Kolmeteistkümnes peatükk

INFOTURVE JA KÜBERTURVALISUS

Janek Metsallik, Mall Maasik, Maarja-Liis Elland

Sisukord

Sissejuhatus

Tervishoiuteenuseid osutades on turvalisus ja hügieen olulised mitte ainult meditsiiniliste protseduuride puhul, vaid ka terviseandmete ja -infoga töötades.

Seoses e-tervise rakendamisega ja valdkonna kiire laienemisega on kiiresti kasvanud ka infoturbe ja andmekaitse tähtsus. Patsientide, aga ka tervishoiutöötajate isikuandmete kaitsmiseks ning terviseandmetele usaldusväärse ja turvalise juurdepääsu tagamiseks on kasutusele võetud ja vaja võtta üha uusi meetmeid ja regulatsioone.

Meetmed, mida seoses e-tervisega rakendatakse ja millest tuleb peatükis juttu, on näiteks:

1. **andmete krüpteerimine**, et takistada volitamata juurdepääsu terviseandmetele;
2. **terviseandmetele ligipääsu kontroll**, mis tagab, et terviseandmetele saavad ligi ainult rollipõhiselt volitatud isikud;
3. **pidev tervishoiutöötajate ja patsientide koolitamine** infoturbe ja andmekaitse teemadel, et tunda ära ohtusid ja toimetada küberruumis vastutustundlikult.

Infoturve ja andmekaitse on olnud olemas sajandeid. Seoses digitaliseerimise ja e-tervise rakendamisega on tuleviku väljakutsed eelkõige seotud küberturbe ohtude kasvuga, mida käesolev peatükk ka käsitleb.

Kui ettevõtetele on viimasel ajal peavalu valmistanud ummistusründed, lunavaranõuded ja andmelekked, siis tavakasutajaid kimbutavad erinevad pettused. Riigi Infosüsteemi Ameti (RIA) 2024 aastaraamatus on kirjas, et õngitsuslehele läheb ligi kolmandik kirja saajatest ja 10–20 protsenti neist sisestab sinna ka küsitud andmed, näiteks oma konto salasõna. Peale õngitsuskirjade on avaliku sektori töötajate puhul nõrkuseks salasõnade ristkasutus ehk sama salasõna kasutatakse mitmes keskkonnas (Riigi Infosüsteemi Amet, 2024l). RIA soovitus on, et küberturvalisuse koolituse läbiksid kõik töötajad vähemalt kord aastas.

Kasutatavad terminid

ISO 22300 ütleb, et **informatsioon** ehk teave on tähendusega andmed, mis on tähenduse saamiseks töödeldud, korraldatud ja korrigeeritud. Teave ei võrdu andmed, sest teave on sisu, andmed on vorm.

Turvalisus on kindlustunne, mis loob aluse jätkusuutlikule arengule.

Turve on tegevuste kogum turvalisuse tagamiseks.

Infoturvalisus, sh küberturvalisus tähendab info kaitstust ohtude eest inimese turvateadlikkuse ja käitumisharjumuste (sh küberhügieeni) toel.

Küberohutus tähendab inimeste kaitstust võrguohtude eest, eeskätt soovimatute sündmuste, nagu tõrgete, kahjustuste, vigade, õnnetuste, kahju või nende tagajärgede eest. Ohutus tähendab siin kindlustatust mingi ohuagendi põhjustatud kahjuliku toime eest.

Küberhügieen on kogum harjumusi ja tegevusi, mis aitavad arvutite ja teiste seadmete kasutajatel säilitada ning parandada veebi turvalisust.

Kui kindlad me saame olla, et kogu info, mida me omame, kasutame, jagame, säilitame, on turvaliselt kaitstud? Kas me saame piisavalt aru, mida ja kuidas on vaja kaitsta? Kas oleme valmis aktsepteerima ja kasutama pidevalt uuenevaid turvameetmeid? Kuigi info- ja sealhulgas küberturvalisusest räägitakse üha rohkem, on oluline iga päev **fookuses hoida** seda, **mis kaitsmist vajab** ja **väärib**. Selleks on **informatsioon** ehk teave, aga ka **identiteet ja privaatsus.**

Igapäevaelus ei võta me üldjuhul liigseid riske – ei astu auto ette, väldime kahtlaste isikutega suhtlemist. Eeldame, et turvalisus on tagatud ka meid ümbritsevates organisatsioonides ja süsteemides. Aga me peame iga päev mõtlema ka sellele, mida meie saame teha ja teeme infoturvalisuse heaks.

Iga tegevus ja süsteem on turvaline esimese turvaintsidendini. Mida kiiremini ebaõnnestumine tuleb, seda kiiremini võetakse kasutusele uued turvameetmed.

13.1 Mis selle infoga siis ikkagi on?

Andmed ja info on **väärtuslikud**, sest need aitavad teha paremaid otsuseid või ennustada otsuseid, mida võib teha keegi teine. Seetõttu ihaldavad andmeid ja infot ka kurjamid. Infosüsteemide ründamise kaudu võib saada lubamatu juurdepääsu või häirida kellegi teise juurdepääsu andmetele.

Terviseandmed on ühed tundlikumad, kuna nende põhjal tehakse otsuseid inimese tervise kohta olukorras, kus andmete õigsust ei ole tihti enam aega kontrollida andmete tohutu hulga tõttu. Igasugused tõrked juurdepääsus või vead andmetes võivad kujutada ohtu inimeste tervisele.

Andmetel ja infol on üldjuhul omanik, kes määrab info kasutajate ringi. Tervishoius reguleeritakse andmetele ja infole ligipääsu infosüsteemide kasutusõigustega. Info kasutamise õiguse tõendamiseks ehk autoriseerimiseks tuleb meil ennast identifitseerida ja autentida. Halval juhul – kui meie identiteet on varastatud – tegutseb meie nime all keegi soovimatu tegelane. Kuna me võtame kasutusele aina rohkem digitehnoloogiat, siis räägime üha rohkem küberruumist ja digitaliseerimisest.

Infovara asemel on uuemates standardiversioonides turbeobjektiks vara ning teave ja kaasnevad muud varad (Cybernetica AS, 2025c). Infovara, sh kübervara on seega igasugused andmed, teave, teadmised, tarkvara, riistvara, IT-teenus, andmesalvestus, IT-seadmed, millel on ettevõtte või inimese jaoks väärtus ja mille kadumine, vargus või väärkasutamine tooks kaasa mittesoovitavaid tagajärgi ettevõtte või inimese igapäevases toimimises. **Kübervara** on osa infovarast.

Küberruum on virtuaalne keskkond (peamiselt) internetis, mis luuakse inimeste, tarkvara ja teenuste interaktsiooniga (Cybernetica AS, 2025d).

Inimene on suure osa oma eksistentsist püüdnud luua masinat, mis teda asendaks. Labakäe asemel, millega ammustel aegadel mulda kraabiti, on meil labidas, teravate hammaste asemel, millega toitu ja vääti rebiti, on nüüd käärid või nuga. Tehnoloogia arenedes, uute tööriistade, seadmete ja tarkvarasüsteemide kasutuselevõtuga osaleb tehnoloogia meie elus järjest rohkem. Mõne tehnoloogiata ei oska elu enam ette kujutadagi. Näiteks prillid on paljudele justkui keha osaks. Paraku on tehnoloogia maailm muutunud sedavõrd keeruliseks, et ükski inimene ei suuda kõigis kasutusel olevates süsteemides enam orienteeruda. Tarkus küberruumist arusaamiseks koondub IT-spetsialistide grupi valdusse. Tegelikkuses ei ole ka IT-spetsialistidel alati võimekust masinate probleeme lahendada. Rakendused pidevalt uuendavad ennast ja esitavad küsimusi. Nende küsimuste sügavam sisu jääb tavakasutajale sageli arusaamatuks. Masin on nagu elusolend, kelle „pähe“ me ei

oska näha. Kas me alati mõistame, kellele ja millele me ligipääsu anname? Mis iga uuendusega arvutis, telefonis, rakenduses muutub? Et töö või toiminguga edasi liikuda, peab seadme esitatavale küsimusele midagi vastama, aga siin on peidus turvarisk, kui me päris täpselt ei tea, mis muutub või kuidas masin pärast muudatust toimib. Kui me ise haldame oma seadet, siis peame õppima ka uuendusi tagasi võtma, kui näiteks uuendus ei toimu nii kiiresti, kui eeldasime, ja töökatkestus venib liiga pikaks. Organisatsioonis proovib IT-osakond enne järele, kas uuendused töötavad, ja alles siis need rakendatakse, aga isiklike seadmete puhul peame enne kümme korda mõtlema, kas ja mis ajal mingi uuenduse teeme. Samas uuendusi tegemata jätta ka ei saa, sest iga uuendusega remonditakse mitu varasemat turvaauku.

