



Funded by the
Erasmus+ Programme
of the European Union

Küberturvalisuse sissejuhatus

Taustalugu – 4. tööstusrevolutsiooni väljakutsed

Safeguarding against Phishing in the age of 4th Industrial Revolution

www.cyberphish.eu

This project has been funded with support from the European Commission.

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



Õppe-eesmärgid



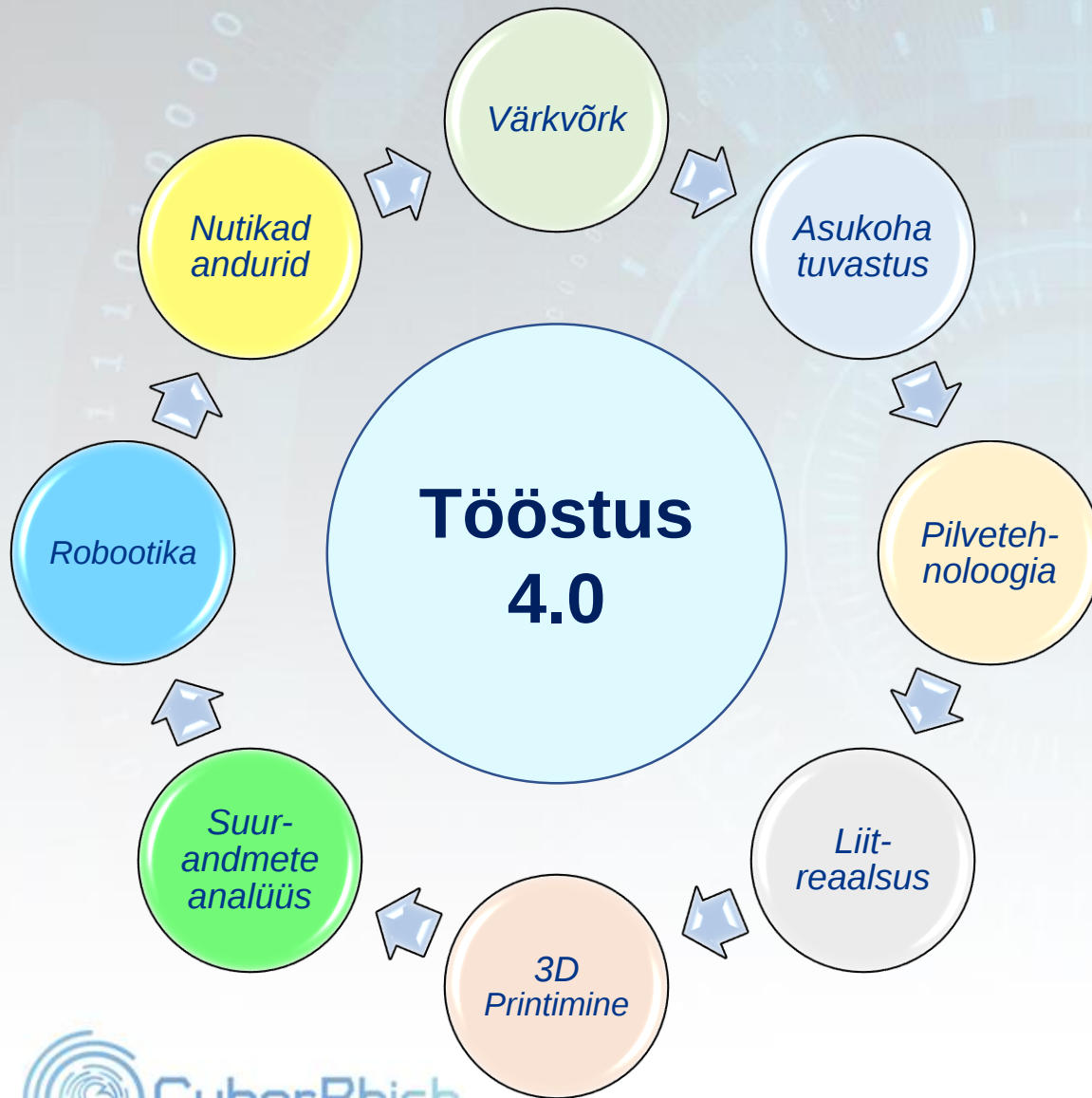
- On teadlik küberturvalisuse kontseptsioonist ja ettevõtete ees seisvatest küberturbe väljakutsetest.
- Mõistab küberturvalise valdkonna arengut ja suurenenud tähtsust viimastel aastatel tööstus 4.0 tulekuga.

Õpilase töökoormus



Loengud	1,5 h
Audio- ja videomaterjal	1,5 h
Juhtumiuuringud	1,5 h
Lisalugemine	4 h
Eksamiks valmistumine	1,5 h

Tehnoloogia meie ümber



Tarkvara ja infosüsteemid mängivad olulist rolli inimelu erinevates valdkondades

Vajadus kaitsta teavet muutub kohustuseks mitte ei ole enam valik

Definitsioon *Infoturve*

Alternatiivsed mõisted

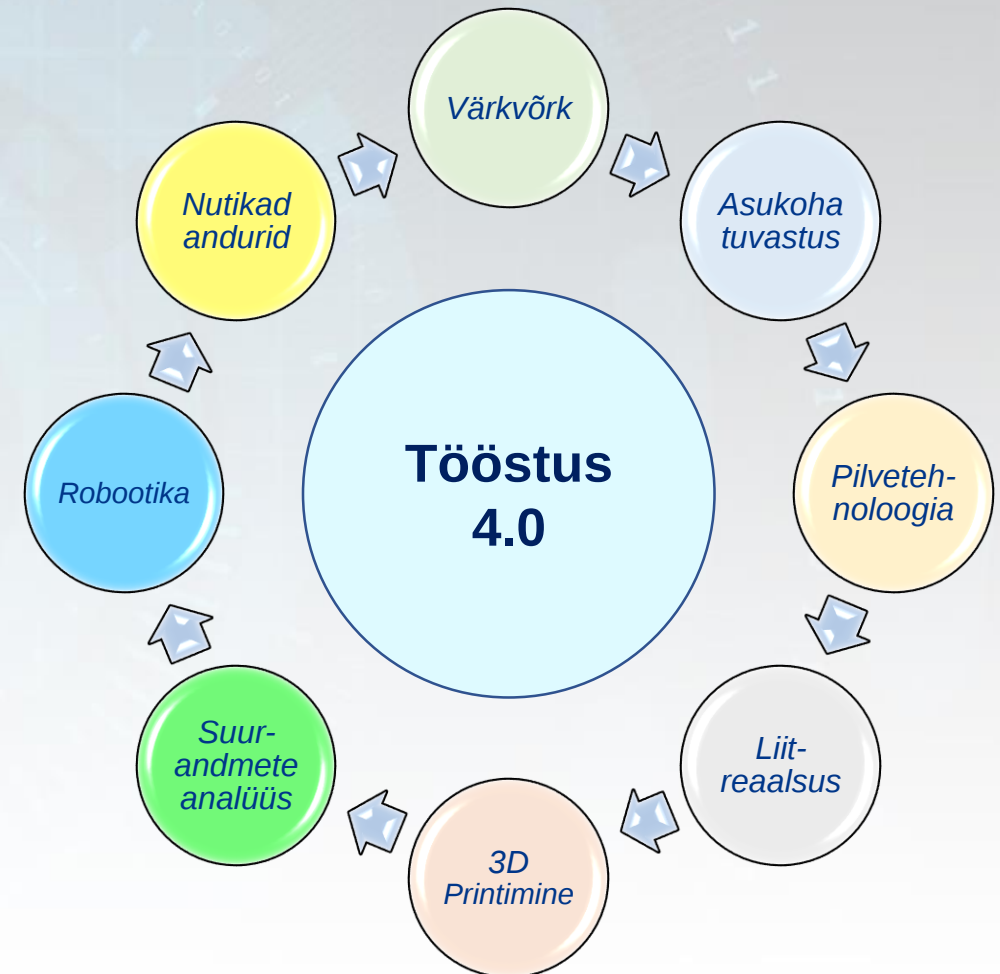
Küberturvalisus, Arvutiturve, infotehnoloogiaturve või IT-turvalisus

