TEADLASE PILGUGA

Riskianalüüs küberturbes käib samamoodi nagu maanteedel või rahanduses

Dan Bogdanov

Oluline on mõista, et kui inimesed kord juba midagi ette võtavad, ei ole sellega seotud ohtude sagedust päris nulli viia võimalik. Risk on seotud tuleviku ebakindlusega. Me ei saa juhtuvat kunagi täielikult ette näha ja peame arvestama võimalusega, et asjad ei lähe plaanipäraselt. Investeeringud võivad hukka minna, maanteel võib loom teele joosta või kontrollimata allikast ostetud sidevahendid võivad sobimatul hetkel käes plahvatada. Mõni halb sündmus on sage (juhtub maailmas iga päev), mõni juhtub harva (kord kümnete aastate jooksul), mõni on nii haruldane, et polegi veel inimkonna ajaloo jooksul kunagi juhtunud.

Evolutsiooni käigus on meie ajus arenenud automaatne ohtude hindamise võime. Eks jäid korilastest ja jahimeestest savannis ellu need varased inimesed, kes oskasid aimata, et mõnes põõsas varitseb neid lõvi. Tänaseks on meie riskide nägemise võime kõrgelt arenenud ning oskame muretseda rohkemgi, kui vaja oleks. Selle nõrkuse tasakaalustamiseks on loodud riskianalüüsi distsipliin.

Kuidas käib riskianalüüs?

Riskianalüüsi käigus mõeldakse läbi kolm asja. Esiteks, kontekst ehk mis on see, mida tahame ohu eest kaitsta. Teiseks, riskide hindamine ehk mis võib halvasti minna ja kui sagedasti seda võib juhtuda. Kolmandaks, riskide käsitlus ehk mida me siis ette võtame.

Rahaliste investeeringute tegemisel on risk hästi mõistetav. On tõenäosus, et saan raha tagasi ja rohkemgi veel, aga võib ka juhtuda, et äri või pank lähevad pankrotti ja ma kaotan kõik. Selliste olukordade tarbeks on riigid kehtestanud seadused, mis kaitsevad investoreid ja sunnivad investeeringute vahendajaid neid põhjalikult teavitama sellest, mis juhtuda võib. Lihtsamate investeeringute jaoks on ka loodud tagatisfondid, mis mõnel juhul aitavad investoril oma raha tagasi saada.

Siin nägime kahte head näidet riski kahandamiseks loodud meetmetest. Risk on, et kodanik kaotab suures mahus oma vara (ning võib jääda riigile koormaks, tekitades ülalpidamiskulusid). Teavitustegevus on ennetav meede, mis aitab inimesel vältida tema riskiisule vastavat käitumist. Tagatisfond on omamoodi kindlustus, mis riski realiseerumisel hüvitab tehtud kahjud varasuhtes nõrgemale osapoolele (sääste kogunud erainvestor). Ka nende meetmete rakendamisel jääb alles teatav risk, aga me mõistame seda ja elame edasi.

Maanteel autoga sõites peame kõik alluma liiklusseadusele, mis on meede sõidukite vaheliste riskide vähendamiseks. Transpordiamet rajab teedele ka turvameetmeid, mis on ette nähtud kaitsma meid nii oma sõiduoskust ülehindavate kaasliiklejate kui ka seaduse eirajate eest.

Maanteed on suurepärane näide sellest, kuidas alati võiks investeerida rohkem, et vähendada õnnetusi teatud lõigul. Aga me saame aru, et igale autole eratunnelit ehitada ei ole majanduslikult mõistlik ja teatud risk jääb alles. Oluline on, et Transpordiamet korraldab riski seire ja suunab enda

TEADLASE PILGUGA

investeeringud eelisjärjekorras neile ristmikele, kus on rohkem õnnetusi või liiklejaid. See on suurepärane näide sellest, kuidas hästi korraldatud riskianalüüs suunab investeeringuid ohutuse tagamiseks.

Kui liiklus ja raha on inimkonnaga olnud aastasadu ja isegi -tuhandeid, siis infotehnoloogia kiire areng on tekitanud riske, mille mõistmise ja analüüsiga jääb tavainimene hätta. Arvutite ja nutiseadmete käitumine on tavakasutajatele tihtipeale ennustamatu, seega on siin hirmud kerged tekkima. Põhjus on infotehnoloogia kõrges keerukuses, mis takistab erialase ettevalmistuseta inimest selle käitumist mõistmast.

Küberturbe riskianalüüs järgib sama mudelit

Infoturbe ja küberturbe riskianalüüs käib täpselt samamoodi nagu maanteedel või rahanduses. Hindame IT-süsteemide ja teenuste ohte ja võimalikke ohustajaid. Otsustame, milliste ohtude vastu me peame või jõuame kaitsta ja siis loome meetmed. Mida olulisem süsteem on, seda põhjalikumad ja keerukamad on ka meetmed.

Eesti e-riigi teenused teevad paljude inimeste elu kiiremaks ja lihtsamaks, aga nende keerukus on kõrge ja ohud arenevad samuti. Selleks, et e-riik oleks kestlikult turvaline, peame leidma kestliku viisi selle riskide analüüsiks ja kulutõhusate kaitsemeetmete leidmiseks. Just selle töö on ette võtnud teaduste akadeemia küberturvalisuse komisjon.

Esimese kahe aasta uurimisobjektiks on olnud Eesti demokraatlike valimiste tehnoloogia, mis kasutab uuenduslikke e-valimisi, kuid ka pabersedelite loendamisel kasutatakse infosüsteeme järjest rohkem.

1. oktoobril avaldas komisjon esmakordselt e-riigi koodivaramus Eesti valimiste tehnoloogia riskianalüüsi. 28. oktoobril on teemast huvitatud oodatud komisjoni ja Riigi Infosüsteemi Ameti korraldatud konverentsile „Usaldusest ja usaldatavusest 2024: valimiste tehnoloogia“.

Ilmunud ajalehes Postimees 12. oktoobril 2024