Mida rohkem me tehnoloogiat kasutama hakkame ja oma elu tehnoloogiatele usaldame, seda suuremasse sõltuvusse me sellest satume. Kas me oleme mõelnud ja kas oleme valmis olukorraks, kui juhtub suurem intsident või rike? Näiteks pikemaajalise elektrikatkestuse korral arvutid ei tööta, pilves olevaid faile kasutada ei saa ja igapäevane elu võib seetõttu olla halvatud. Mil määral me üldse oskame ette näha võimalikke katastroofe küberruumis? Kuidas ja kui kaua saab ilma elektri või internetita toimida haigla, perearstikeskus või tervisekeskus? Kas meie endi digidokumentide allkirjad kehtivad ka aastate pärast? Selleks, et digidokumendid oleksid loetavad ka tulevikus, on vaja iga paari aasta tagant oluliste dokumentide digiallkirja RIA juhiste kohaselt uuendada. Tuleviku-uurijad on jõudnud välja „digipimeduse“ ideeni. Digitaalne pimedus sümboliseerib katkestust ajaloolises mälus. See on olulise teabe puudumine olukorras, kus teabele juurdepääs on katkenud failivormingute, tarkvara või riistvara aegumise või mõne suurema õnnetuse tõttu. Tulevastel põlvkondadel võib digiandmete taastamine olla raske või võimatu, kuna need on salvestatud aegunud vormingusse või andmekandjale. Näiteks on juba praegu üsna keeruline kasutada diskettidele salvestatud dokumente. Digiajastu näilise infokülluse taga on pidev andmetele juurdepääsu kaotamise oht.

Kindlasti ei ole meil oma isiklike dokumentide hulgas vaja säilitada kõiki kunagi digiallkirjastatud dokumente. Peab lihtsalt teadma, kus ja **millised dokumendid** on meie jaoks olulised ning **pikaajalist säilitamist** ja **kaitsmist väärt**.

Kuidas olulised dokumendid ja info oleksid turvaliselt säilivad ja kättesaadavad ka tulevikus, selle kohta tasub kindlasti jälgida Riigi Infosüsteemi Ameti juhiseid.

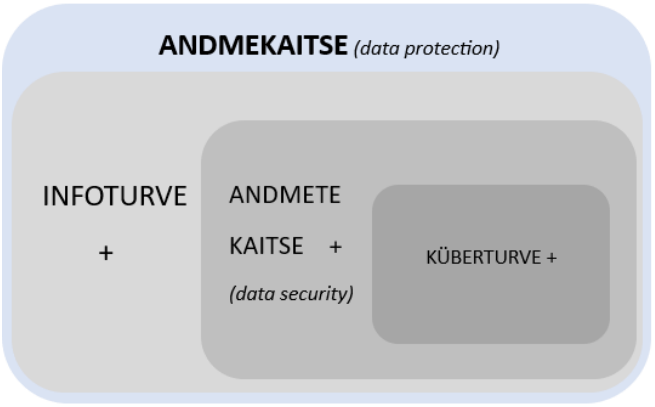
13.2 Ohud ja riskid

Iga organisatsioon on täpselt nii tugev, kui tugev on tema kõige nõrgem lüli.

Kõik organisatsioonid kaitsevad oma äriprotsessidega seotud infot ja vara, et tagada organisatsiooni toimimine. Vara kaitsmiseks on vaja peale sisemiste ohtude tegeleda ka väliste ohtudega.

13.2.1 Infoturve ja küberturve

Termineid infoturve ja küberturve kasutatakse sageli samatähenduslikena, kuigi nad tähendavad siiski erinevaid asju. Või aetakse need kaks mõistet lihtsalt segi. Järgnev mõisteskeem (joonis 13.1) aitab selgust luua.



Joonis 13.1. Infoturve ja küberturve (M. Maasik, 2024).

Infoturve (ingl k *information security*) keskendub teabe ja sellest sõltuvate äriprotsesside kaitsmisele ning sellest tulenevalt infotöötluse ja infotehnoloogia kaitsmisele. Infoturve tegeleb informatsioonile lubamatu juurdepääsu ning selle lubamatu kasutamise, avaldamise, rikkumise, muutmise, vaatamise, registreerimise või hävitamise ära hoidmisega. Kaitstav informatsioon või andmed võivad olla mis tahes vormingus, nii elektroonilises kui ka füüsilises (näiteks paberdokumendid). CISCO järgi viitab infoturve protsessidele ja tööriistadele, mis on loodud ja kasutusele võetud info kaitsmiseks (CISCO, 2025).

Infoturbe eesmärk on infoturvalisus (Cybernetica AS, 2025f).

Järgnevalt on toodud mõned näited infoturbe erinevustest digitaalses ja füüsilises maailmas.

Tabel 13.1. Infoturbe erinevused

Füüsiline maailm	Küberruum
Rünnaku ulatus ja kiirus	
Füüsilised rünnakud eeldavad füüsilist kohalolu ja on aeganõudvad. Näiteks hoonesse sissemurdmine või dokumentide vargus saab mõjutada korraga ühte asukohta.	Küberrünnakud võivad toimuda korraga globaalselt ja levida sekundite või minutitega.
Kaitse ja turvapiiri olemus	
Kaitse füüsiliste rünnakute eest põhineb füüsilistel kaitsemeetmetel nagu lukud, uksed, võred, turvakaamerad ja valvurid. On lihtne aru saada, kus lõppeb turvaline tsoon ja algab ohutsoon.	Küberruumis tagavad kaitse tulemüürid, krüpteerimine, paroolid ja autentimissüsteemid. Turvapiirid on virtuaalsed ja sageli hajutatud ning turvatsoonid ei ole alati selgelt määratletud.
Tõendite ja jälgede säilimine	
Füüsilistest rünnetest jäävad üldjuhul nähtavad jäljed - sõrmejäljed, lõhutud lukud, videokaamerate salvestised, tunnistajad. Tõendeid ei ole lihtne kustutada või muuta	Küberruumis saab rünnete jälgi kergesti muuta, kustutada või varjata. Ründajad kasutavad anonüümsuse tagamiseks VPN-e, proxy-servereid ja teisi tööriistu. Küberünnete tagajärgede tuvastamine nõuab erioskustega inimesi.

Küberturve (ingl k *cyber security*) on küberruumi kaitsmine küberohtude eest. Erinevalt infoturbest, mis käsitleb teavet sõltumatult selle vormist, keskendub küberturve digitaalses vormis varale. Küberturbe eesmärk on küberturvalisus (Cybernetica AS, 2025e).

Andmete kaitse ehk turve (ingl k *data security*) ei ole andmekaitse, vaid infoturbe üks osa – turvameetmestik, mis on suunatud otseselt andmebaaside ja andmeüksuste kaitsele ohtude eest (Cybernetica AS, 2025b).

Andmekaitse (ingl k *data protection*) on spetsiifiline valdkond, peamiselt juriidiline, seega mitte andmete turve infoturbe osana, vaid arvutites või muul viisil talletatavatele andmetele juurdepääsu reguleeriv õigusnorm ja selle rakendamine (Cybernetica AS, 2025a).

Infoturbe osa on andmete kaitse ja selle sees omakorda on küberturve, mis tegeleb küberruumi, sh digiandmete kaitsmisega küberohtude eest. Üle nende kõigi toimib andmekaitse.

INFOKILD: Isikuandmete kaitse kohta saad lugeda Riigi Infosüsteemi Ameti lehelt (Andmekaitse Inspektsioon, 2025a).

Küberturvalisuse seadus ütleb, et süsteemi turvalisus tähendab süsteemi võimet osutada vastupanu mis tahes tegevusele, mis ohustab süsteemis töödeldavate andmete või süsteemi kaudu osutatavate või juurdepääsetavate teenuste käideldavust, autentsust, terviklust ja konfidentsiaalsust (Küberturvalisuse Seadus, 2024). Seega seaduse järgi kuuluvad infoturbe kaitsealasse ka teenused, mille pakkumiseks või tarbimiseks kasutatakse infosüsteeme.

13.2.2. Infoturbe põhialused

Infoturbe eesmärk on andmete käideldavuse, konfidentsiaalsuse ja tervikluse tagamine.

Käideldavus (ingl k *availability*) tähendab, et informatsioon ja infosüsteemid on volitatud kasutajatele kättesaadavad siis, kui neid on vaja ja sellises formaadis, nagu neid on vaja.

Konfidentsiaalsus (ingl k *confidentiality*) ehk salajasus on andmetele juurdepääsu võimaldamine ainult selleks volitatud inimestele või süsteemidele.

