Küberkaitse ja infoturve

Euroopa Liit
Euroopa Sotsiaalfond

Eesti
tuleviku heaks

Laura Kask

PROUD ENGINEERS CEO

TARTU ÜLIKOOLI DOKTORANT, KÜLALISLEKTOR

6.06.2019

TARTU ÜLIKOOL

10 eestlaste populaarseimat parooli:

1. 123456
2. parool
3. qwerty
4. 123456789
5. lammas
6. 12345
7. minaise
8. maasikas
9. kallis
10. Killer

Allikas: https://digi.geenius.ee/rubriik/uudis/suured-lekked-just-need-eestlaste-koige-populaarsemad-paroolid/

TARTU ÜLIKOOL

Mis on küberturvalisus?

Küberturvalisus

- Tegemist on määratlemata õigusmõistega, kuigi kasutuses üsna laialt;
- Inimeste, tarkvara ja teenuste interaktsiooniga tekitatav virtuaalne keskkond (sageli interneti kui sünonüümi) turvalisus (andmekaitse ja infoturbe leksikon);
- ühiskonna seisund, mida iseloomustab võrgu- ja infosüsteemi kaudu avalikku korda, isikute tervist, vara ja keskkonda mõjutavate ohtude realiseerumise madal tõenäosus, võimekus ohtudele reageerida ja leevendada ohtude realiseerumisel tekitatud kahjulikku mõju ning mis tagatakse füüsiliste, organisatsiooniliste ja infotehniliste abinõude rakendamisega (KüTS seletuskiri);
- Võrgu- ja infosüsteemide turve, mis on ühendatudorganisatsioonilise struktuuri ja teadliku käitumisega

Küberturvalisuse strateegia 2019–2022

Uues (kolmandas) küberturvalisuse strateegias on seatud neli olulist eesmärki:

- Eesti on jätkusuutlik digitaalne ühiskond, millel on tugev tehnoloogiline vastupanuvõime ja valmisolek kriisidega toimetulekuks.
- Eestis on tugev, innovaatiline, teaduspõhine ja globaalselt konkurentsivõimeline küberturbe sektori ettevõtlus ning teadus- ja arendustegevus, mis katab riigi jaoks olulised võtmekompetentsid.
- Eesti on arvestatav ja tugev partner rahvusvahelisel areenil.
- Eesti on ühiskonnana küberteadlik ning tagatud on valdkonna spetsialistide järelkasv.

Loe lähemalt: Küberturvalisuse strateegia: https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf

Küberturvalisuse seadus ja NIS direktiiv

- Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/1148, 6. juuli 2016, meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus
- EESMÄRK: kehtestada ühiskonna ja majanduse jaoks määrava tähtsusega teenustele miinimumstandardid võrgu- ja infosüsteemide kaitseks ning saavutada siseturul ühtlaselt kõrge tase

- Küberturvalisuse seadus (vastu võetud 09.05.2018)
- EESMÄRK: tugevdada ühiskonna jaoks määrava tähtsusega teenuste ning riigi ja kohaliku omavalitsuse üksuste töö toimimiseks kasutatavate võrgu- ja infosüsteemide kaitset

Küberturvalisuse seadus ja NIS direktiiv

- Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/1148, 6. juuli 2016, meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus
- EESMÄRK: kehtestada ühiskonna ja majanduse jaoks määrava tähtsusega teenustele miinimumstandardid võrgu- ja infosüsteemide kaitseks ning saavutada siseturul ühtlaselt kõrge tase, majanduslik areng, piiriülese koostöö parandamine.

- Küberturvalisuse seadus (vastu võetud 09.05.2018)
- EESMÄRK: tugevdada ühiskonna jaoks määrava tähtsusega teenuste ning riigi ja kohaliku omavalitsuse üksuste töö toimimiseks kasutatavate võrgu- ja infosüsteemide kaitset

Küberturvalisuse seaduse subjektid:

- Küberturvalisuse tagamiseks peavad meetmeid kasutama:
  - ühiskonna toimimise seisukohast oluliste teenuste (sealhulgas elutähtsa teenuse osutajad, olulised infrastruktuuri ettevõtted);
  - digitaalse teenuse osutajad (pakuvad internetipõhise kauplemiskoha teenust, otsimootori teenust või pilveandmetöötlusteenust);
  - riigiasutused ja kohaliku omavalitsuse üksused, kes võrreldes NIS direktiivi kohaldamisala subjektide ringiga on KüTS lisandunud, kuigi nõudeid neile on rakendatud juba ka varem.

