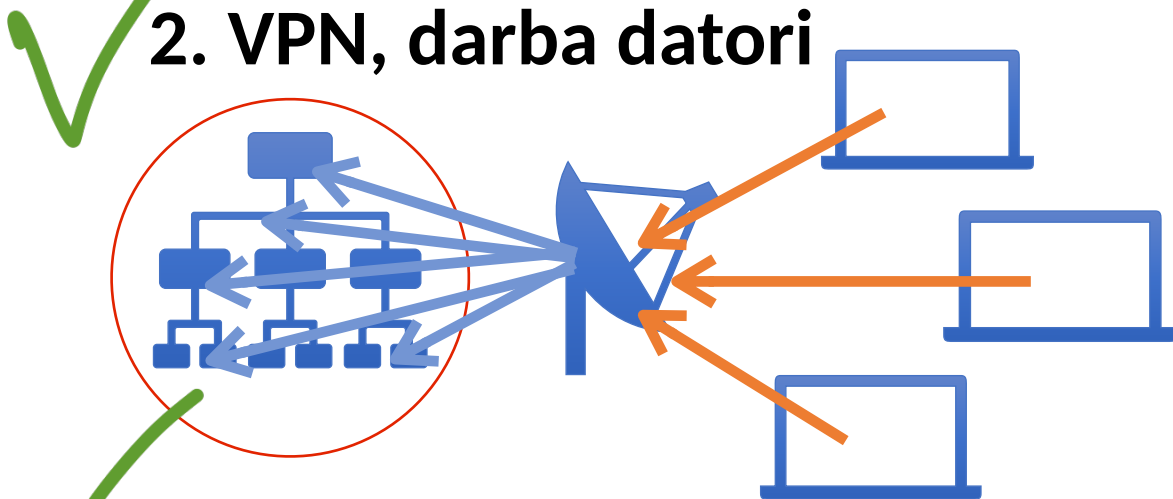


Attālinātā darba topoloģijas

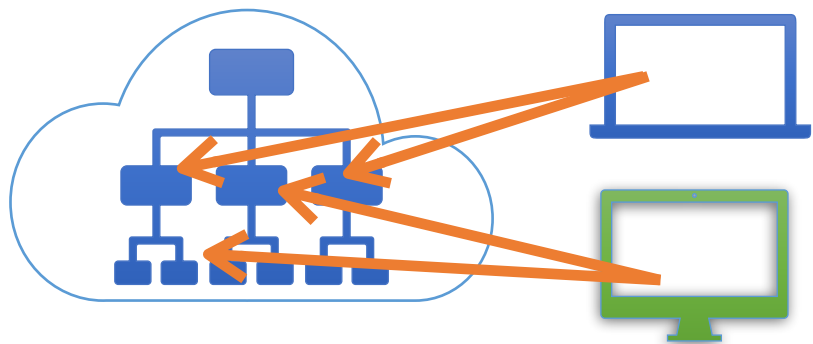
~~1. Atslēgts ugunssmūris~~



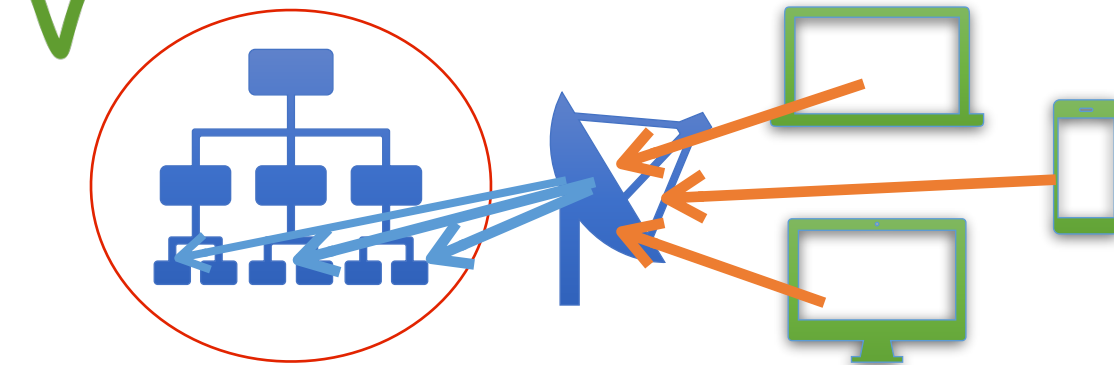
2. VPN, darba datori



3. Mākoņ tehnoloģijas / "Zero trust"



4. VPN -> RDP, lietotāju datori



VPN drošība

- Atvērti tikai porti, kas vajadzīgi VPN darbībai
- Autentifikācija caur sertifikātiem
- Žurnālfaili:
 - Ielogošanās mēģinājumi (veiksmīgi + neveiksmīgi)
 - Sessiju garums, trafiks (netflow)
- Ierobežota piekļuve VPN (LV diapazoni: nic.lv/lix)
- **Arī VPN (gan softam, gan appliances) nāk atjauninājumi!**
- Vairāk par IPSEC konfigurācijas detaļām: <https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/vpns>

Ar datoriem līdzņemšanai

- Automātiska pieslēgšanās pie iestādes VPN (vai Direct Access)
- Jāpielāgo tīkla profili un ugunsmūris - darbinieku datoros
- Jāpielāgo tīkla konfigurācija - iestādē:
 - Caur VPN parasti IP adreses tiek iedalītas jaunā diapazonā
 - No VPN izdalītām IP adresēm jāspēj piekļūt pie resursiem
 - Iespējams jāpielāgo monitorings korektai trafika analīzei
- Lai samazinātu trafiku, var sūtīt caur VPN tikai daļu no tā

Bez datoriem līdzņemšanai

- Ieteicamais risinājums - lietotāji slēdzas caur RDP/VNC pie saviem darba datoriem ofisā
- RDP/VNC konekcijas jāpasargā ar VPN
- Publiskajā internetā jābūt redzamam tikai VPN portam (vai integrētam risinājumam, piem. *Apache Guacamole*)
- Risinājuma attīstība:
 - Remote Desktop Gateway
 - Citrix

Riski saistībā ar privāto iekārtu lietošanu

- Iekārtas neatbilst uzņēmuma IT drošības politikai
 - Ja jānodrošina lietotāju atbalsts: ~~Remote Desktop~~, Remote Assistance / Quick Assist
- Iekārta var būt koplietojumā ar radniekiem/bērniem
- Darbinieki izmanto dažādas OS veidus un versijas, dažādas programmatūras versijas:
 - nesaderība
 - drošības caurumi
 - autortiesību ierobežojumi
- Iekārtas tiek izmantotas arī privātiem epastiem, soc. tīkliem
- Lielāka ļaunatūras, t.sk. šifrējošo izspiedējvīrusu varbūtība
- Iestādes vadībai jābūt informētai par šiem riskiem!

legādājoties datorus līdzņemšanai

- Jāizvērtē prasības pret:
 - ātrdarbību
 - integrācijām ar esošajiem risinājumiem
 - iebūvēto funkcionalitāti & iespēju pieinstalēt trešo pušu programmatūru
- Ja ir iespējams:
 - Windows 10 S
 - Chrome OS

Web servisu aizsardzība

- iespējot auditēšanas opcijas, veikt monitoringu; jāatpazīst:
 - parolu minēšana
 - ievainojamību skenēšana
- izmantot Web Application Firewall
- pasargāt servisu ar TLS šifrēšanu
 - valīdi bezmaksas sertifikāti - [Let's Encrypt](#)
- papildus autentifikācija web-servera līmenī - lietotāju sertifikāti