Terviklus (ingl k *integrity*) on andmete õigsuse, täielikkuse, ajakohasuse ja eheduse (autentsuse) tagamine. Terviklus tähendab, et andmeid ei ole ilma volituseta muudetud, kustutatud ega võltsitud.

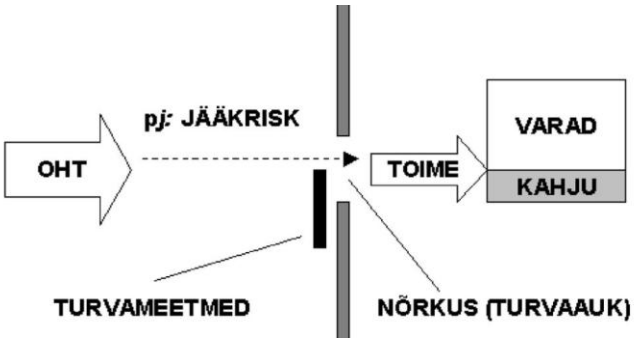
Kõige olulisem põhimõte on **andmete käideldavus** ehk andmetele ligipääs siis, kui andmeid on vaja otsuste tegemiseks. **Terviseandmete puhul** on aga ülimalt tähtis **andmete terviklus** ehk andmed peavad olema muutmata kujul, sest sellest sõltub raviotsuste õigsus. Andmetele tohivad ligi pääseda ainult need isikud, kellele on antud vastav õigus. Ligipääsuõiguste andmine peab olema põhjendatud.

13.2.3. Seadmete, võrkude ja rakenduste ning nende kasutamisega seotud peamised nõrkused, ohud ja riskid

Terviseandmete kogumiseks, töötlemiseks, jagamiseks kasutavad tervishoiutöötajad erinevaid rakendusi, infosüsteeme, seadmeid, aga tervishoiuteenuse pakkumiseks läheb vaja ka ruume ja inimesi. Kõigil eelnimetatud varadel, mida tervishoiuteenuse osutaja peab kaitsma, on mingid nõrkused.

Nõrkus on vara või meetme **nõrk koht**, mille saab ära kasutada üks või mitu ohtu (Riigi Infosüsteemi Amet, 2024c). **Oht** on olukord, kus kedagi/midagi ähvardab **ebasoovitav sündmus** (kahju) vara või meetme nõrkuse tõttu (joonis 13.2).

Infoturbes tähendab oht potentsiaalset infoturbe rikkumist kas tervikluse, käideldavuse või salajasuse osas.



Joonis 13.2. Oht ja nõrkus infoturbes (V. Praust, 2001).

Tervishoiuteenuse osutaja peab hindama **riske** ehk **ohu realiseerumise** ja võimalike halbade tagajärgede tekkimise **tõenäosust**. Pärast kõigi teadaolevate riskide käsitlemist jääb enamasti ikkagi alles mingi risk, mida organisatsiooni vaatest ei ole enam mõistlik rohkem minimeerida või mille olemasolust organisatsioon lihtsalt ei ole teadlik. Sellised riskid moodustavad **jääkriski**.

Ohte on võimalik liigitada

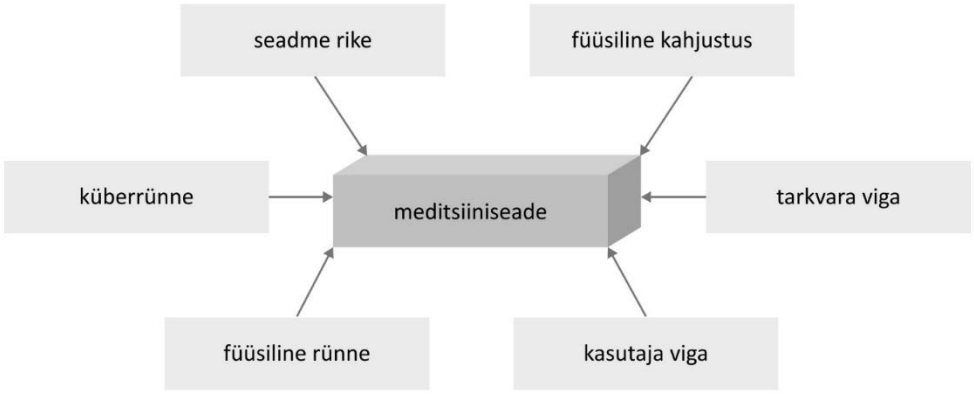
1) turvalisuse komponendi järgi (mida ohustab?);
2) allika järgi (mis põhjustab?);
3) kahjustuse olulisuse seisukohalt (kui suure kahju tekitab?).

Riskide tuvastamiseks on vaja tuvastada võimalikud ohud. Ohtude hindamisel arvestatakse ohu **relevantsust** (asjakohasust).

Relevantsed on need ohud, mis

- võivad tekitada tõsist kahju;
- on konkreetse rakenduse ja kasutusala puhul realistlikud.

Näiteks **meditsiiniseadmetega seotud peamised ohud** on esitatud joonisel 13.3.



Joonis 13.3. Meditsiiniseadmetega seotud ohud (M. Maasik, 2024).

INFOKILD: Ohtude kohta saad põhjalikumalt lugeda E-ITS standardist (Riigi Infosüsteemi Amet, 2024c).

> Standardis on toodud 47 alusohtu, mis tõenäoliselt katavad ära ka meditsiiniseadmed. E-ITS-is ei ole eraldi meetmeid nende seadmete kaitsmiseks/turvamiseks. Need tuleb tervishoiuteenuse osutajal riskihalduse teel ise välja töötada. Kui alusohtude loetlus ei ole ohtusid, mis tervishoiuteenuse osutaja meditsiiniseadmeid ohustaksid, siis tuleb need riskihalduse abil välja selgitada.

Infoturve tegeleb **võimalike ohtude ärahoidmisega** ehk riskide minimeerimisega, **rakendades** mitmesuguseid **meetmeid** taristule, tehnoloogiale, inimestele.

Ohtude realiseerumisel on tervishoiuteenuse osutaja või saaja jaoks mingi **tagajärg** – halvemal juhul tervisekahju, rahaline kahju, rahatrahv. Selleks, et neid tagajärgi ei tekiks, on vaja kaitsta organisatsioonis ja ka isiklikus vaates arvuteid, ühendusi, andmeid, tegevusi, hooneid. Nende objektide ja varade kaitseks on võimalik kasutada **kaitsemeetmeid**, nagu

1) tulemüür, ID-kaart autentimiseks ja digiallkirjastamiseks, salasõnad jmt arvutis oleva infovara kaitseks;
2) füüsilised kaitsemeetmed (uste lukustamine, turvakaamerad jne).

Näide kaitsemeetmete kohta E-ITS standardist

INF.8.M4 Kodutöökoha õige korraldus

a. Kodutöökoht asub võimaluse korral eluruumidest eraldi paiknevas lukustatava uksega ruumis.

b. Kodutöökoha sisustus on valitud ergonoomika, tööohutuse ja tervisekaitse nõudeid arvestades.

c. Kodutöökohas on järgitud organisatsioonis üldkehtivaid nõudeid töökohale ja töökeskkonnale.

d. Arvutiekraan on paigutatud nii, et valgus ekraanilt otse ei peegelduks ja kõrvalised isikud töötaja selja tagant ekraani ei näeks.

e. Kodutöökoht on konkreetsete tööülesannete täitmiseks piisavalt varustatud, selleks vajalikud töövahendid annab tööandja (Riigi Infosüsteemi Amet, 2024f).

Rakendatavatel kaitsemeetmetel on siiski omad nõrkused, näiteks ei kannata põrutamist, kardavad vett, päikest, tulemüüris on „augud“, salasõnad on nõrgad, inimlikud eksimused. Nõrkused on liigitatud:

1) taristu nõrkused (amortiseerunud taristu, hoone uste ja akende füüsilise kaitse puudused, puudulik võrguhaldus jmt);
2) personaliga seotud nõrkused (kogenematus, liigne usaldamine, turvanõuete eiramine, vähene koolitus jmt);
3) organisatsioonilised nõrkused (juhtkonna vähene toetus ja pühendumus, töökorralduse puudused, dokumentatsiooni puudumine jmt);
4) tehnoloogia nõrkused (puudused turvameetmete valikul, väär pääsuõiguste jaotamine, halb salasõnahaldus jmt).

Nende nõrkuste tõttu võivad organisatsiooni, inimesi ja infotehnoloogiat ohustada erinevad sündmused – füüsiline kahjustus, küberrünne, loodussündmus, elektrikatkestus, tarkvara viga, riistvara viga, füüsiline rünne, kasutaja viga, administreerimisviga jmt. Eeltoodud sündmused võivad olla isetekkelised, aga neid võivad põhjustada ka nn ohuagendid ehk kurjategijad.