Tänapäeval on andmete turvaline töötlemine peaaegu kõigi ettevõtete ja asutuste jaoks eksistentsiaalse tähtsusega. Seejuures võivad andmed olla salvestatud nii paberile, arvutitesse kui ka töötajate mälusse. Andmete kaitseks ei piisa ainult tehniliste turvameetmete rakendamisest. Nõuetele vastavat infoturbe taset on võimalik saavutada ja säilitada vaid kõigi asjaosaliste plaanipärase ja organiseeritud tegevusega. Turvameetmete otstarbekohase rakendamise ning efektiivsuse kontrollimise eelduseks on süstemaatiline tegutsemisviis. Seda planeerimis-, suunamis- ja kontrollifunktsiooni nimetatakse infoturbe halduseks või ka IT-turbe halduseks.

https://iske.ria.ee/8_06/ISKE_kataloogid/5_Kataloog_B/B1/B_1.0

Loenguteemad

- Ettevõtluse väljakutsed
- Küberturvalisuse rünnakute kasv
- Tehnoloogia kasutamine ja turvaprobleemid
 - Värkvõrk
 - Pilvetechnoloogia
 - Tark infrastruktuur
 - Tark kodu
 - Plokiahela tehnoloogia
 - Suurandmete analüüs
- Kasvavate ohtudega kaasa arenemine
- Riiklikud ohud



Ärivaljakutsed

- Digirevolutsioon
- Pilveandmed
- Seadusandlus
- Automatiseerimine
- Värkvõrk
- Integratsioon ja uuendused
- Tehisintellekt ja masinõpe



- Kaugtöö võimaldamine
- Andmehaldus
- Mobiilsus
- Sotsiaalmeedia
- Projekti juhtimine
- Infrastruktuuri muudatused
- Puudulik tehniline väljaõpe

Ärivaljakutsed

- Digirevolutsioon
- Pilveandmed
- Seadusandlus
- Automatiseerimine
- Värkvõrk
- Integratsioon ja
- Tehisintellekt ja masinõpe



Kolmanda osapoole risk – risk, mis tuleneb organisatsiooni sidemetest väliste osapooltega äriiga seotud tarnete või teenuste pakkumisel

- *Seadusandluslik vastavus*
- *Rahaline*
- *Töökorralduslik*
- *Maine*
- *Strateegiline*

<https://hyperproof.io/resource/author/hyperproof-team/>

- Kaugtöö võimaldamine
- Andmehaldus
- Mobiilsus
- Sotsiaalmeedia
- Projekti juhtimine
- Ühiskondlike väärtuste muudatused
- Inimline väljaõpe

Ärivaljakutsed

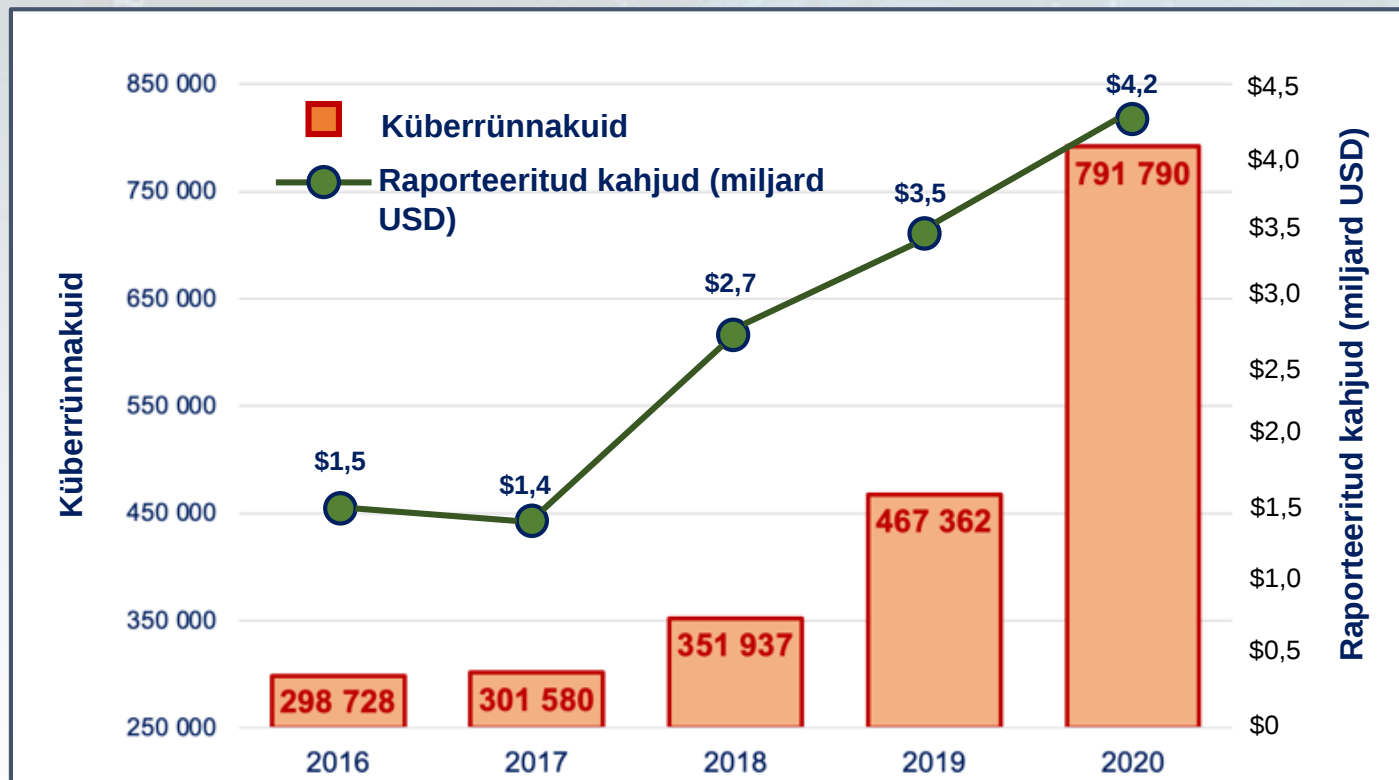
- Digirevolutsioon
- Pilveandmed
- Seadusandlus
- Automatiseerimine
- Värkvõrk
- Integratsioon ja uuendused
- Tehisintellekt ja masinõpe



- Kaugtöö võimaldamine
- Andmehaldus
- Mobiilsus
- Sotsiaalmeedia
- Projekti juhtimine
- Infrastruktuuri muudatused
- Digiline väljaõpe

