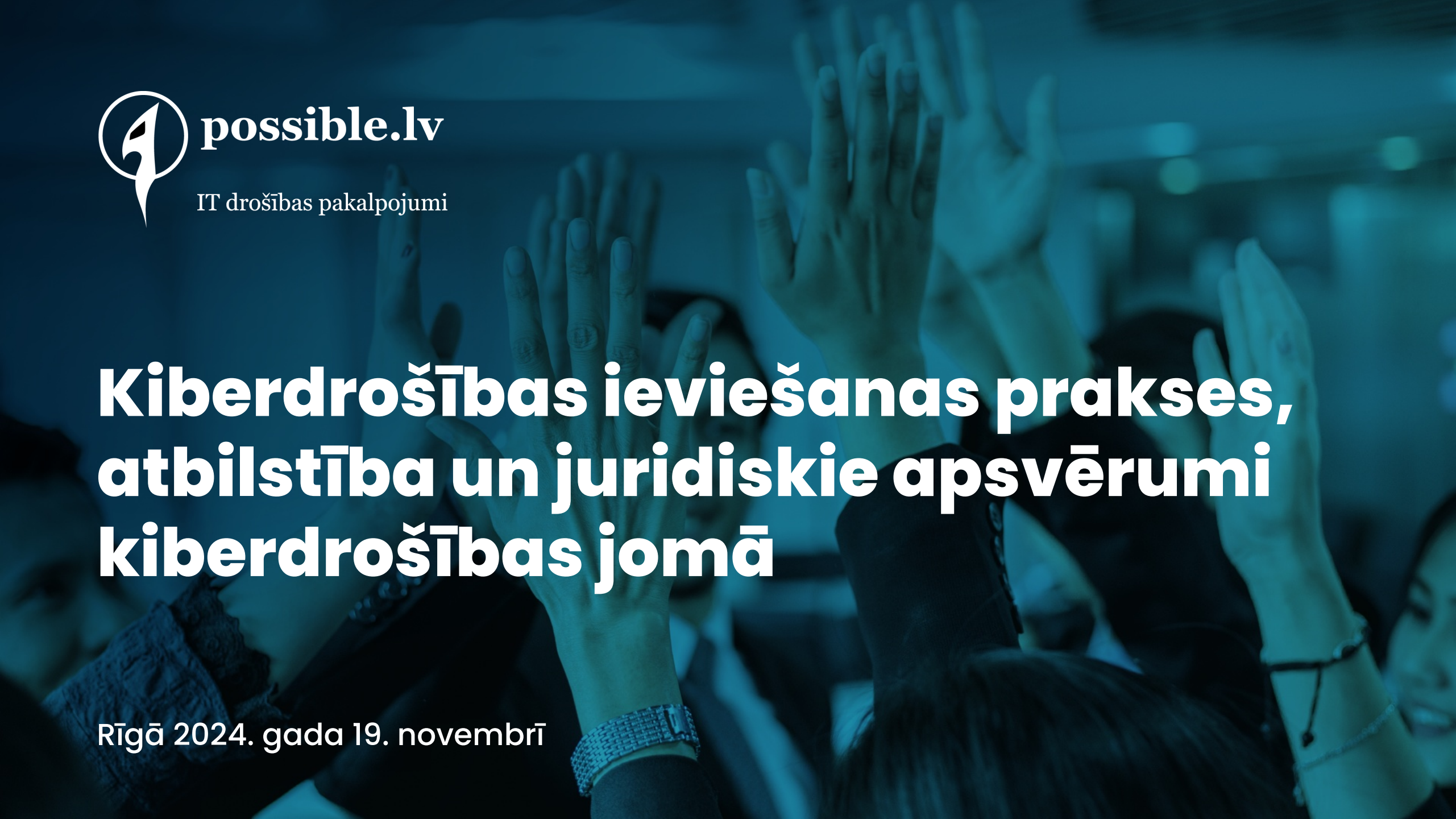


possible.lv

IT drošības pakalpojumi

Kiberdrošības ieviešanas prakses, atbilstība un juridiskie apsvērumi kiberdrošības jomā

Rīgā 2024. gada 19. novembrī

Mg.sc.comp, Mg.phys Kirils Solovjovs

- *Possible Security* vadošais pētnieks
- Baltās cepures hakeris
  - Tīkla plūsmas analītika
  - Reversinženierija
  - Sociālā inženierija
  - Klientu konsultācijas
- https://kirils.org/
- Mastodon: @k@masts.lv