Järgnevalt on selgitatud infovaradega seotud riske (joonis 13.4).

Joonis 13.4. Infovaraga seotud riskid (J. Metsallik).

Infovara on igapäevaste toimetuste jaoks sageli hädavajalik. Neid vahendeid ja andmeid on vaja kaitsta väärkasutuse ja rikkumise eest. Digitehnoloogia maailma riske ei ole lihtne hinnata. Arvatakse, et küberõnnetusi kutsuvad esile peamiselt häkkerid, kes ründavad ainult mõjuvõimsaid isikuid ja asutusi. Jah, kuritahtlik digilahenduste kahjustamine on kindlasti üks rikete põhjusi, kuid kaugeltki mitte ainus. Iga võrguga ühendatud arvuti võib sattuda rünnaku sihtmärgiks, kuna pakub võimalust rünnakute jätkamiseks teise kasutaja identiteedi ja asukoha kattevarjus. Tahtliku rünnaku alla võib liigitada ka arvutivarguse. Varga motiiv ei pruugi olla seotud arvutis sisalduvate andmetega ega arvuti omaniku isikuga, arvutil on väärtus ka tühja riistvarana. Arvuti kadumine aga tekitab tõenäoliselt katkestuse kasutaja töös ja põhjustab ka majanduslikku kahju.

Kujutame näiteks ette olukorda, kus visiiti ootav patsient haarab tervishoiuteenuse osutaja ooteruumist kaasa vastuvõtutöötaja arvuti. Isegi kui patsient õnnestus tuvastada ja politsei leidis arvuti kiiresti üles, viibis seade mõned tunnid väljaspool tavapärast turvatsooni. Kas andmete salajasust, terviklust või käideldavust rikuti? Ilmselgelt ei ole ohutu sellise arvutiga kohene töö jätkamine, kuna andmete terviklus võib olla rikutud. Arvuti kõvakettast täieliku koopia tegemine võtab aega mõnikümmend minutit. Arvutis mõne faili väljavahetamine ei võta ka palju aega. Kui pikaks kujuneb tervishoiuteenuse osutaja töö katkestus sõltub sellest, kas leidub asendusarvuti töö jätkamiseks. Sellised küsimused kuuluvad tervishoiuteenuse osutaja riskianalüüsi juurde, sest arvutid ei ole seina või põranda külge kinnitatud ja keskuste uksed ei ole väljumiseks lukustatud.

Digiandmetega seotud rikete põhjuseks võib olla ka kasutaja tahtmatu eksimus. Näiteks võib andmetesse viga tekkida töötaja tähelepanematuse, oskamatuse või ebaselge kasutajaliidese tõttu. Volitamata muudatused saavad meie arvutis või muus digiseadmes toimuda, kui oleme ise hooletud oma salasõnadega, unustame arvuti lukustamata, kui lahkume seadme juurest või kui meie arvutisse keegi ebaseaduslikul teel sisse murrab.

Kasutaja ise võib kogemata vigastada infosüsteemi osaks olevaid seadmeid, näiteks ajades ümber kohvitassi või komistades juhtmete otsa. Seadmeid võivad rikkuda ka loodusjõud – näiteks hoonesse või väliseadmesse sattunud tulvavesi või näriliste hävitustöö internetijuhtmete kallal. Toodud näidetes kirjeldatud sündmustel on erinev tõenäosus ja erineva kaalukusega tagajärjed. Võrguühenduse

katkemine küll takistab andmete levitamist ehk käideldavust, kuid samal ajal võib suurendada andmete salajasust ja terviklust. Eks ole huvitav! Organisatsiooni talitluspidevust võivad sellised intsidendid mõjutada, kui ei ole rakendatud piisavaid infoturbemeetmeid.

Tabelis 13.2 on toodud mõnede olukordade kirjeldused, nendega kaasnevad ohud ja võimalikud tagajärjed organisatsiooni jaoks.

Tabel 13.2 Organisatsiooni tegevused, ohud ja tagajärjed.

Sündmus / olukorra kirjeldus	**Oht**	**Tagajärg organisatsioonile**
Kahe haiglatöötaja samaaegne haigestumine.	Personali piisamatus. Suureneb hooletusest tehtud vigade arv (Riigi Infosüsteemi Amet, 2024i)	Üks ülekoormatud töötaja märgib valele patsiendile vähidiagnoosi, mistõttu tekib tervikluskadu.
Esimene juhtum: Kuna krüptimine on liiga keeruline, edastab tervishoiutöötaja patsiendi andmed e-kirjaga avateksti kujul. Teine juhtum: töötaja küll krüptib, aga kasutab oskamatusest liiga lihtsat salasõna või saadab salasõna sama kirjaga, kus on krüptitud andmed.	Andmete konfidentsiaalsuse või tervikluse kadu kasutamisvigade tõttu (Riigi Infosüsteemi Amet, 2024d).	Konfidentsiaalsuse kao tõttu on ründajatel võimalus edastatavaid andmeid pealt kuulata ja tervishoiuteenuse osutajat nende andmete alusel rünnata. Tervikluskao puhul võib tervishoiutöötaja teha vale raviotsuse.
Töötaja on jätnud töökohalt lahkudes arvuti lukustamata.	Isikliku vastutuse puudumine turbeprotsessis. Töötajad enamasti väldivad lisakohustusi, mistõttu jäävad turvameetmed rakendamata (Riigi Infosüsteemi Amet, 2024g).	Volitamata isiku ligipääs tervishoiuteenuse osutaja infosüsteemidele ja andmetele, mille tõttu võib tekkida andmete konfidentsiaalsuse ja tervikluse kadu. Tervikluse kao tagajärjeks võib olla raviviga.
Töötaja kasutab sotsiaalvõrgustikes ja töökeskkonnas samu salasõnu.	Hooletus andmete kasutamisel. Sotsiaalvõrkudes ja töökeskkonnas samade salasõnade kasutamine võib viia IT-süsteemide kuritarvitamiseni salasõna äraarvamise kaudu (Riigi Infosüsteemi Amet, 2024i).	IT-seadmete ja tarkvara manipuleerimine või väärkasutamine võib tervishoiuteenuse osutajale kaasa tuua tundlike andmete lekkimise või IT-süsteemide kahjustumise ja seeläbi töö katkestuse, majandusliku kahju, lepingulise kahju.
Töötaja jagas haiglavälise partneriga patsientide terviseinfot puudutavaid faile, mis asuvad pilves.	Sõltuvus pilvteenuseandjast (kontrolli kaotamine) (Riigi Infosüsteemi Amet, 2024h).	Välise pilvteenuse kasutamisel sõltub organisatsioon pilvteenuseandjast ega oma täit kontrolli äriprotsesside ja nende turvalisusega seotud teabe üle. Organisatsioon ei tea, kas pilvteenuseandja rakendab turvameetmeid nõuetekohaselt.
Töötaja unustas oma tööarvuti rongi.	Isikuandmete konfidentsiaalsuse kadu. Andmete sattumine volitamata isikute kätte (Riigi Infosüsteemi Amet, 2024e).	Andmelekke tagajärjel võib toimuda mõne isiku identiteedivargus.
Töötaja lubas kodus lastel kasutada tööarvutit veebis surfamiseks.	Kodus töötamise eeskirja puudumine või puudulikkus. Kui kodus töötamise eeskirjaga ei ole sätestatud siseteabe töötlemise korda, võib töötaja talletada tundlikke andmeid ebaturvalisse	Võib tekkida andmete konfidentsiaalsuse ja tervikluse kadu, mille tagajärjeks võib olla vale raviotsus, identiteedivargus või konfidentsiaalse info sattumine volitamata isikute kätte.

	asukohta, näiteks koduarvutisse, millele võivad ligi pääseda ka teised pereliikmed (Riigi Infosüsteemi Amet, 2024f).	
Töötaja paigaldab tööandja telefoni suhtlusrakenduse matkaklubiga suhtlemiseks. Suhtlusrakendusega toimimiseks aktiveerib töötaja asukohajälgimise ja kõnedele juurdepääsu. Suhtlusrakenduse teenuse pakkuja saab juurdepääsu töökõnedele ja sõnumitele.	Organisatsiooni mobiiltelefoni kasutamine isiklikuks tarbeks. Organisatsioonile kuuluva mobiiltelefoni kasutamisel võivad tekkida hooletusvead, mille käigus aetakse segi konfidentsiaalsust nõudvad tööasjad ja erasuhtlus (Riigi Infosüsteemi Amet, 2024j).	Volitamata isikud võivad saada organisatsiooni kohta konfidentsiaalset teavet või tekib organisatsioonile lisakulu.