Infoturve

Küberturvalisuse rünnakute kasv

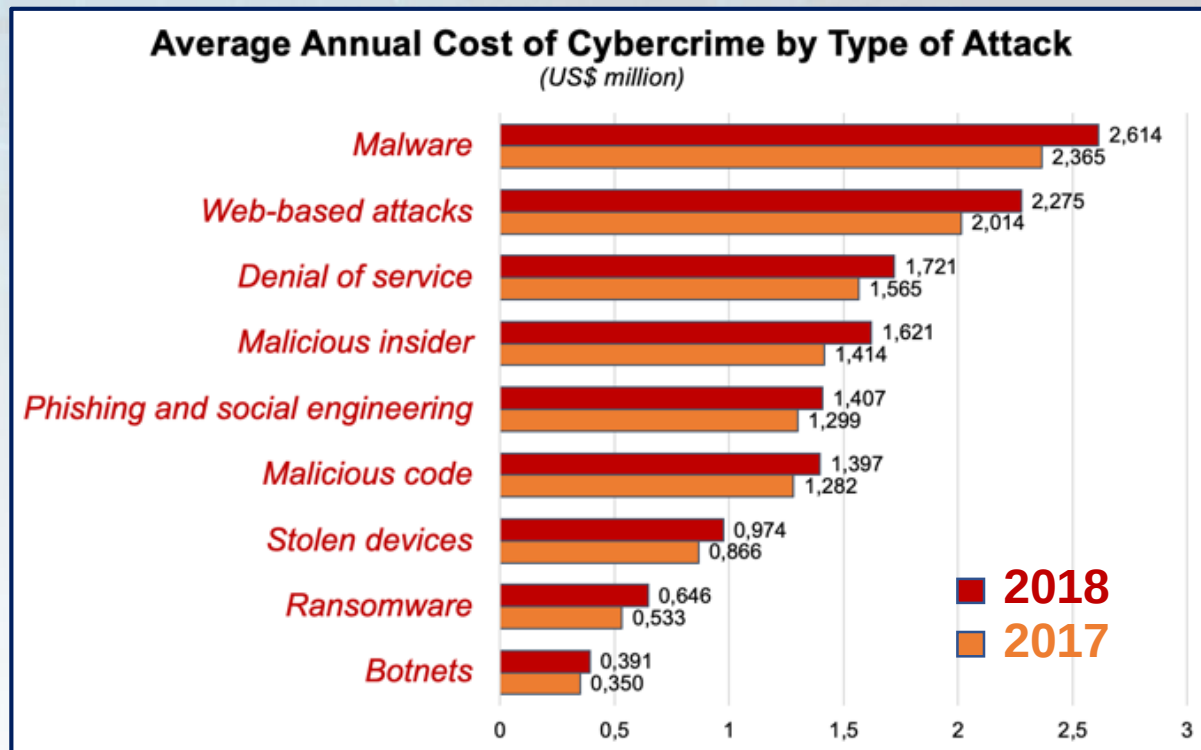
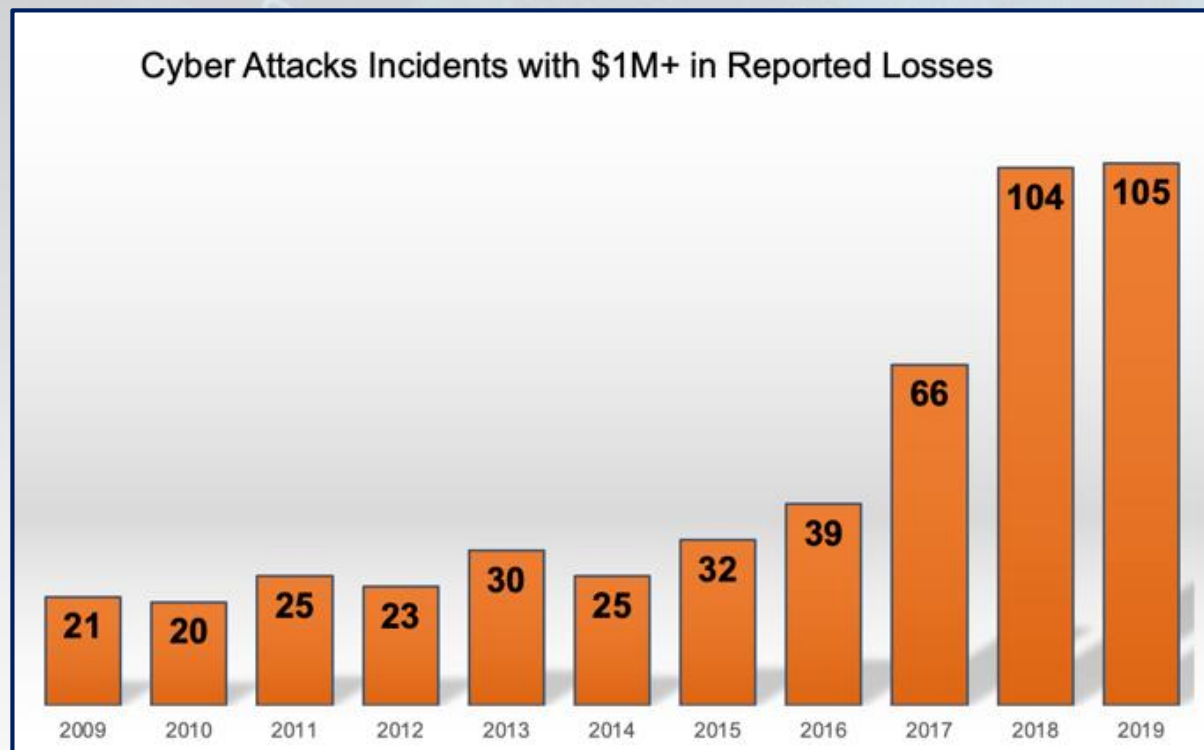


- Sihitud ründed
- Kaugtöö riskid
- Piisab kui väike arv langeb ohvriks
- Pettused arenevad edasi
- Kurjategijad müüvad varastatud teavet
- Kannatlikkus ja visadus tasuvad end ära
- Kurjategijad võivad tegutseda kõikjal

<https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime>

<https://www.forbes.com/sites/forbestechcouncil/2019/12/23/seven-reasons-for-cybercrimes-meteoric-growth/?sh=17cfbc8c5fa2>

Küberturvalisuse rünnakute maksumus



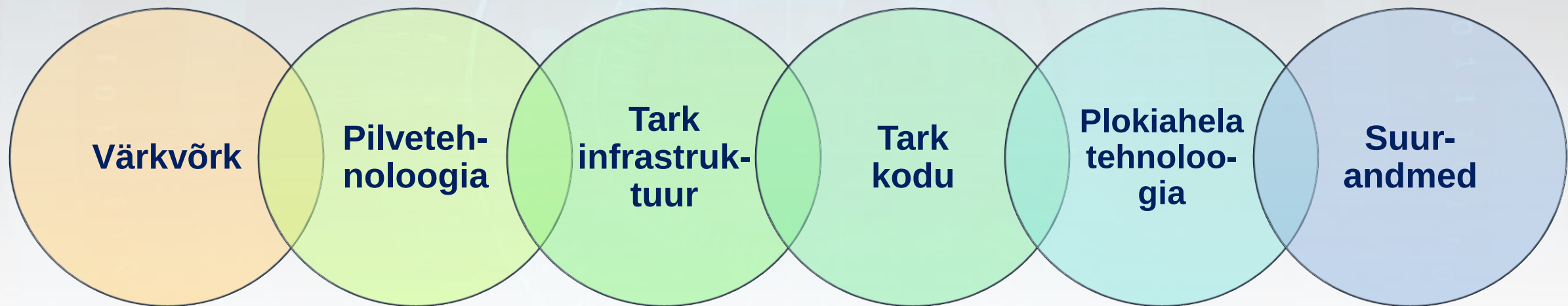
Viimase kümnendi jooksul – **490** olulist küberintsidenti

2018 kokku = US\$ **13** miljonit

<https://sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade/>

<https://www.digitalmarketingcommunity.com/researches/ninth-annual-cost-of-cybercrime-research-2019/>

Küberturvalisuse väljakutsed
Mobiilse tehnoloogia laialdane kasutamine



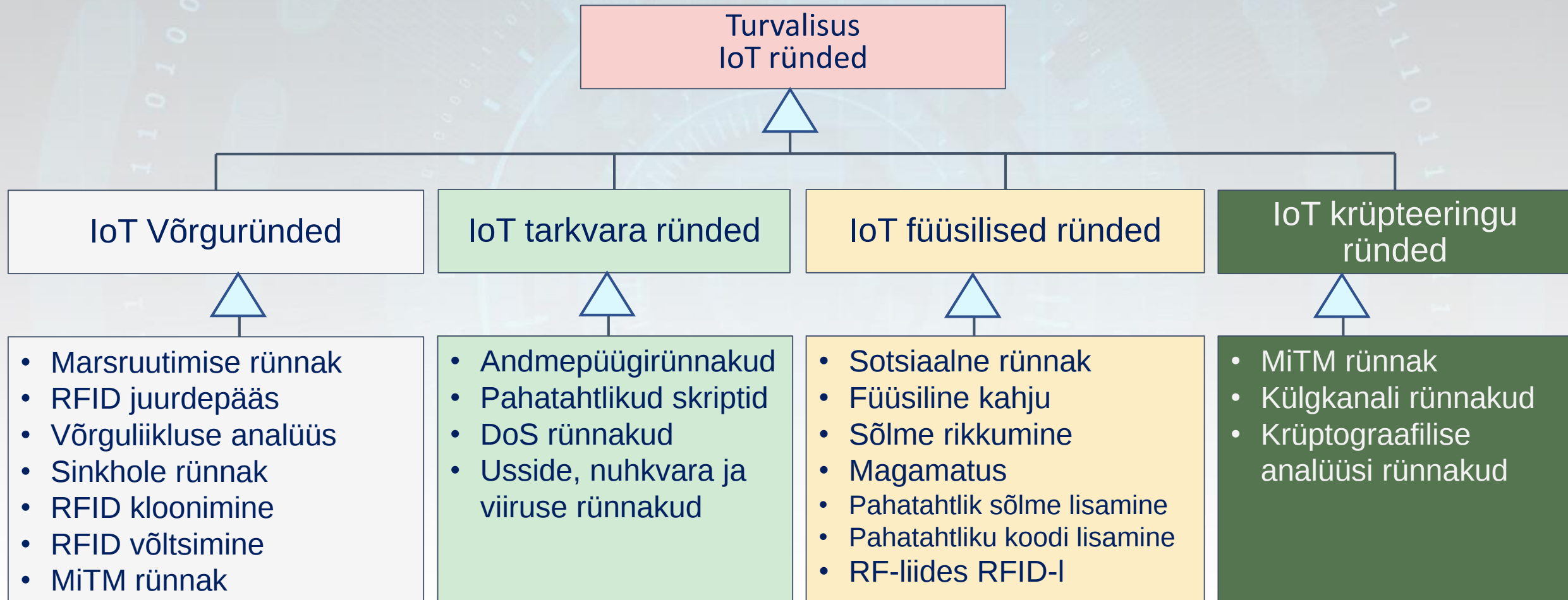
Värkvõrk ehk **Asjade internet (IoT)** kirjeldab füüsiliste objektide võrku, mis on manustatud andurite, tarkvara ja muude tehnoloogiatega, et luua Interneti kaudu ühendust ja vahetada andmeid teiste seadmete ja süsteemidega.

