Aktuālie izaicinājumi un risinājumi kibernoturības un darbības nepārtrauktības plānošanā

Vitālijs Rakstiņš, LSM, RSU

Kas ir noturība?

- organizācijas spēja ilgtspējīgi uzturēt un nodrošināt plānotos biznesa procesus / rezultātus, neskatoties uz notikumiem digitālajā vidē;

- **spējas** sagatavoties dažādiem satricinājumiem vai katastrofām (**all-hazard approach**), pretoties tiem, reaģēt uz tiem (un arī pielāgoties, transformēties krīzē) un atgūties no tiem;

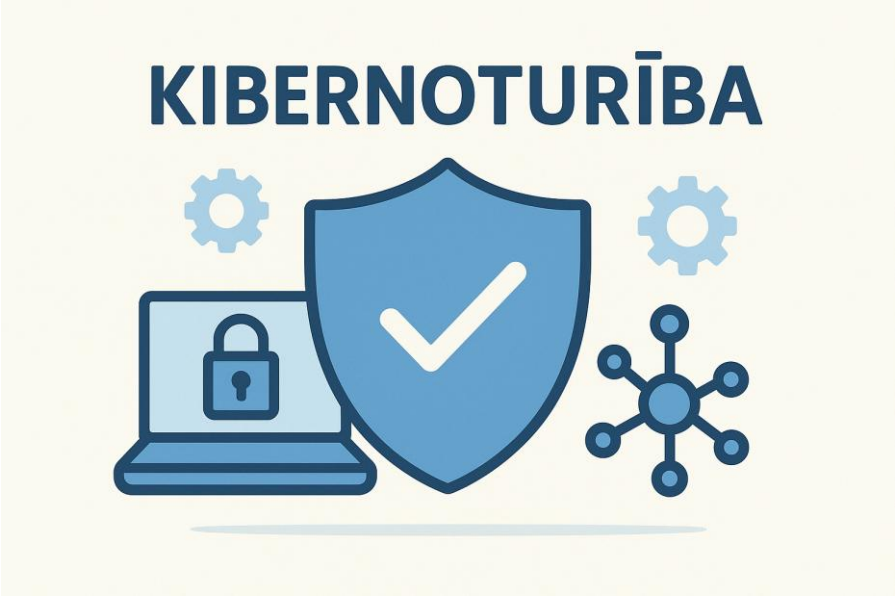
- Nevienu objektu / sistēmu nav iespējams aizsargāt no dažādu veidu apdraudējumiem ilglaicīgi / visu laiku!

- Fokuss uz kritisko pakalpojumu / funkciju nepārtrauktību;

- Noturība ir **aktīvā rīcība** adaptācijai un transformācijai;

- Noturība nav konkrēta riska novēršanas stratēģijā, drīzāk integritātes stiprināšana pret daudziem apdraudējumiem;

- Nepieciešams veidot spējas, kas nav balstītas tikai uz riskiem, bet veidot arī iekšējās spējas/rezerves (scenāriju pieeja), lai spētu funkcionēt jebkādā krīzē



BCP & SoS

NATO septiņas noturības pamatprasības:
1) valdības un kritiski svarīgu pakalpojumu nepārtrauktības nodrošināšana;
2) noturīga energoapgāde;
3) spēja efektīvi risināt nekontrolētas cilvēku pārvietošanās problēmas;
4) noturīgi pārtikas un ūdens resursi;
5) masveida cietušo aprūpe;
6) noturīgas civilās sakaru sistēmas;
7) noturīgas civilās transporta sistēmas

ES:
--Kiberdrošības akts
-NIS 2 direktīva / DORA
-Kritiski svarīgu struktūru noturības direktīva (CER)
-Digitālo pakalpojumu akts,
-Kiberdiplomātijas rīku kopums,
- Nīniste (Niinistö) ziņojums un ES
- Sagatavotības stratēģija