Infoturbe üks eesmärk on tagada organisatsiooni **talitluspidevus**. Talitluspidevuse halduse sisuks on organisatsiooni ettevalmistamine **teenuse osutamise jätkamiseks** või **teenuste kiireks taastamiseks** pärast intsidenti.

Intsident on ebasoovitav vahejuhtum, nagu loodusõnnetus, elektrikatkestus, küberintsident. **Küberintsident** on olukord, kus rikutakse organisatsiooni või üksikisiku infosüsteemi või selles oleva info konfidentsiaalsust, terviklust ja käideldavust.

Talitluspidevuse tagamiseks peavad organisatsioonid ja ka üksikisikud hindama info ja andmetega seotud ohtusid ning nende ilmnemise tõenäosust ehk tegema riskianalüüsi. **Riskianalüüs** on riski iseloomu ja taseme väljaselgitamine, mis loob aluse riskide hindamiseks ja riskikäsitluseks.

Riskianalüüsi läbiviimise ja infoturbe meetmete rakendamise eest organisatsioonis vastutab üldjuhul infoturbejuht või kui sellist ametit ei ole, siis organisatsioonis selleks määratud töötaja.

13.3 Küberrünnakud ja -pettused

Küberrünnak on pahatahtlik tegevus, mis seisneb suunatud sissetungimises võõrasse arvutivõrku, et varastada või muuta andmeid või kahjustada süsteemi. Küberrünnakud pannakse toime IT-vahendite nõrkusi kasutades. Küberrünnakud on kas isikuvastased (erinevat liiki ahistamised, ebaseaduslik ligipääs seadmetele, identiteedivargus jne) või omandivastased (pahavara levitamine, intellektuaalomandi vargus, arvutiressursi vargus jne).

Iga töötaja peab olema suuteline ära tundma peamisi küberkuritegusid ning oskama nendele töökeskkonna nõuete kohaselt reageerida. Kui langed eraisikuna küberpettuse ohvriks, võib olla sellel mõju sinule ja sinu lähedastele. Kui seesama juhtub sinu kui organisatsiooni töötajaga, võib see mõjutada juba märksa suurema hulga inimeste ja ka ettevõtte heaolu. Näiteks tervishoiuasutuses töötades võid seada ohtu patsientide privaatsuse ja tervise.

Küberrünnakute alla kuuluvad küberpettused, millest saad järgnevate selgituste abil ülevaate.

13.3.1 Pahavara

Pahavara on selline tarkvara, mille eesmärk on kahjustada sinu seadmeid. Erinevat tüüpi pahavarade puhul kasutatakse tihti ka sõna „viirus“. Pahavara võib sattuda seadmesse näiteks tundmatutelt

saatjatelt tulnud linkide või manuste avamisel, tundmatute mälupulkade sisestamisel või mitteametlikelt kodulehtedelt tarkvara alla laadimisel. Rohkem infot pahavara ja selle kohta, mida teha, kui kahtlustad pahavaraga nakatumist, leiad RIA kodulehelt (Riigi Infosüsteemi Amet, 2024n).

Pahavaraga nakatumisest võib märku anda see, kui

- arvuti on aeglane;
- mõned lehed ei avane (näiteks viirusetõrjetarkvara tootjate veebilehed);
- ootamatu reklaamakende avanemine ja veateadete kuvamine.

Selleks, et pahavaraga nakatumist vältida, tuleb

1. alati kasutada seadmetes tarkvara uusimaid versioone ja paigaldada vajalikud turvauuendused;
2. tarkvara alla laadimiseks ja viirustõrje paigaldamiseks kasutada ainult tootjate ametlikke kodulehti;
3. hoiduda tundmatute mälupulkade arvutisse panemisest ning võõrastelt saatjatelt saabunud e-kirjades manuste ja veebilinkide avamisest;
4. vältida mittevajaliku tarkvara paigaldamist arvutisse/süsteemi;
5. operatsioonisüsteemi turvasätted nõuetekohaselt seadistada;
6. tulemüür seadistada ja sisse lülitada.

Reklaamvara (ingl k *adware*)

- Suunab kasutajale reklaami ja/või kogub andmeid tema võrgukäitumise kohta.
- Nakatunud seadmes loob reklaamvara töölauale ja stardireale uued ikoonid.
- Veebilehitseja välimus võib muutuda ja käituda ebatavaliselt.
- Otsingumootor on tundmatu, avanevad võõrad veebilehed ja avanenud veebilehti on raske sulgeda või need avanevad iseenesest uuesti.
- Töölauale või Start-menüüsse on tekkinud uued ikoonid või otseteed.
- Reklaamvara suunab ohvri leheküljele, mille vaatamise eest tuleb raha maksta.
- Reklaamvara on nuhkvara tüüp, mis genereerib hüpikakna tüüpi reklaame.
- Erinevalt teistest nuhkavara tüüpidest keskendub reklaamvara peamiselt reklaamile, mitte isikliku teabe kogumisele ega volitamata juurdepääsu saamisele süsteemile.

Lunavara

Üks pahavara liike on lunavara, teise nimega ka krüptoviirus või krüptouss. Lunavara eesmärk on krüptida arvutis olevaid andmeid. Seejärel nõuavad kurjategijad lunaraha, pakkudes vastu andmete dekrüptimisvõtit. Arvuti või nutiseadme lunavaraga nakatumisele võib viidata see, kui

- ekraanile ilmub lunarahanõude teade;
- veebilehitseja suunab lehele, kust saab osta failide dekrüptimise tööriista, või pakub lunaraha tasumise võimalust.

13.3.2 Õngituslehed

Õngituslehtede puhul maskeerivad kurjategijad veebilehe nii, et see oleks võimalikult sarnane reaalse asutuse, tootja või kaubamärgi veebilehega. Nad tekitavad tunde, et tegemist on õige veebilehega, kuigi tegelikult on veebilehe eesmärgiks varastada sinu andmeid.

Kuidas pettusele jälile saada?

- Jälgi veebilehe aadressi, kas sinna on lisandunud tähti, numbreid või on aadress täiesti erinev. Aadress peab olema täht-tähelt sama originaaliga!

- Kontrolli kahtluse korral teises veebilehitseja aknas otsingumootori abil, milline on sinu soovitud kaubamärgi või keskkonna täpne nimi ja ametlik koduleht.

Veel ennetusmeetmeid ning viise, kuidas käituda, kui oled langenud sellise pettuse ohvriks, leiad RIA kodulehelt (Riigi Infosüsteemi Amet, 2024n).

Arvepettused

Arvepettuste puhul võetakse ühendust kirja, e-kirja või telefoni teel ning väidetakse end esindavat näiteks mõnda teenusepakkujat või tarnijat. Seejärel palutakse tulevaste arvete jaoks muuta teenusepakkuja pangaandmeid nii, et uued maksed laekuvad petiste kontole.

Kui puutud töötades kokku arvetega, siis:

- kontrolli alati kõiki päringuid, mis sinu ettevõtte partnerid saadavad, kuid eriti siis, kui asi puudutab maksete sooritamiseks pangaandmete muutmist;
- kui makse ületab limiiti, kontrolli partneri andmed enne üle, näiteks telefoni teel;
- jälgi hoolega, millist infot sa sotsiaalmeedias oma tööandja kohta jagad.

Rohkem viise, kuidas ettevõte ja töötaja saavad arvepettusi vältida, leiad RIA kodulehelt arvepettuse kampaania plakatilt (Riigi Infosüsteemi Amet, 2018).

Õngitsuskirjad

Paljusid pettuseid püütakse toime panna e-kirja teel. Ka tervishoiuvaldkonnas töötades on e-kirjade saamine ja saatmine tavapärase tööprotsessi osa. Tüüpilisemad pettused, mis levivad e-kirja teel, on õngitsuskirjad, mille eesmärk on varastada andmeid või raha.

Kuidas õngitsuskirja ära tunda?

- Kirja saatja on sulle võõras.
- Kirjas on palju grammatikavigu.
- Pealkiri võib olla kirjutatud läbivalt suurte tähtedega.
- Kirja sisus võib olla ähvardamist, hirmutamist või kiireloomulisuse rõhutamist.

Suhtlusrünne ehk sotsiaalne manipuleerimine

Suhtlusründe (ingl k *social engineering*) tulemusel võib ründaja saada teabele või IT-süsteemidele lubamatu juurdepääsu, luues kontakte telefoni, e-posti või sotsiaalvõrgu kaudu ning kasutades ära inimeste abivalmidust. Suhtlusründe ohvri poole pöördumisel kasutatakse talle tuttavate inimeste nimesid, et saavutada usaldusväärsust. Kui töötaja sellist ründeviisi piisaval määral ei tunne, siis osavalt suheldes suunatakse töötaja toimima lubamatul viisil. Suhtlusründe tulemusena võib ründaja hankida konfidentsiaalset teavet, levitada kahjurtarkvara või koguni sundida töötajat väidetavale äripartnerile raha üle kandma (Euroopa Ülemkogu & Euroopa Liidu Nõukogu, 2025).