- "Asjad", st tehnoloogiad, seadmed, objektid, loomad või inimesed
- Sidevõrgud, mis seadet ühendavad
- Arvutivõrgud andmete voogesituse kaudu Internetist seadmesse

Aasta	Maakera rahvaarv (miljard elanikku)	Internetiga ühendatud seadmeid (miljardites)	Suhe
2003	6,3	0,5	0,08
2010	6,8	12,5	1,84
2015	7,2	25	3,47
2020	7,6	50	6,58

Küberturvalisuse väljakutsed

Värkvõrk



Küberturvalisuse väljakutsed
Pilvetehnoloogia



Küberturvalisuse väljakutsed

Pilvetechnologia

Sülearvutid

Serverid

Telefonid

*Pilvandmetöötluse kuritarvitamine
ja väärkasutus*

Liidesed ja ebaturvaline API

Sisemised ohud

Ühistehnoloogiatest tulenevad probleemid

Teabe kadumine või lekkimine

Seansi või teenuse kaaperdamine

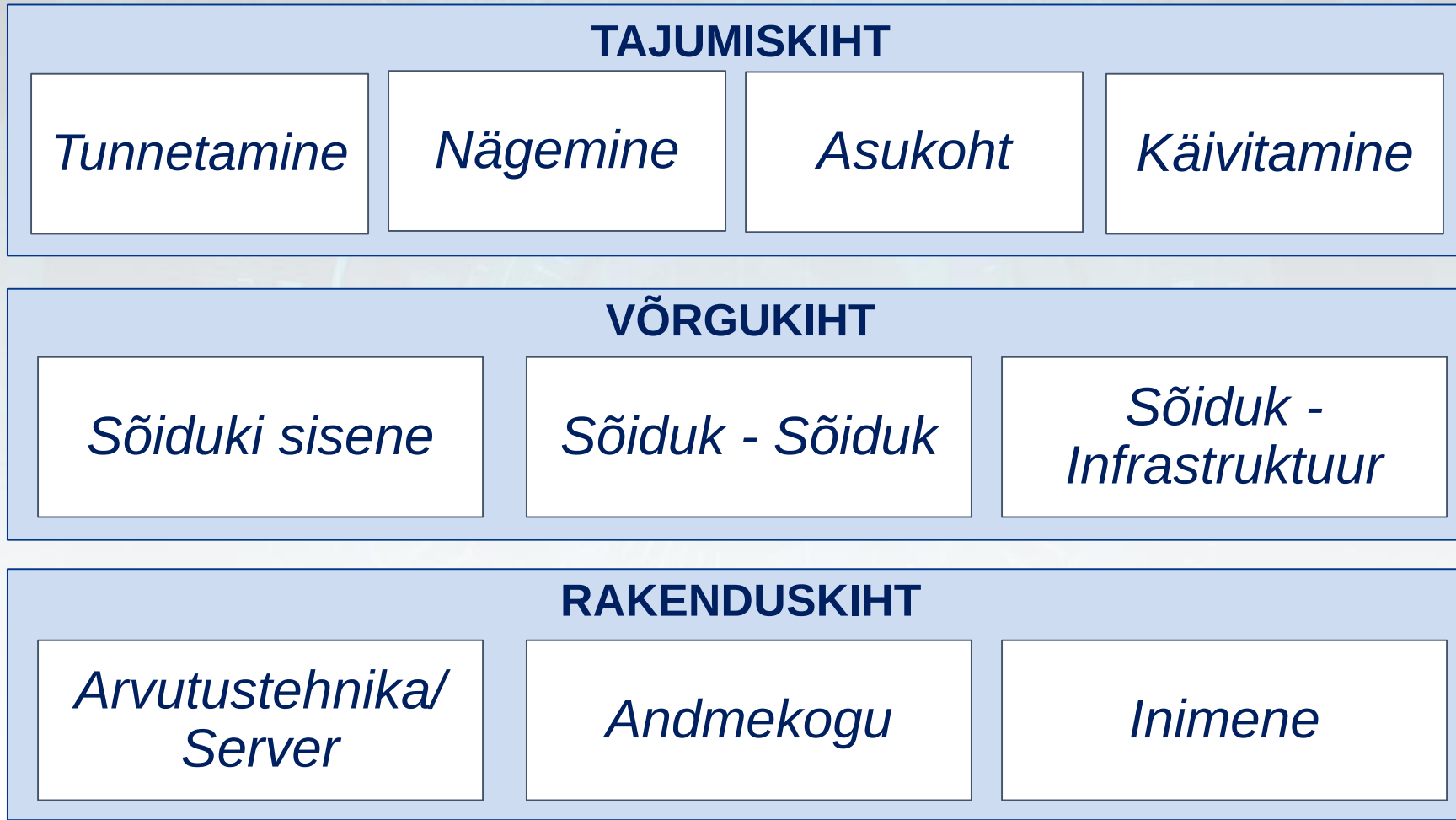
Teadmiste puudumisest tulenevad riskid

Tahvelarvutid

Arvutid

Küberturvalisuse väljakutsed

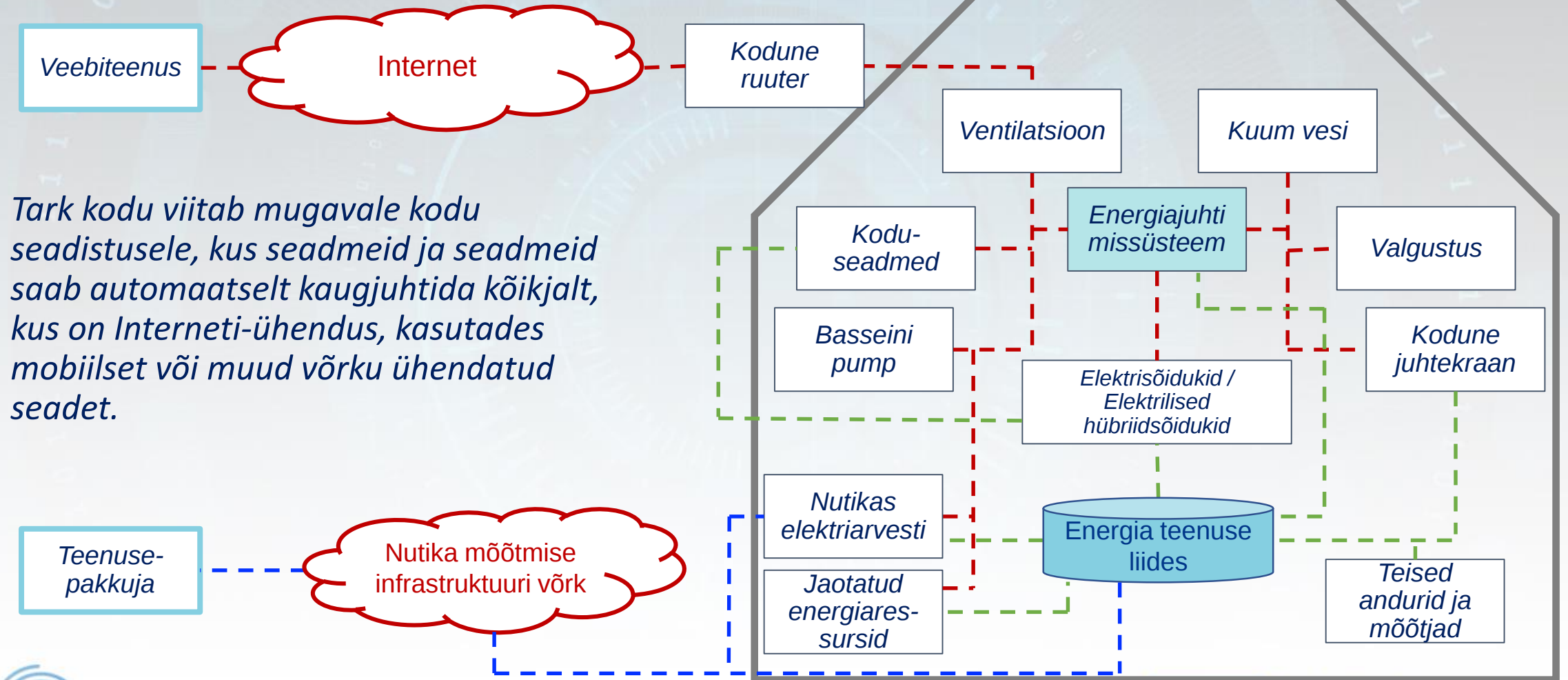
Intelligentsed süsteemid



	TURVAOHUD					
Süsteemi varad	<i>Pettus</i>	<i>Muutmine</i>	<i>Äraütlemine</i>	<i>Informatsioon paljastus</i>	<i>Teenuse tõkestus</i>	<i>Õiguste suurendamine</i>
Andur, positsioneerimine, nägemise tehnoloogiad	Spoofing, Node impersonation, Illusion, Replay, Sending deceptive messages, Masquerading	Forgery, Data manipulation, Tampering, Falsification of readings, Message injection	Bogus message	Stored attacks, Eavesdropping	Message saturation, Jamming, Denial of service (DoS), Disruption of system	Backdoor, Unauthorized access, Elevation of privilege, Remote update of ECU
Sõiduki sisene võrk, sõidukitevaheline (V2V), sõiduki ja infrastruktuuri vaheline võrk (V2I)	Sybil, Spoofing, Replay attack, Masquerading, Fingerprinting, Wormhole, Camouflage attack, Impersonation attack	Timing attacks, Injection, Manipulation, Routing manipulation, Tampering, Forgery, Malicious update	Bogus messages, Rogue Repudiation, Loss