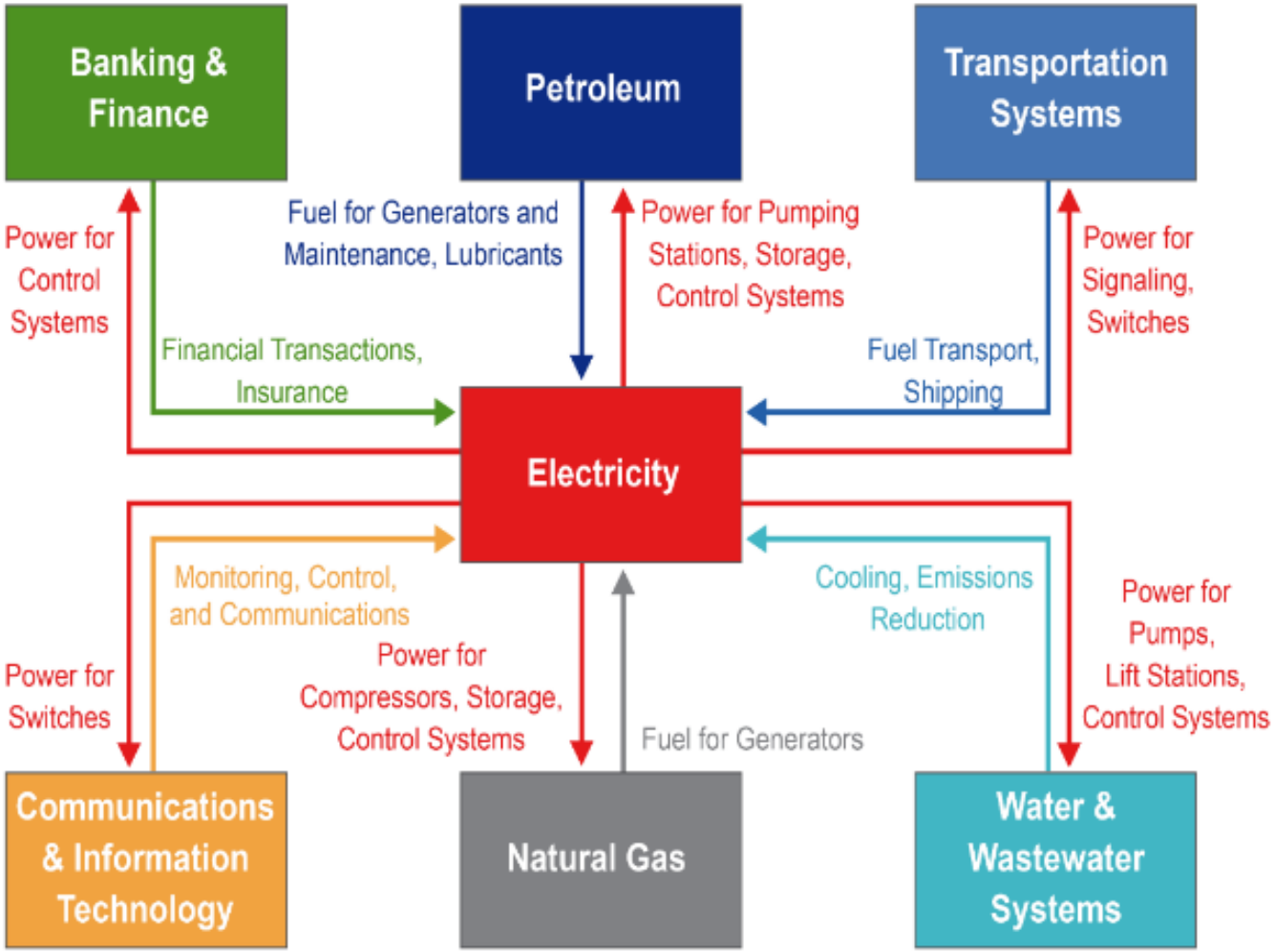
OECD ieteikumi
uzņēmumiem nodrošināt uzņēmējdarbības nepārtrauktību:
-nodrošinot, ka kritiskā infrastruktūra un informācijas sistēmas darbojas arī pēc satricinājuma;
Darbības noturība = kā uzņēmējdarbības veicinātājs

Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību (2017)

- [..] Vienotais kiberdrošības tirgus:
  - ES kiberdrošības sertifikācijas satvars:
    - drošība kritiskās vai augsta riska līmeņa lietotnēs
    - kiberdrošība digitālajos produktos, tīklos, sistēmās un pakalpojumos
    - integrētās drošības metožu izmantošana lietu interneta ierīcēm
  - Nozaru kiberdrošības prasības (finanšu, enerģētika, transports, veselība…)

IZAICINĀJUMS: visu iniciatīvu (starptautisko, ES, nacionālo, industrijas) koordinācija / savietojamība

Darbības nepārtrauktības plānošana



Atslēgšanās no BRELL tīkla = reality check

- Ģeneratoru pieejamība
- Degvielas piegāde
- Apkope/remonts
- Prasmes
- Piegādātāji
- Loģistika

Kaskadējošie efekti

Major cyberattack on Ukrainian mobile operator disrupts banking services and air raid sirens

By Sean Lyngaas, CNN

4 min read · Updated 9:36 PM EST, Tue December 12, 2023

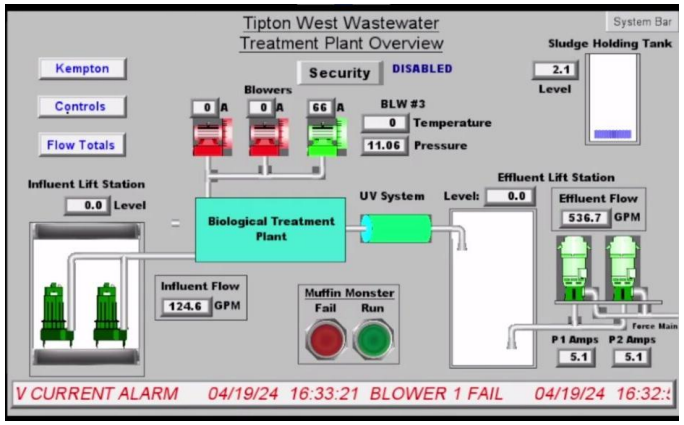
Largest cyberattack on Ukraine's state registers: Ministry of Justice systems shut down

IVAN DIAKONOV — FRIDAY, 20 DECEMBER 2024, 00:46

THE MOSCOW KREMLIN. PHOTO: GETTY IMAGES

Ukraine has experienced the largest cyberattack on government registries in recent times. The operation of key Ministry of Justice systems has been temporarily suspended as a result of the attack conducted by Russian hackers. The hackers claimed to have destroyed all data they gained access to, including backup copies stored on servers in Poland.