13.4 Küpsised ja küberturvalisus

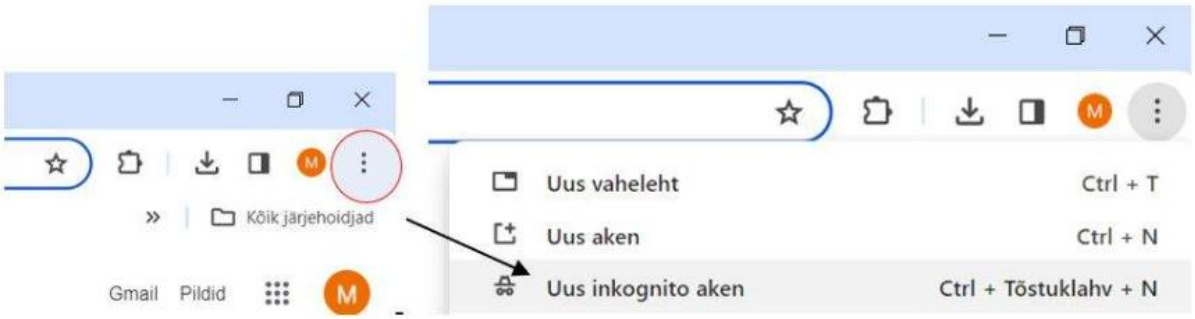
Küpsised on väikesed failid, mis laaditakse alla ja salvestatakse sinu seadme veebilehitsejasse sel ajal, kui veebilehte külastad. Küpsised on mõeldud näiteks selleks, et saada infot kasutaja veebisaidi külastuse detailide kohta või salvestada sisestatud andmeid. Kuigi küpsised on tavapäraselt ohutud,

võivad küberkurjategijad neid osavalt ära kasutada, et internetis meiena esineda ja saada seeläbi juurdepääs meie kontodele.

Selleks, et küpsistega seotud ohte vältida, peame

1. alati olema ettevaatlikud, kui oma andmeid kuhugi sisestame;
2. deaktiveerima oma veebilehitsejas küpsiste salvestamise;
3. vältima salasõnade salvestamist veebilehitsejasse;
4. hoidma pahavara tõrjuvad tarkvarad uuendatuna.

Kui soovime veebis ringi liikuda nii, et meist ei jääks maha küpsisepuru, siis peaksime kasutama **inkognito veebiakent**, mis on leitav, avades näiteks Google Chrome'i veebiakna. Ülemises paremas nurgas on kolm punkti, millel klõpsates avaneb järgmine ekraanipilt:



Ent privaatsusrežiim pakub kohalike ründajate vastu **kaitset ainult siis**, kui oleme hoolikad ja ettevaatlikud. Näiteks **ei ole soovitatav** privaatsusrežiimis **faile alla laadida** ega **brauserisse järjehoidjaid seada**.

Küpsised saab ka ära kustutada. Veebibrauseri akna ülemises paremas nurgas kolme punkti peal klõpsates tuleb valida **Seaded** ja avaneva akna vasakus menüüs **Privaatsus**. Sealt on leitav info küpsiste kohta ja ka kustutamise võimalus.

13.4.1 Turvaline veebileht

Turvaliseks toimetamiseks internetis peame veenduma, et:

- veebileht, kuhu on tarvis isiklikke andmeid sisestada, on kaitstud turvalise krüptitud ühendusega – **aadressi alguses on https://**. Seda saab vaadata, kui liikuda aadressi peale ja parema hiireklahviga avanevast menüüst valida **Kuva alati täielikud URL-id**. Siis saab näha tervet aadressi.

- veebiaadress, millel oleme, on täht-tähelt seesama, mis peaks olema (google.com *vs*. g00gle.com).

Küberturvalisuse ABC-d saab korrata RIA kodulehelt (Riigi Infosüsteemi Amet, 2024m).

13.5 Küberintsidentidest teavitamine

Kui sulle tundub, et oled tööga seoses **avastanud** võimaliku **küberpettuse** või langenud selle ohvriks, anna sellest viivitamatult teada oma organisatsiooni IT-osakonnale, infoturbe juhile või **inimesele, keda peab organisatsiooni reeglite kohaselt teavitama.**

Kas sina tead, keda sa pead oma organisatsioonis informeerima küberpettusest?

Küberintsidendist teavitamiseks on välja töötatud küberintsidendi teavitusvorm (cert.ee). Lihtsa intsidenditeavituse võib saata ka aadressil cert@cert.ee (Riigi Infosüsteemi Amet, 2025). Peale RIA võivad nii organisatsioonid kui ka eraisikud pöörduda Politsei-ja Piirivalveameti poole veebilehe kaudu (Politsei- ja Piirivalveamet, 2025).

Ära karda küberpettusest teada anda, sest isegi kui kellelgi ei õnnestu aidata sind tekkinud kahju vähendamisel, võib see ära hoida tulevasi kuritegusid.

13.6 Turvastrateegiate rakendamine

Infoturvalisus, sh küberturvalisus on info kaitstus ohtude eest inimeste turvateadlikkuse ja käitumisharjumuste (sh küberhügieeni) toel. Turvalisus on kindlustunne, et elu ja vara on kaitstud ning kasutatavad turvastrateegiad ja käitumisharjumused on õiged ja tõhusad.

Organisatsioon loob küll infoturbe meetmestiku ja reeglistiku, kuid **iga üksiku inimese kohustus on nendest reeglitest kinni pidada**. Töötades mingis organisatsioonis, peaksid infoturbe reeglid olema paigas ja töötajad koolitatud, kuid eraelus peab iga inimene suutma oma infovara ise kaitsta.

Infovara hulka, mida on vaja infoturbe mõistes kaitsta, loetakse:

- IT-seadmed (riistvara, sideseadmed, toiteseadmed jm);

- andmesidekanalid;
- tarkvara (süsteemne ja rakendustarkvara);
- andmed ja informatsioon;
- andmekandjad (sh dokumendid);
- füüsiline taristu (hooned, tööruumid, jms);
- transpordivahendid (nt autod – kui nendega veetakse strateegiliselt olulist infovara).

Kaitsta on vaja ka **töötajaid**, kes kannavad organisatsiooni jaoks olulist teadmist.

13.6.1 Infoturve organisatsioonis

Infoturbe ülesanne organisatsioonis on **säilitada** igapäevatöö käigus kasutatava **teabe turvalisus** ja seeläbi **organisatsiooni tõrgeteta toimimine**.

Infoturve on pidev protsess, mitte ühekordne tegevus, ja algab juhtkonna pühendumusest. Infoturbe tagamiseks avaliku sektori organisatsioonis, sealhulgas enamikus tervishoiuorganisatsioonides, on oluline juurutada E-ITS standard või ISO 27001.

INFOKILD: E-ITS standardi kohta saad rohkem infot RIA lehelt (Riigi Infosüsteemi Amet, 2024k).

> Digiriigi Akadeemias on ka kaks kursust E-ITS teemadel (DigiriigiAkadeemia.ee, 2025):
>
> 1. Eesti infoturbe standardi (E-ITS) ABC
> 2. E-ITS rakendamine: kaitsetarbest rakendusplaanini
>
> ISO 27001 kohta saad lugeda Eesti Standardimis- ja Akrediteerimiskeskuse kodulehelt (Eesti Standardimis- ja Akrediteerimiskeskus, 2024).

Organisatsiooni infoturbe toimimise eelduseks on juhtkonna eraldatud ressursid ja üheks alustalaks kõigi töötajate süsteemne koolitamine. Infoturve kaitseb organisatsiooni ohtude eest üksnes juhul, kui see on loomuliku osana äriprotsessidesse integreeritud. Infoturbe nõuetega peavad kursis olema ja neid oma töös arvestama **kõik töötajad**, igaüks oma töölõigu ja vastutuse ulatuses.

Kui turvateadlikkus on madal ja -koolitus ebapiisav, siis

1. ei suuda töötajad turvaintsidentidel ja tehnilistel riketel vahet teha;
2. turvaintsidentidele ei reageerita;
3. nõrkused jäävad parandamata.

Üks infoturbemuresid on ka hooletus. Kui töötaja jätab konfidentsiaalse teabega dokumendid printerisse või oma töölauale või viskab need prügikasti, millele igaüks ligi pääseb, ei ole failide krüptimisest kõvakettal kasu.