of event traceability	Eavesdropping, MiTM, ID disclosure, Location tracking, Message interception, Information disclosure	DoS/DDoS, Spam, Jamming, Flooding, Message suppression, Channel interference, Black hole	Malware, Brute Force, Gaining control, Social engineering, Logical attacks, Unauthorized access, Session Hijack
Rakendusserver, äärealalüütika andmekeskus, inimene	Spoofing, Sybil, Illusion attack	Malicious update	--	Eavesdropping, Location tracking, Privacy leakage	Deny of Service	Jail-breaking OS, Social engineering, Rogue data-center, malware

Küberturvalisuse väljakutsed

Targa kodu süsteemid



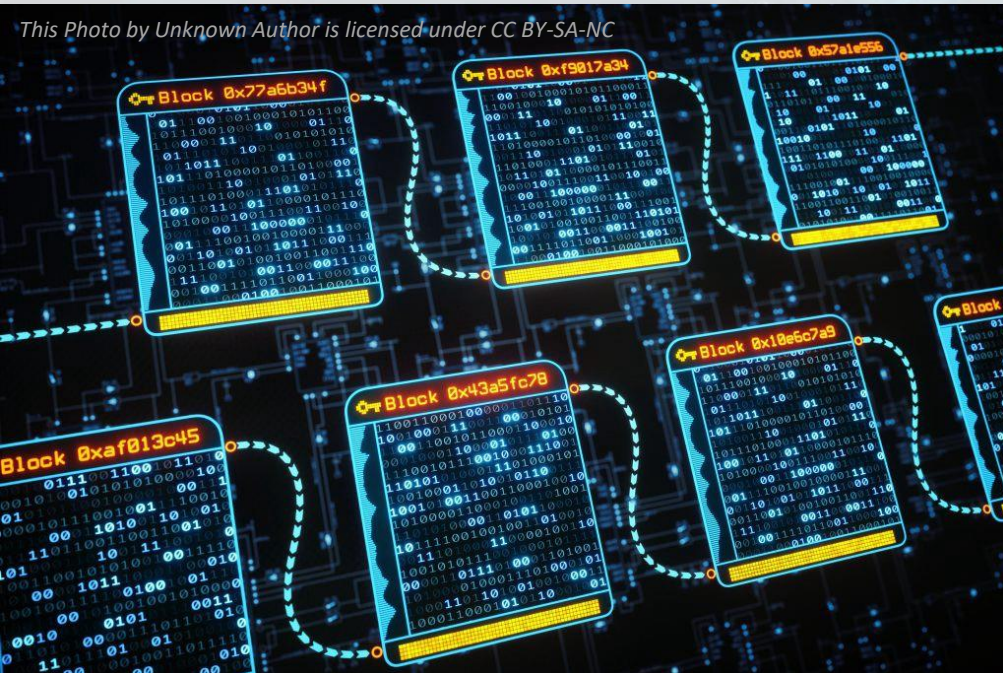
Küberturvalisuse väljakutsed

Targa kodu süsteemid

Stsenaarium	Võimalik oht (N – networking domain, SH – smart home concept)	Turva kriteerium mida rikutakse
AS1: Attacks Threatening Successful Device Energy– Consumption Reporting	Eavesdropping (N), Traffic analysis (N), Message modification (N), Reply attack (N), Energy management system impersonation (SH)	Confidentiality, Integrity, Authentication
AS2: Attacks Aiming Energy Import/ Export Signals at the Energy service interface or Home area network	Repudiation (N), Message modification (N), Replay attack (N)	Non-repudiation, Integrity, Authentication
AS3: Physical Meter Tampering/ Reversal or Removal	Tampering/ Reversal, Removal of meter (SH), Illegal software modification / update (SH)	Authentication, Integrity
AS4: Attacks Against Remote Home Monitoring and Control	Customer impersonation (N), Device impersonation (SH), Message modification (N), Replay attack (N), Repudiation (N)	Integrity, non-repudiation, Authentication
AS5: Attacks Aiming the Requests for Energy Usage Data	Customer impersonation (N), Eavesdropping (N), Interception (N), Message modification (N)	Confidentiality, Integrity, Availability