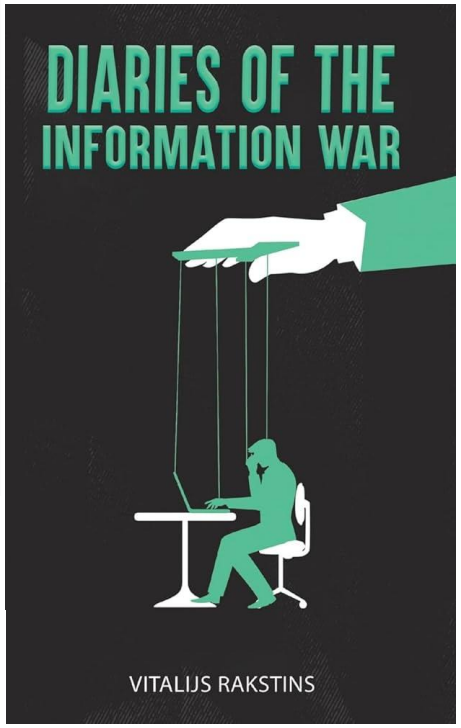
Apdraudējums

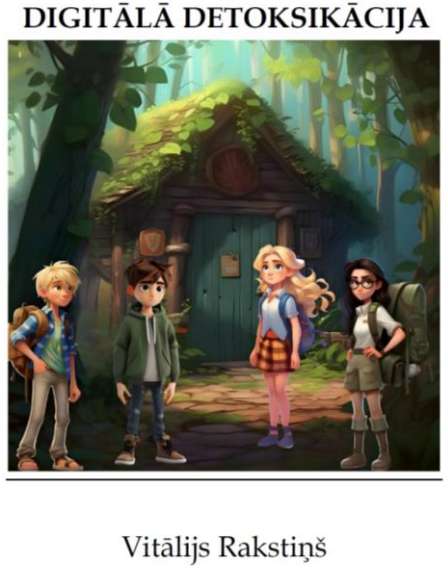


- Ievainojamības (Attack Surfaces) eksponenciāli pieaug;
- graujošo tehnoloģiju (ģeneratīvā mākslīgā intelekta, kvantu tehnoloģiju) nekontrolētā izplatība;
- piegāžu ķēžu drošība / noturība
- aktoru skaits turpina pieaugt
- kibernoziegumi kā pakalpojums (Cybercrime as a Service)
- Graujošo tehnoloģiju nekontrolētā izplatība
- Daudz standartu (t.sk. nesavienojamo / outdated);
- Iepirkumi / programmēšana «pa taisno»
- «Nedraudzīgo valstu» programatūra, lietotnes, sistēmas, mākoņi
- Pārrobežu standartu (sertifikācijas) savstarpējā atzīšana;
- Sertifikācijas standarti ierīcēm un pakalpojumiem;
- Kompleksa risinājumi (kinetiski / digitāli / DNP);
- **Piegāžu drošība - iepirkumi un monitorings: apakšnieki, trešās puses, pakalpojuma sniedzēji (Tier 1, Tier 2, Tier 3)**
- Lietu internets (Ali Express, Temu etc.)
- Sadarbības kultūra!
- Divējādā lietojuma tehnoloģiju aprite (end user)

Kā motivēt MVU investēt kiberdrošībā un noturībā?

- Nepieciešams investēt:
  - lai būtu daļa no starptautiskās ekosistēmas
  - lai kvalificētos publiskiem iepirkumiem;
  - Lai kvalificētos apdrošināšanai u.tml.
- Piegādātājs / apakšnieks «vienmēr būs vainīgs»;
- Daļa no kiberdrošības pasākumiem neprasa lielus resursus;
- Reputācija un sociāla atbildība





Cilvēks joprojām centrā

- Mindset
- Uz cilvēku orientēta pieeja kiberdrošībai (human-centric approach to cyber security);
- Sadarbības kultūra = cilvēku sadarbība;
- Sabiedrības plašāks akcepts kiberdrošības ierobežojumiem;
- Atbildības personificēšana;
- Indivīdiem pašiem jāuzņemas lielāka atbildība par savu kiberdrošību;
- Atturēšanas efekts (visas sabiedrības noturība liedzot sasniegt uzbrucēja mērķus (“kopīga atbildība”).


MANA LATVIJA
MANA ATBILDĪBA