Organisatsioonid rakendavad väga palju erinevaid turvastrateegiaid, millest paljud on kasutatavad ka eraelus.

Tabel 13.3. Infoturbestrateegiad

Autentimine	Eestis on igal inimesel riigi poolt antud isikukood, mis on tema esmane identiteet ja riik tagab ka iga isikukoodi omava inimese isikusamasuse. **Autentimine** on protsess, mille käigus kontrollitakse ja kinnitatakse kasutaja identiteet mingit tüüpi identsustõendi alusel, milleks võib olla: • esitatud teave, näiteks salasõna;

	• ese, näiteks kiipkaart või muu turvatõend; • eristav püsitunnus ehk biomeetrik (Riigi Infosüsteemi Amet, 2024b) • eristav asukoht (aadress) (Riigi Infosüsteemi Amet, 2024a)
ID-kaardi kasutamine	**ID-kaardil** on isikuandmete fail, kus on kirjas isiku nimi ja põhiandmed. Kaardi sisestamisel kaardilugejasse on info kohe loetav, kuna fail ei ole kaitstud. Iga kord on vaja enne mõelda, kui ID-kaart kuhugi lugejasse panna. Tervishoiuasutuses töötades tuleb sageli arvutisse või programmidesse ligipääsuks logida sisse just ID-kaarti kasutades. **ID-kaardi ohutu kasutamise kõige olulisem põhimõte: ID-kaarti ei tohi jätta lugejasse kauemaks kui hädavajalik.**
Kaheastmeline autentimine	**Turvategevus**, mis nõuab kasutajalt enda identifitseerimist **kahel** sõltumatul viisil. Näiteks ID-kaardiga autentimisel peab kasutama: 1) ID-kaarti (ese). 2) PIN-koodi (teadmine). Kaheastmelise autentimise vahendid on veel biomeetriline pass, Mobiil-ID, Smart-ID, mis võimaldavad tuvastada, kas • kasutajal on võti füüsiliselt kaasas (spetsiaalne seade, nutiseade); • inimene oskab teha dokumendil näidatud allkirja (biomeetriline pass); • kasutajal on õiged sõrmejäljed (biomeetriline pass); • kasutajal on sobiv näokuju (biomeetriline pass); • kasutaja mäletab oma PIN-koodi (Smart-ID, Mobiil-ID)
Digi-allkirjastamine	**Digiallkiri** on tavalise allkirjaga võrdväärne allkiri digitaalsel kujul oleva info allkirjastamiseks. Digiallkirja abil tõendab allkirja andja oma seost dokumendiga ja kinnitab, et dokumenti ei ole muudetud kolmandate isikute poolt info edastamise protsessi käigus. Samas ei kaitse Digiallkiri dokumenti infolekke eest. Eestis saab digiallkirja anda ID-kaardi, Mobiil-ID ja Smart-ID abil.
Krüptimine	**Krüptimise** eesmärk on muuta dokumendis olevad andmed võõrastele loetamatuteks ja võimaldada ligipääs ainult volitatud osapooltele, kes teavad salasõna või krüptovõtit. Krüptimine on väga oluline näiteks terviseandmete liigutamisel, sest vastasel korral näeksid neid andmed kõik, kes võrguliiklust jälgivad.
Inkognito lehitsemine	**Inkognito režiim** ehk privaatne lehitsemine on veebis surfamise meetod, mida võimaldavad kõik suuremad veebibrauserid. Inkognito režiimil saab internetis liikuda n-ö puhta lehena. See tähendab, et sulle ei näidata personaliseeritud pakkumisi ning sa ei saa kasutada brauserisse salvestatud salasõnu, kasutajanimesid ega muud sarnast infot. Täpsemaid juhiseid inkognito režiimis veebiakna avamisest leiad erinevate teenusepakkujate veebilehitsejate kasutusjuhenditest, näiteks Google Chrome'i abikeskusest (Google, 2025).

13.6.2 Andmete hoidmine pilves

Tänapäeval on enamik meie digimaterjalidest ja andmetest kuskil pilves ja me väga täpselt ei tea, kus need andmed tegelikult on. Kui andmed on pilves, siis peame arvestama, et **pilv ei hoolitse meie arhiivi eest**. Pilv on vaid üks teenus. Töökohas hoolitseb pilveandmete ja failide varundamise eest IT-osakond. Isiklike andmete ja failide puhul peame oma andmete paiknemise ja säilimise eest ise hoolitsema. **Lihtsaim võimalus** on **dubleerida** enda jaoks olulist infot mitmes kohas.

13.7 Kaugtöö

Tegemist on väga levinud töötamise viisiga, kus töötajad sageli kasutavad oma isiklikku arvutit, nutiseadet jmt IT-vara. Kaugtöö lubamine või mittelubamine on iga organisatsiooni otsustada. Kui organisatsioon lubab teha kaugtööd, siis on seda kõige turvalisem teha organisatsiooni antud arvutiga ja turvatud virtuaalse privaatvõrgu (ingl k *virtual private network*, VPN) kaudu. **Organisatsiooni arvutit ei tohi ühelegi kõrvalisele isikule kasutada anda.**

Kui töötaja teeb kaugtööd oma isikliku arvuti või nutiseadmega, siis sinna ei tohiks salvestada tööga seotud andmeid ega informatsiooni. Neid ei tohi salvestada ka isiklikule **mälupulgale** ega kõvakettale. **Mälupulk** on andmekandja, millega on seotud turvariskid. Esimene neist on seotud mälupulga kadumisega, kui see sisaldab tundlikke andmeid, mis pole mõeldud asutusväliseks kasutuseks. Teiseks võidakse mälupulki kasutada pahavara levitamiseks. Seetõttu ei tohi kunagi ühendada arvuti külge sellist andmekandjat, mille päritolu pole teada. **Oma arvutiga töötades peaksid töödokumendid olema pilves.** Iga tööandja peab kehtestama reeglid, kus ja kuidas tööfaile hoida. Kaugtööd tehes peame jälgima ka füüsilise turvalisuse aspekte, näiteks töötamise koht.

Kaugtööd tehes kasutame enamasti Wifit. Riigi Infosüsteemi Ameti selgituse kohaselt on **Wifi** traadita sidevõrk, mille kaudu saab näiteks sülearvuti arvutivõrku ühendada ilma võrgujuhtmeta. Avalik võrk, isegi kui see küsib salasõna ja on krüpteeritud, ei pruugi olla turvaline. Seetõttu ei tohiks tööd tehes kasutada avalikku võrku ja ka isiklike asjade ajamiseks **tuleks eelistada** näiteks **sülearvutis olevat mobiilse interneti SIM-kaarti** või luua oma **mobiiltelefoniga *hotspot*-ühendus**.

Järgnevalt on selgitatud töö ja isiklike toimingute eristamise olulisust infoturbe mõistes.

Töötades mingis organisatsioonis, on tänapäeval infoturbereeglid paigas ja töötajad koolitatud, kuid eraelus peab iga inimene suutma oma infovara ise kaitsta. Samuti on oluline kaitsta organisatsiooni antud töövahendeid kaugtöö puhul.

Kas me kasutame pereliikmetega suhtlemiseks nutiseadmeid või arvutit? Kus me hoiame teavet oma sõprade sünnipäevade ja kultuurisündmuste kohta? Kus on meie perepildid, reisiplaanid, isiklikud failid? Nutiseadmed ja Internetipõhised tehnoloogiad on ammu levinud väljapoole kontori-, labori- ja tootmisruume. Meil on isiklikud e-postiaadressid, kodulehed, kalendrid, internetipanga, e-kooli ja veebipoe kontod. Me oleme pidevalt Interneti levialas. Internet on meil kaasas kodus, rongis, kohvikus, teatris, koolis, metsas ning isegi vannitoas, saunas ja tualetis. Kontor ei ole selles mõttes ju midagi erilist, ka seal oleme ühendatud Internetiga. Tööl puutume me kokku andmeruumiga, mida reguleerib meie tööleping. Muus osas on töö- ja eraelu sageli läbi põimunud. Oleme igal pool nutiseadmetega Internetis.