Küberturvalisuse väljakutsed

Plokiahela tehnoloogia



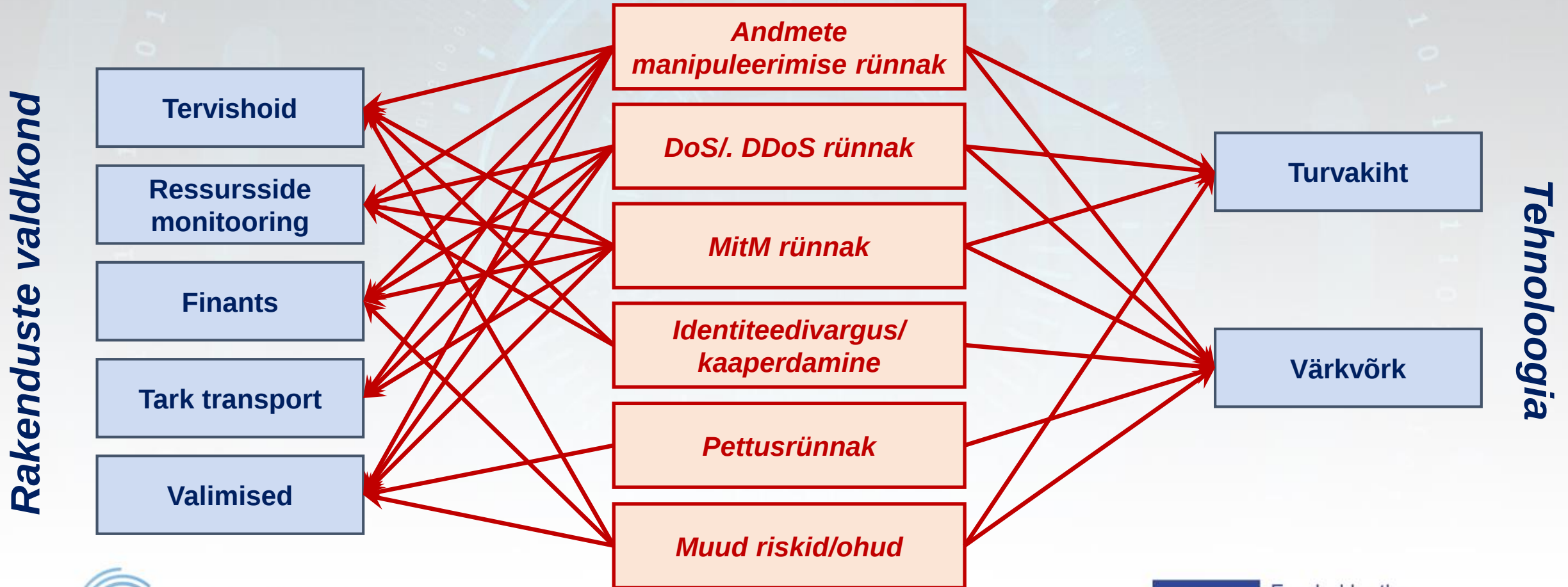
POKIAHEL - Järjestikustest andmeplokkidest moodustatud andmestruktuur, mis võimaldab tehingute digitaalset identifitseerimist ja jälitamist üle hajussüsteemi. Plokiahel pakub hajusraamatu (hajuspäeviku) tehnoloogiat, mis võimaldab läbipaistvat ja turvalist vahendit varade kuuluvuse ja ülekandmise jälitust.

www.vallaste.ee

Küberturvalisuse väljakutsed

Plokiahela tehnoloogia

Turvariskid erinevates rakendusvaldkondades on leevendatud plokiahela rakenduste abil

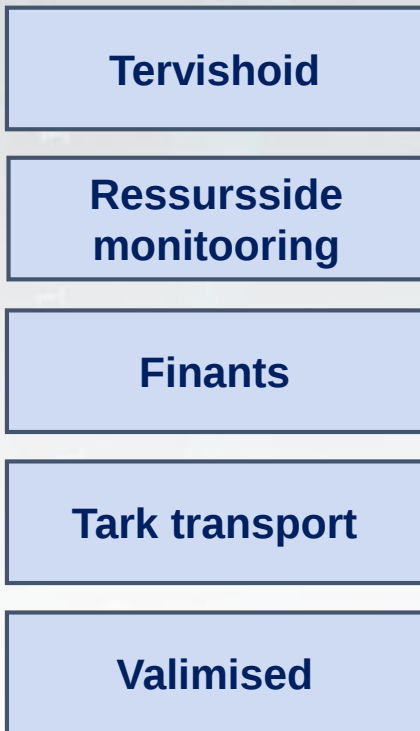


Küberturvalisuse väljakutsed

Plokiahela tehnoloogia

Turvariskid plokiahela rakendustele

Rakenduste valdkond



Tehnoloogia

Küberturvalisuse väljakutsed

Suurandmete ekosüsteem

INIMENE

Äri, teave, sotsiaalne, professionaalne

VÄLJAKUTSED

Nõusoleku puudumine, teadmiste sotsiaalne väärkasutus, volitamata juurdepääs, andmete üleujutus, sobimatu analüüs, kättesaadavus, täpsus

TEHNOLOOGIA

Rakendus, platvorm, andmeinfrastruktuur

Andmete mitmekordne kasutamine, tehnoloogilised lüngad, kokkulepitud andmekasutus, andmed, õigeaegsus, andmete päritolu, seadme heterogeensus, kättesaadavus, andmete kogumise haldamine ja edastamine, andmetüübid ja -vormingud, mittetäielikud ja ebajärjekindlad andmed

RAJATISED

Ruumiline, HVAC, energeetika, abisüsteemid

Salvestus ja töötlemine, erinevad andmeallikad, saadavus

KESKKOND

Poliitiline, keskkonnaalane, sotsiaalne, tehnoloogiline, juriidiline

Juhtimise puudumine, poliitikad, seadused, organisatsiooniline vastupanu, andmepõhise kultuuri loomine

Küberturvalisuse väljakutsed

Suurandmete ekosüsteem

INIMENE

Äri, teave, sotsiaalne, professionaalne

LAHENDUSED

Kasutajate valideerimine, oskused, juurdepääsukontroll, kasutajakoolitus, auditid, sideturve, ohtude modelleerimine, riskihindamine, andmete klassifikatsioon, andmepõhine privaatsuse säilitamine, privaatsus sotsiaalsõrgustikes

TEHNOLOOGIA

Rakendus, platvorm, andmeinfrastruktuur

Lõpp-punkti valideerimine ja krüpteerimine, turvalised päringud, diferentsiaalne privaatsus, varjatud andmete privaatsus, turvaline andmete kogumine, talletamine ja teisendamine, masinõppe algoritmid, sissetungi tuvastamine, andmete anonüümseks muutmine

RAJATISED

Ruumiline, HVAC, energeetika, abisüsteemid

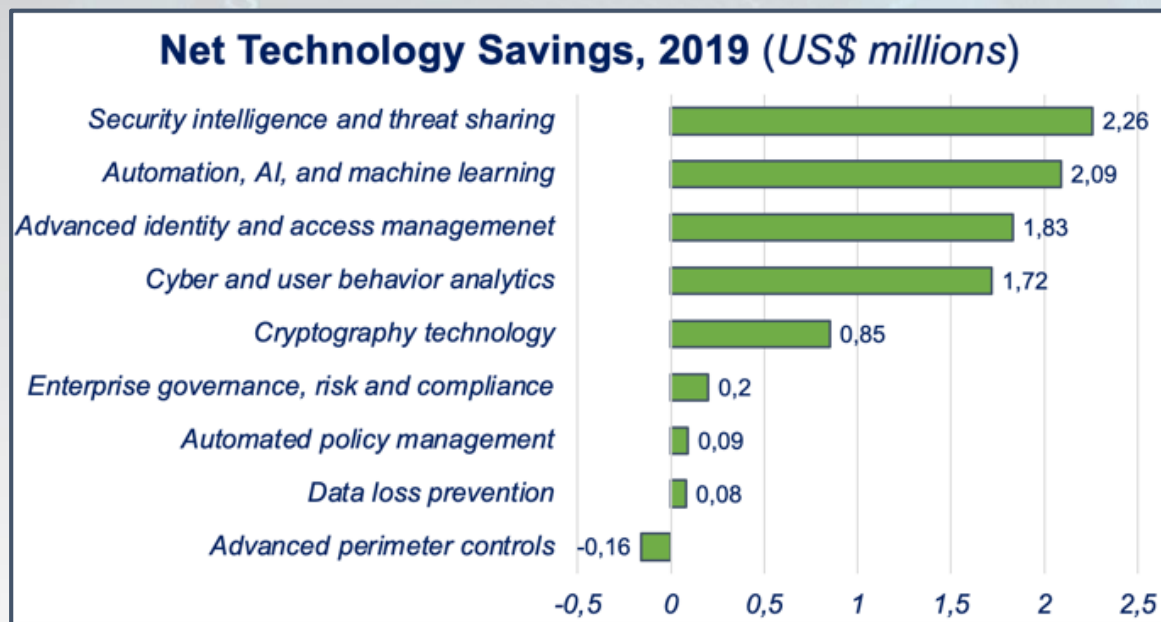
Andmete hajutatud allikad Krüpteeritud päise teabe varundamine ja taastamine