Possible Security

- Specializēts kiberdrošības uzņēmums
- Augstākā līmeņa pakalpojumi
- Biznesa virzieni:
  - Ielaušanās testi, *Red Team* uzbrukumu simulācijas
  - Ievainojamību pētniecība, reversā inženierija
  - Konsultācijas
  - IT drošības apmācības
  - e-Saeima un e-RīgasDome

Saturs

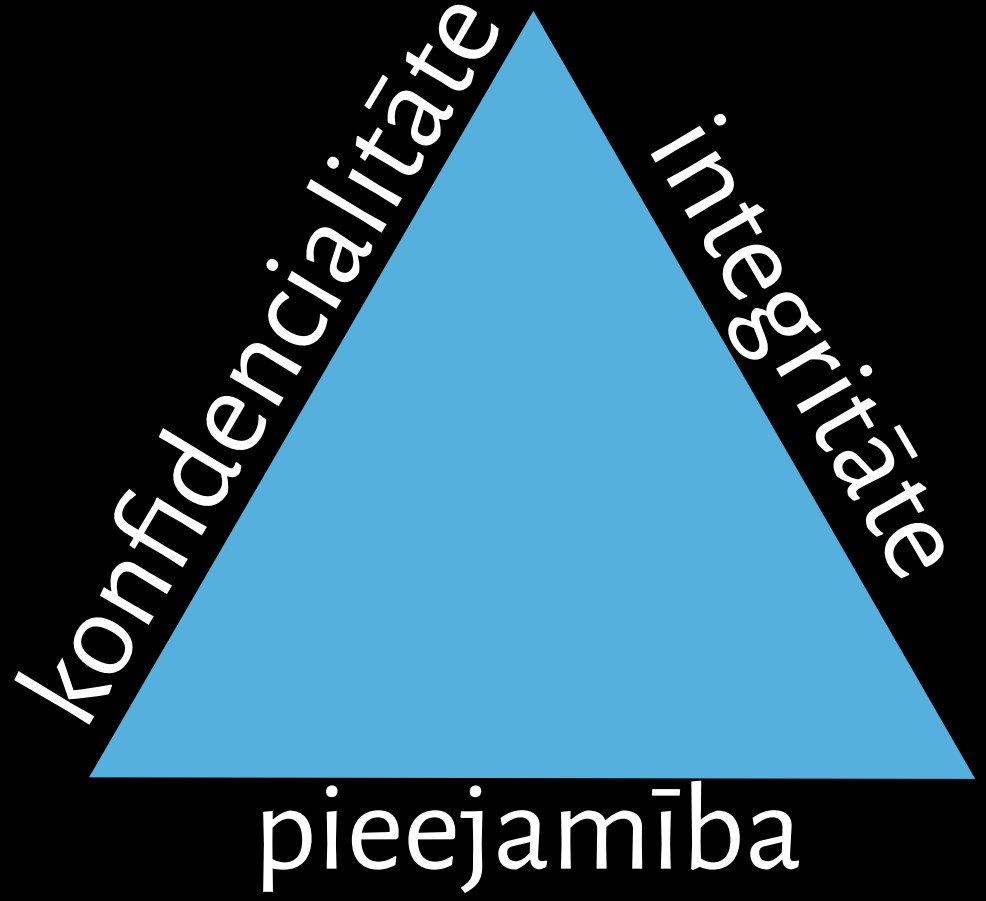
- Kiberdrošības pamati
- Kiberdrošības instrumenti un to ieviešana
- Kiberdrošības juridiskie aspekti
- Kiberdrošības nākotnes tendences

Temata aktualitāte

Avots: 14.02.2014. Security, Protection, Antivirus image. https://pixabay.com/photos/security-protection-antivirus-265130/

Definīcijas

Informācijas drošība (CIA)



Apdraudējumi

Apdraudējums

Iekšējie apdraudējumi

- Cilvēku apdraudējumi
  - Ļaunprātīgi
  - Nejauši
- Tehnoloģiski apdraudējumi
- Vides apdraudējumi

Ārējie apdraudējumi

- Cilvēku apdraudējumi
  - Ļaunprātīgi
  - Nejauši
- Tehnoloģiski apdraudējumi
- Vides apdraudējumi

Avots: 01.2014. Classification of security threats in information systems - ResearchGate. https://www.researchgate.net/publication/315714820_Classification_of_security_threats_in_information_systems

Biežākie apdraudējumi

- Konfigurācijas nepilnības
- Ļaundabīgs kods
- Ielaušanās mēģinājumi
- Krāpniecība

Avots: 08.02.2024. CERT.LV https://cert.lv/uploads/parskati/cert-ceturksna-C4-atskaite-2023-LV-v4-3.pdf