Kes on ETO, OTO, DTO…

- ETOd ehk elutähtsa teenuse osutajad on reguleeritud HOSis;
- OTOd ehk olulise teenuse osutajad on näiteks suuremad transporditaristu ettevõtted (raudtee- ettevõtja, lennuvälja käitaja, sadamateenuse osutaja), sideteenuse pakkujad (üle 10 000 kliendiga sideettevõtja, kriitilise tähtsusega mere- ja raadiosidevõrgu teenuse osutaja), tervishoiu teenuse pakkuja (statsionaarne eriarstiabi osutaja, kiirabibrigaadi pidaja, perearstid), Eesti Interneti Sihtasutus, Eesti Rahvusringhääling;
- DTO ehk digitaalse teenuse osutajad on näiteks internetipõhise kauplemiskoha pakkujad (e-poed), pilveandmetöötlusteenuse ja otsingumootori teenuse pakkujad.

Mis on nõuded?

Kohustus rakendada turvameetmeid küberintsidendi ennetamiseks ja lahendamiseks, intsidendi mõju leevendamiseks:

- viia läbi infosüsteemide riskianalüüsid ja koostada turvaeeskirjad,
- planeerida ja kirjeldada rakendatavad turvameetmed intsidentide puhuks;
- seirata ennetavalt süsteeme intsidentide vältimiseks ja edastada ohtude kohta teavat RIA-le;
- kontrollima turvameetmete toimimist;
- küberintsidendi korral vajadusel piirama süsteemi kasutamist või juurdepääsu sellele;
- 24h jooksul teavitama RIAt olulise mõjuga küberintsidendist + selle lahendamisel saatma RIAle raporti toimunu, tehtu ja mõju kohta.

Millised on rollid küberturvalisuse tagamisel?

- Riigi Infosüsteemi Amet + CERT
- Majandus- ja Kommunikatsiooniministeerium
- Kaitseministeerium ja Kaitsevägi
- Välisministeerium
- Haridusministeerium
- Rahandusministeerium
- Siseministeerium
- Tartu Ülikool, Tallinna Tehnikaülikool …
- ETOd, OTOd
- KOV
- Küberturvalisuse- ja teadlikkusega tegelevad ettevõtted
- SINA!

Millega tegeleb Riigi Infosüsteemi Amet?

- juhib riikliku koordinatsiooni ülesande küberturbe alal
- teostab küberintsidentide ennetamiseks üldist seiret ja analüüsib süsteemide turvalisust ohustavaid riske ja nende mõju;
- edastab küberintsidentide ennetamiseks ja lahendamiseks ohuteateid;
- edastabvajadusel informatsiooni EL vastavatele pädevatele asutustele;
- peab küberintsidentide registrit (plaanis);
- teostab järelevalvet seaduses sätestatud nõuete täitmise üle ning annab korraldusi turvameetmete rakendamiseks (sh vajadusel määrab trahve);
- küberintsidendi korral kõrgendatud ohu korral selle tõrjumiseks piirab süsteemi kasutamist või juurdepääsu sellele – ainult juhul kui intsident võib ohustada ka teisi süsteeme, süsteemi haldaja ei saa ise ohtu tõrjutud, see tegevus on proportsionaalne (sh ei tekitata liigset kahju).

TARTU ÜLIKOOL

KüTS vs IKS?

NIS vs GDPR?

TARTU ÜLIKOOL

Turvaline elektrooniline ja digilahendustele orienteeritud virtuaalne keskkond ei ole saavutatav mitte üksnes võrgu- ja infosüsteemide turbe, vaid ka organisatsioonilise ning teadliku käitumise kaudu.

Küberruumi turvalisuse tagamiseks on oluline nii riigi, ettevõtete kui ka akadeemia koostöö.

Loe lähemalt: L.Kask. Küberturvalisuse seadusest. Õiguskeel. Kättesaadav: https://www.just.ee/sites/www.just.ee/files/laura_kask._kuberturvalisuse_seadusest.pdf

TARTU ÜLIKOOL

unitartu

tartuylikool