KESKKOND

Poliitiline, keskkonnaalne, sotsiaalne, tehnoloogiline, juriidiline

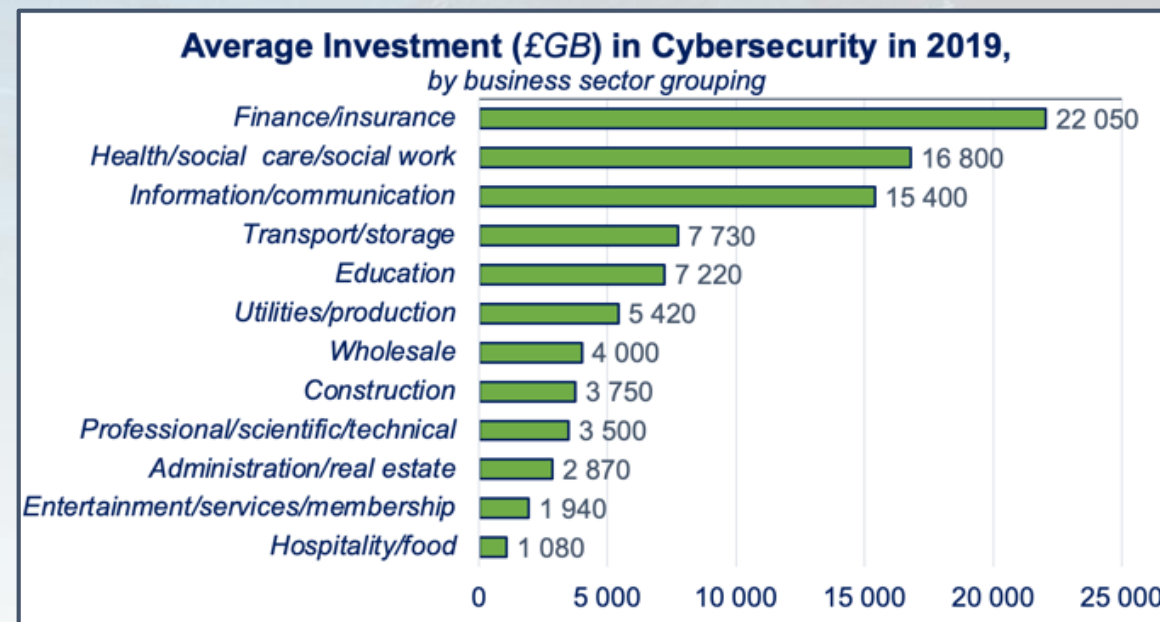
Juhtimine ja juriidiline tugi

Investeeringud turvalisusesse



Turvaluure ja ohtude jagamine on enimkasutatavad turvatehnoloogiad

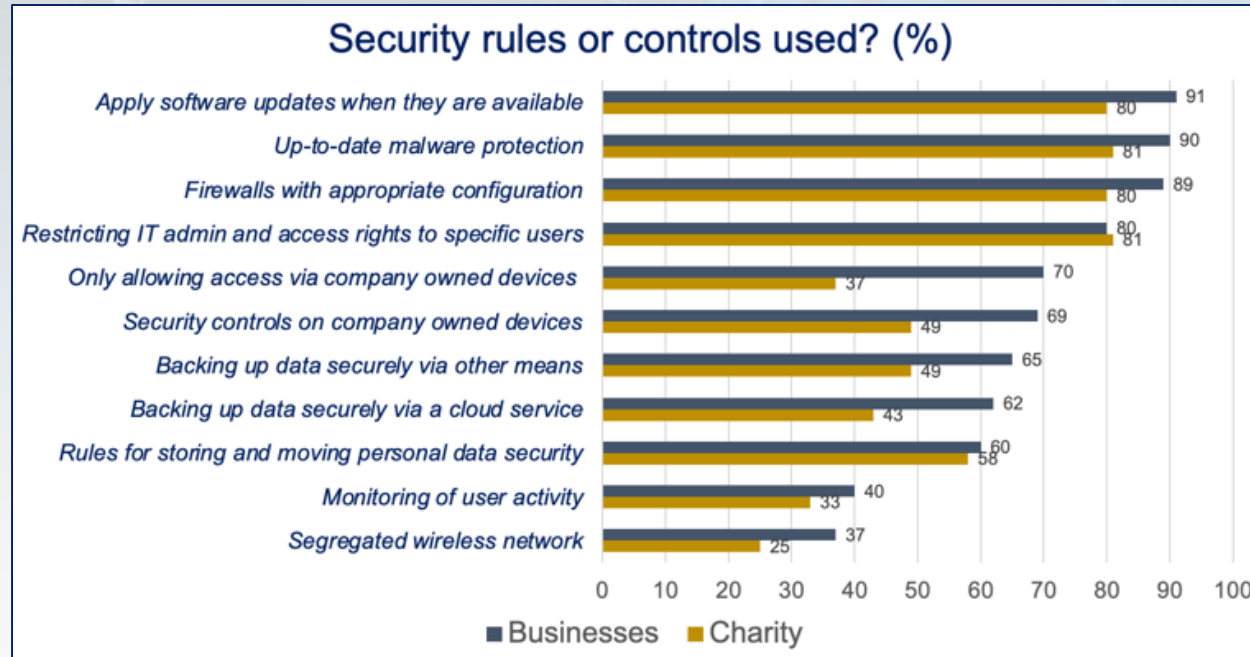
<https://www.digitalmarketingcommunity.com/indicators/security-technologies-cost-saving-2019/>



Finants- ja kindlustussektorid on kõrgeimad küberturvalisusesse investeerinud ärisektorid

<https://www.digitalmarketingcommunity.com/indicators/cyber-security-investment-2019/>

Kasvavate ohtude väljakutse



<https://www.digitalmarketingcommunity.com/indicators/preventing-minimizing-cyber-security-2019/>

- Äрге eitage ohtu, kuna see toob kaasa tõrkeid
- Eeldage, et juhuslikud teaberikkumised on tõenäolisemad kui pahatahtlikud rünnakud
- Äрге oodake tegutsega, kuni teid rünnatakse või teid lekitatakse
- Rakendage eeskirju järjekindlalt
- Käsitleda kultuuriprobleeme erinevatel tasanditel
- Tasakaalustage investeeringud välimiste ja sisemiste ohtude vahel
- Aktsepteerige maksiimi "haridus, haridus, haridus"!

[Colwill, 2009]

Riiklikul tasandil ohud

- Küberspionaaži sihtmärgid:
 - *tööstussektor*
 - *kriitilised ja strateegilised infrastruktuurid*
 - *valitsusasutused*
 - *raudteed*
 - *telekommunikatsiooni pakkujad*
 - *energiaettevõtted*
 - *haiglad*
 - *pangad*

Küberspionaažist
ajendatud
andmerikkumised
20%

Pahatahtlikud
tegutsejad, kes
on seotud
riikidega
38%

Küberspionaažist
ajendatud
juhtumid
11,2%

Andmepüügiga
seotud
küberspionaaži
juhtumid
63%

Riiklikul tasandil ohud

- Küberspionaaž keskendub:
 - Geopoliitika juhtimisele
 - riigi- ja ärisaladuste varastamine
 - intellektuaalse vara õigused
 - varaline teave strateegilistes valdkondades.
- 2019 aastal, *kasvas riiklikul tasandil toetatud majandusele suunatud küberrünnakute arv ja see tendents jätkub*
- Rahvusriikide toetatud rünnakud tööstusliku asjade Interneti (IIoT) vastu sagenevad
 - *kommunaalteenused*
 - *kütuse ja gaasi jaamad*
 - *Tööstus ja tehased*



This Photo by Unknown Author is licensed under CC BY-NC

Safeguarding your digital future



Riiklikul tasandil ohud

- Küberspionaaž keskendub:

- Geopoliitika juhtimisele

- riigi- ja äri

- intellektua

- varaline t

- valdkond

- 2019 aastal,

kasvas riiklikul tasandil toetatud

Tehke kindlaks missioonikriitilised rollid organisatsioonis ja hinnake nende kokkupuudet spionaažiriskidega

Looge turvapoliitika

Looge ettevõtte tavad suhtlemiseks ja töötajate koolitamiseks

Töötage toimingute võrdlemiseks välja hindamiskriteeriumid (KPI-d).