Apdraudējumu meklēšana un modelēšana

- Apdraudējumu meklēšana — meklē eksistējošos apdraudējumus
- Apdraudējumu modelēšana — apdraudējumu ietekmes novērtēšana un tās mazināšanas stratēģijas

Metodes risku novērtēšanai

- Resursu apzināšana
- Risku noteikšana
- Risku analīze un novērtēšana
- Drošības testi

Resursu apzināšana

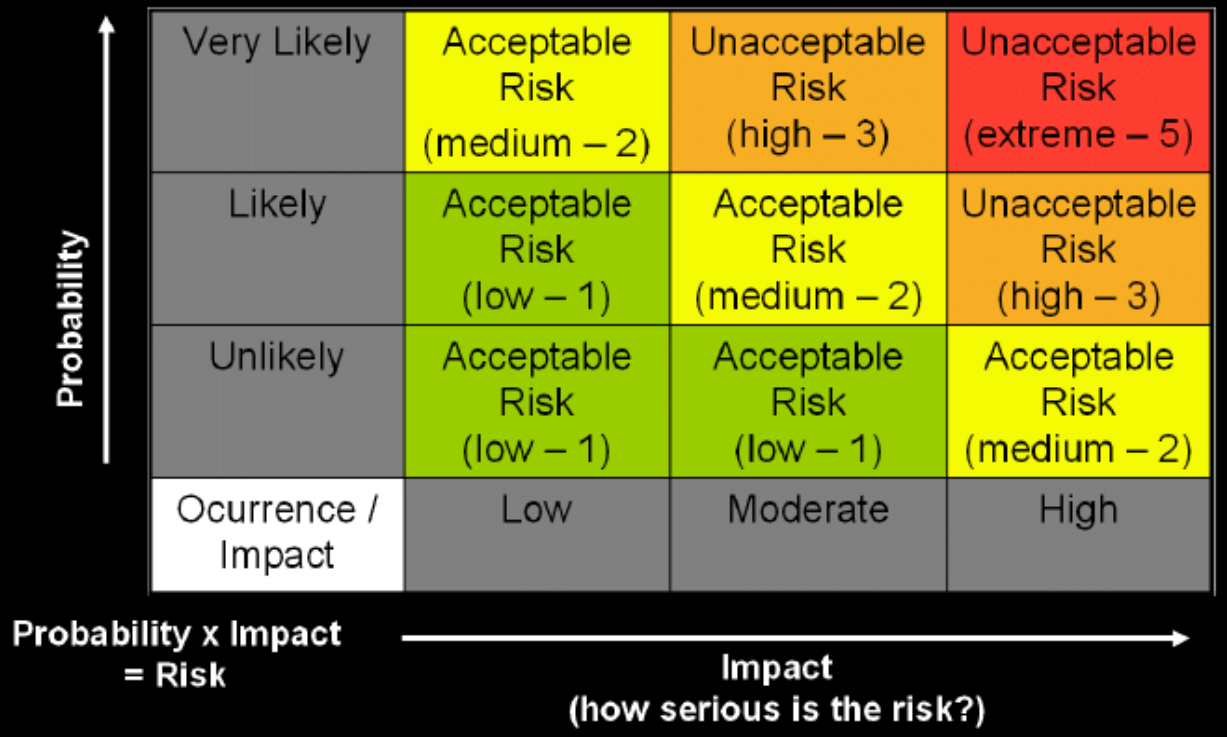
- Dokumentācija
- Inventarizācija
- Intervijas ar tehniskajiem darbiniekiem

Risku noteikšana, analīze un novērtēšana

- Riski izriet no resursiem un to apdraudējumiem
- Apdraudējuma avoti
- Kādi ir apdraudējumi?
- Kādas būs apdraudējuma sekas?
- Cik liela varbūtība, ka risks iestāsies?
- Kā to varētu novērst?

Metodes risku novērtēšanai

Risks = varbūtība X ietekme



Avots: 10.2014. Managing e-Learning Content Development Risks - ResearchGate. https://www.researchgate.net/figure/Qualitative-Risk-Matrix-Probability-x-Impact_fig3_275155519

Drošības testi

- Uzbrukuma simulācija IT resursiem
- Tīmekļa lietotņu, servisu un citas programmatūras drošības testēšana
- Atrasto ievainojamību izmantojamības pārbaude
- Rekomendāciju sagatavošana problēmu novēršanai
- Ziņojums un sanāksme tā apspriešanai

Praktiskais darbs

Dota situācija — jūs vēlaties savā pašreizējā darba vietā uzlabot kiberdrošību, ieviešot jaunus drošības mehānismus. Individuāli atbildēt uz jautājumiem par situāciju.