Looge kriitiliste rakendusteenuste jaoks valge nimekiri

Hinnake turvaauke ja parandage tarkvara regulaarselt

Juurdepääsuõiguste määratlemisel rakendada teadmismajaduse põhimõtet

Sisu filtreerimine kõigi sissetulevate ja väljaminevate kanalite jaoks

- Tööstus ja tehased

Kokkuvõte

- Ärивäljakutsed kübervaldkonnas
- Küberturvalisuse rünnakute kasv
- Tehnoloogia kasutamine ja turvaprobleemid
- Kasvavate ohtude väljakutse
- Riiklikul tasemel ohud



Ülesanded

Arutage, mis on äritegevuse suuruselt teine väljakutse (loomulikult pärast infoturvet)

Mis on teie arvates kõige ohtlikum julgeolekuoht/rünnak?

Kas kasutate oma igapäevaelus mõnda (mobiil)tehnoloogiat? Milline? Kas see on turvatud?

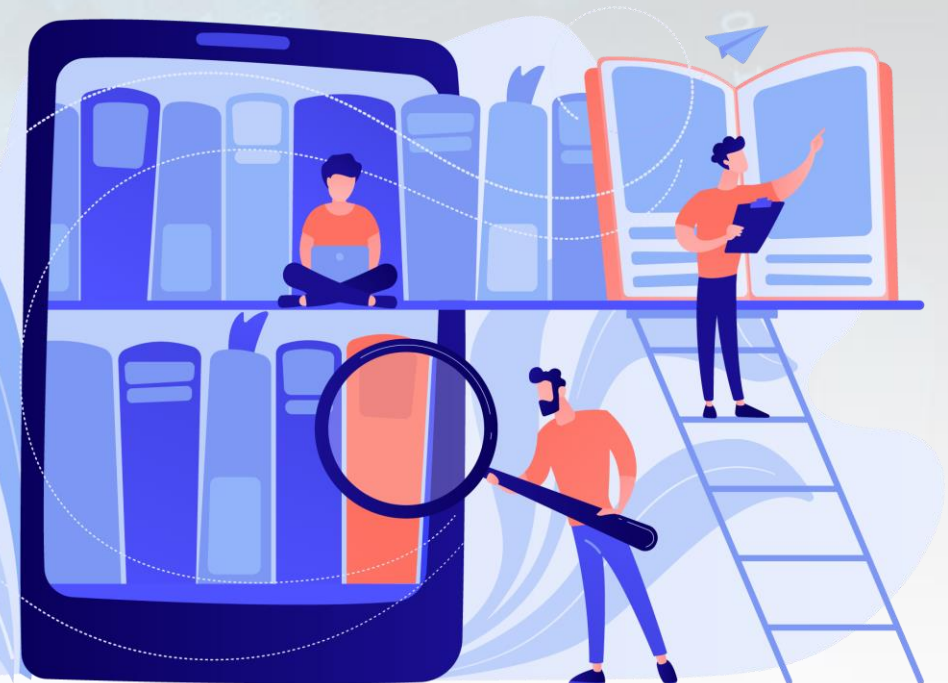
Kas teate või olete lugenud mõnest riigi tasemel ohust? Kas saaksite sellest rääkida ja selgitada, milles asi?



Lisalugemist

Material used in preparation of this lecture

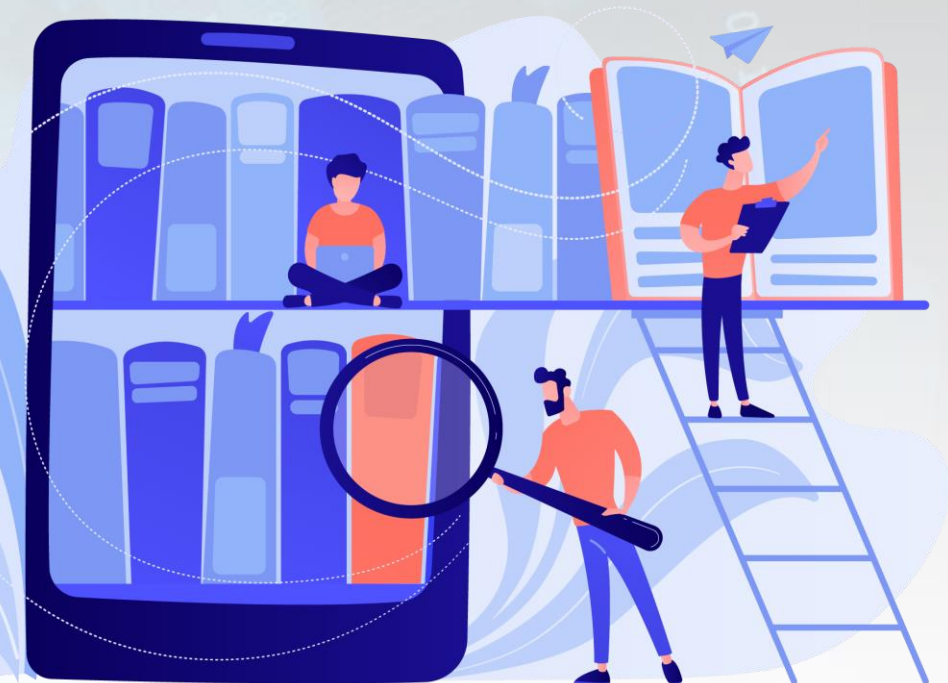
- **Abiodun O. I. A., Abiodun E. O., Alawida M., Alkhawaldeh R. S., Arshad H.,** (2021). A Review on the Security of the Internet of Things: Challenges and Solutions. *Wireless Personal Communications* 119:2603–2637 <https://doi.org/10.1007/s11277-021-08348-9>
- **Affia A-a. O., Matulevičius R., Nolte A.** (2019): Security Risk Management in Cooperative Intelligent Transportation Systems: A Systematic Literature Review. *Panetto H. et al. (eds.), LNCS 11877, CoopIS 2019, Springer*
- **Anwar M. J. Gill A. Q., Hussain F. K., Imran M.** (2021), Secure big data ecosystem architecture: challenges and solutions. *J Wireless Com Network* 2021:130 <https://doi.org/10.1186/s13638-021-01996-2>
- **Colwill C.** (2009) Human factors in information security: The insider threat e Who can you trust these days? *Information Security Technical Report* 14,186-196
- **Iqbal, M., Matulevičius, R.** (2019) Blockchain-Based Application Security Risks: A Systematic Literature Review, *Proceedings of CAiSE 2019 International Workshops, 2019 Workshop, LNBIP 349, 176-188*
- **Komninos N., Philippou E., Pitsillides A.** (2014). Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures, *IEEE Communication Surveys & Tutorials*, 16(4)



Lisalugemist

Material used in preparation of this lecture

- **Lewis, A.** (2015): Blockchain technology explained (2015). <http://www.blockchaintechnologies.com/blockchain-definition>
- **Orantes-Jimenez A.D., Aquirre E.** (2020): A Survey on Information Security in Cloud Computing, *Computacion y Sistemas* 24(2)
- **Perdomo R.** (2021): 15 Technology Challenges Business May Face in 2021, URL: <https://blog.systems-x.com/author/rubens-perdomo>
- **Sato, T., Himura, Y.** (2018): Smart-contract based system operations for permissioned blockchain. *NTMS 2018*, vol., 1–6
- **Schatz, D., Bashroush, R., Wall, J.** (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*. 12 (2).
- **Tahirkheli, A.I.; Shiraz, M.; Hayat, B.; Idrees, M.; Sajid, A.; Ullah, R.; Ayub, N.; Kim, K.-I. A.** (2021). Survey on Modern Cloud Computing Security over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges. *Electronics* 2021,10,1811. <https://doi.org/10.3390/electronics10151811>



Lühivideod

- Business Technology Trends
<https://youtu.be/DOAnYtqhXBU>
- The Internet of Things Security
<https://youtu.be/IQkRscixagM>
- Cloud Cybersecurity
<https://youtu.be/k2684fuzHLs>
- Hacking your Home
<https://youtu.be/iRQPfISsG9k>
- Introduction to Blockchain Security
<https://youtu.be/dl8HI91siM8>
- Challenges of Securing Big Data
<https://youtu.be/3xlulcPzMVs>
- What are the Current Data Security Threats?
<https://youtu.be/WugGZaT2oHE>
- Top 7 Most Elite Nation State Hackers
https://youtu.be/S_IPgHbondk



Tänan kuulamast!