Praktiskais darbs

- Kāda ir pašreizējā kiberdrošības situācija uzņēmumā? Novērtējiet skalā no 1 līdz 10. Pamatojiet vērtējumu.
- Kāda ir vēlamā kiberdrošības situācija uzņēmumā? Novērtējiet skalā no 1 līdz 10.
- Kādi kiberdrošības apdraudējumi pastāv uzņēmumam?

Praktiskais darbs

- Kuri kiberdrošības apdraudējumi ir iekšējie apdraudējumi, kuri ir ārējie? Ja nepieciešams, papildiniet apdraudējumu sarakstu.
- Kuri apdraudējumi atstāj vislielāko ietekmi uz CIA uzņēmumā? Pamatojiet savu atbildi.
- Veiciet aptuvenas aplēses, cik daudz resursus uzņēmums zaudēs, ja piepildīsies apdraudējums ar vislielāko ietekmi.

Kiberdrošības ieviešana

Kiberdrošības instrumenti

- Kiberdrošības stratēģijas
- Drošības politikas
- Atjauninājumi
- Rezerves kopijas
- MFA un drošas paroles
- Drošības auditi
- Regulāras darbinieku apmācības

Biežākie šķēršļi ieviešanā

- Zināšanu un prasmju trūkums
- Nevēlēšanās apgūt jaunus instrumentus
- Resursu trūkums
- Neprecīzi risku novērtējumi

Ieviešanas efektivitātes rādītāji

Veiktspējas rādītājiem izvēlētajam kiberdrošības risinājumam (KPI)

- Pamanītie ielaušanās mēģinājumi
- Pamanītie drošības incidenti
- Vidējais drošības incidenta piefiksēšanas laiks
- Vidējais drošības incidenta atrisināšanas laiks
- Izmaksas pret ieguvumiem

Atbilstība un juridiskie aspekti

- ES kiberdrošības akts
- Vispārīgā datu aizsardzības regula
- NIS2 direktīva
- Nacionālais kiberdrošības likums

Atbilstība un juridiskie aspekti

ES kiberdrošības akts (2019)

- ENISA (Eiropas Savienības Kiberdrošības aģentūra)
- IKT produktu, servisu un procesu standartizācija
- Minimālās drošības prasības IKT pakalpojumu sniedzējiem

Vispārīgā datu aizsardzības regula

- Tehniskie un organizatoriskie pasākumi personas datu aizsardzībai

Atbilstība un juridiskie aspekti

NIS2 direktīva

- Instruments EU kopējās kiberdrošības uzlabošanai
- Minimālās drošības prasības kritisko pakalpojumu sniedzējiem
- EU valstu sadarbība kiberincidentu gadījumā

Nacionālais kiberdrošības likums

- Latvijas IKT drošības uzlabošana
- Minimālās drošības prasības dažādām pakalpojumu sniedzēju grupām

Praktiskais darbs

- Izvēlieties kādu kiberdrošības instrumentu, kas visefektīvāk varētu samazināt lielāko kiberdrošības risku ietekmi vai piepildīšanās varbūtību. Pamatojiet savu atbildi.
- Aprakstiet tā ieviešanas stratēģiju. Kādi departamenti jāiesaista, kādas izmaiņas jāveic esošajos procesos?

Praktiskais darbs

- Kā jūs pamatotu savai priekšniecībai izmaiņas procesos un ieguldījumus, kas jāveic, lai ieviestu kiberdrošības uzlabojumus?
- Kā jūs pamatotu saviem padotajiem izmaiņas procesos, ja tās skartu viņus?

Praktiskais darbs

- Kā jūs zināsiet, ka ieviestais kiberdrošības instruments ir efektīvs? Kādas pazīmes par to liecinās?
- Kādas darbības būtu jāveic, lai ilgtermiņā nodrošinātu šī instrumenta efektivitāti?

Nākotnes tendences

- Normatīvo aktu attīstība
- Mākslīgais intelekts
- Kvantu skaitļošana

Papildus avoti

- Nacionālais kiberdrošības likums
  - http://eja.lv/3ub
- Ekonomikas ministrijas padomi uzņēmumiem
  - http://eja.lv/3td
- CERT.LV vispārīgi kiberdrošības ieteikumi un rīki
  - https://cert.lv/lv/ieteikumi-un-riki

possible.lv

IT drošības pakalpojumi

Paldies par uzmanību!

https://kirils.org/
Mastodon: @k@masts.lv