Kas meil on vaja eraldi nutiseadmeid töö- ja eratoimetusteks? Kas meil on vaja eraldi kalendreid töö- ja erasündmuste märkimiseks? Kas meil on vaja eraldi e-postiaadresse töö- ja erakirjade jaoks? Kas meil on vaja eraldi telefoninumbreid töö- ja erakontaktideks? Meid on ju üks! Osutub, et nendele küsimustele ei olegi nii lihtne vastata. Erinevad inimesed ja organisatsioonid kehtestavad andmekaitse tagamiseks erinevad reeglid. Nii võivad organisatsioonid pakkuda töötajatele võimalust töötada oma seadmetega. Seda põhimõtet tähistatakse inglise keeles terminiga „bring your own device“ (BYOD) ehk maakeeli „tule tööle oma töövahendiga“. Näiteks pandeemia-aegse kaugtöö olukorras võiski see mudel olla paljudele enam-vähem normiks. Pea võrdväärne alternatiiv oma seadmete kasutamisele on kogu elu korraldamine töökoha antud seadmete kaudu. Miks peaks olema probleemiks laste e-kooli külastamine või õhtuks teatripiletite ostmine töökoha arvutist? Kasutaja peab hoidma erinevat kaitset vajavad andmed eraldi (kataloogid, suhtlusprogrammid jmt). Alustuseks võiksid otsida üles oma

organisatsioonis kehtivad dokumendid, mis räägivad töökoha seadmete ja andmete kasutamisest ja kaitsest. Kas sa teed nii, nagu töökoht on ette näinud?

Tehnoloogia võimaldab eraldada erinevate reeglite järgi toimuva andmekasutuse. Näiteks on võimalik andmekasutused eraldada füüsiliselt nii, et kindlas asukohas või ruumis on olemas ühendus ainult ühte liiki andmetega – tööl tööandmed ja kodus koduandmed. Võib eristada ka võrguühendused töö tegemiseks ja eraasjade ajamiseks. Nii on tervishoiuteenuse osutajal üldjuhul eraldi Wifi külastajatele ja tööarvutite ühendamiseks. Niisamuti on kodukontoris töötamiseks vaja luua turvaline võrguühendus töökoha arvutivõrguga (VPN). Vaja on leida lahendus, mis toetab kasutajate valmisolekut ja oskusi tehnoloogiat turvaliselt kasutada. Mõnikord tähendab see füüsilist, mõnikord sisulist eristamist. Kui me ise ei tea või ei oska oma töö- ja eraasju arvutis ja nutiseadmes eraldada, siis peame otsima abi kasutajatoelt või mõnelt IT-asjatundjalt. Infoturvet organisatsioonis ja eraelus toetab enda järjepidev koolitamine, sh sellise internetitehnoloogia tundmine nagu küpsised, krüptimine, inkognito veeb.

Tähtis on kogu aeg arvestada, kus, kelle seadmega, millises võrgus me tööd teeme. Kõik, mis me kord internetis oleme jaganud, jääb sinna alatiseks ning võib ilmuda välja täiesti suvalisel hetkel ja kahjustada nii meid endid, meiega seotud organisatsiooni, aga ka meie lähedasi.

13.8 Terviseandmete kaitse

Teadmised tervishoiuteenuse osutamise käigus tekkivate andmete turvalisest kogumisest, kasutamisest ja jagamisest ning oskus neid teadmisi oma töös rakendada on tervishoiutöötaja suurim panus oma organisatsiooni infoturbesse.

Terviseandmed on isiku füüsilise ja vaimse tervisega seotud isikuandmed, sealhulgas temale tervishoiuteenuste osutamist käsitlevad andmed, mis annavad teavet tema endise, praeguse või tulevase tervisliku seisundi kohta (Andmekaitse Inspektsioon, 2025b).

Terviseandmed on ka inimese enda kogutud andmed tema tervise ja haiguse olukorra kohta. Andmed koos kontekstiga moodustavad informatsiooni, mida tervishoiutöötajad kasutavad raviotsuste tegemisel ja inimeste suunamisel terviseteekonnal.

Terviseandmed jagunevad struktureeritud andmeteks (näiteks haigla või perearsti infosüsteemi konkreetsetesse lahtritesse sisestatavad andmed) ja tekstilisteks andmeteks – anamneesid, epikriisid, muud tööalased dokumendid, kirjavahetus, telefonivestlused.

Terviseandmete kaitse on tervishoiuvaldkonna ja iga tervishoiuteenuse osutaja **prioriteet** tervishoiuteenuse osutamisel.

Terviseandmeid on inimeste kohta kogunenud juba nii palju, et tervishoiutöötajad ei suuda neid kõiki raviotsuste tegemisel kasutada. Raviprotsessi on lülitunud otsustustoed, mis aitavad tervishoiutöötajatel raviotsuseid teha.

Järgnevalt on arutlus terviseandmetest ja tehisintellektist.

Jätkuv digitaliseerimine võimaldab terviseotsuste tegemisse kaasata järjest rohkem andmeid. Igal inimesel ja tervishoiutöötajal on kasutada üksikasjalik tervisesündmuste logi, andmed kõikvõimalike ravivõimaluste ja ravimite kohta, inimese geeniinfo, andmed perekonnas esinevate tervisemurede kohta ja palju muud. Selline andmete paljusus võimaldab otsida inimese tervisehädade algpõhjuseid ja seeläbi ravivõtteid veelgi täpsemini sihtida. Räägitakse meditsiini personaalsemaks ehk inimkeskseks

muutumisest. Inimese tervist mõjutavate andmete kättesaadavus paraneb, kuid nende läbitöötamine muutub aina masinlikumaks. Andmeid on lihtsalt inimlikuks uurimiseks liiga palju. Seetõttu jääb üha rohkem masina otsustada, kuhu peab suunama oma tähelepanu inimene ise või talle tervishoiuteenust osutav tervishoiutöötaja. Me ei näe enam kõiki andmeid, mille järgi me otsustame. Ja me kasutame otsustamisel väga väikest osa andmetest, mis võib lõppkokkuvõttes mõjutada ravi- ja terviseotsuseid.

Tehnoloogia eduka rakendamise tulemusena kujuneb infosüsteemis olevatest andmetest ja teadmistest justkui inimese digitaalne kaksik. See on „miski“, mis peegeldab inimese terviseseisundit, ennustab võimalikke riske ja annab vajalikul hetkel märku vajadusest sekkuda. Digikaksik on suurepärane abivahend – otsustustugi, mis üllatab meid täpselt õigete soovitustega, kui tal on kasutada piisavad ja kvaliteetsed terviseandmed. Et meie elu oleks veelgi lihtsam ja turvalisem, võimaldab tehnoloogia areng digikaksiku juhtimisel automatiseerida meie tervisega seotud toiminguid. Digikaksik võib tellida meie eest meile uusi ravimeid, kutsuda vajaduse korral kiirabi, broneerida terviseseisundist lähtuvalt arstiaegu jne. Digikaksik on nagu Eesti müütiline kratt, kes teeb täpselt seda, mida me temalt oskame tahta.

Nii nagu Eesti kratilood lõpevad enamasti mingi tagasilöögiga (kes täpsemalt ei tea, peab ise raamatust järele vaatama!), tuleb meil mõtestada ja juhtida ka tehnoloogilisi riske, mida kannavad endas meditsiinilised otsustustoed. Samal ajal tehnoloogia arendamisega tuleb meil uurida, milline on olnud senine digitaliseerimise mõju tervishoius ja kuidas kontrollida digiteadmiste õigsust. Euroopa meditsiiniseadmete õigusruum (EHDS), sellesse kaasatud standardid ja organisatsioonide võrk on üks krattide kasutamist reguleeriv meede. Küberturbe ja andmekaitse meetmed peavad aitama meil samuti ennetada võimalikke õnnetusi.

Pikemas vaates peame mõtlema ka sellele, kas ja kuidas inimene vajab privaatsust. Kratt või digikaksik on küll masin, mis ei plaani meid kuidagi ahistada. Kuid mis saab, kui kratil tekib probleeme andmekvaliteediga, näiteks osalise „mälukaotuse“ tõttu (puudulik andmete terviklus), milliseid soovitusi me temalt siis saama hakkame? Kas masinad võivad omavahel patsiendi kohta käivaid andmeid jagada? Kuidas saab patsient masinalt küsida teist arvamust oma tervise kohta? Kas digikaksiku saab välja ja hiljem jälle sisse lülitada? Tehisintellekt ja suuremahulised andmed inimeste tervise kohta on küll väga kasulikud, aga neid peab turvaliselt rakendama.

Infoturbe, sh andmete kaitse alustalad on konfidentsiaalsus, terviklus ja käideldavus. Need kolm omadust peavad olema tagatud nii paber- kui ka digikujul olevate andmete korral. Terviseandmed on Eestis ja paljudes teistes riikides tänapäeval valdavalt digitaalsed.

Digiandmete tervikluse tagamiseks on olulisim andmete varustamine **digitempliga** ehk digiallkirjastamine. Digitempel või digiallkiri põhineb krüptograafial, mis võimaldab luua erinevas kohas paiknevate andmete vahel seoseid, mida on keeruline võltsida või ära aimata.

Digiallkirjastamine aitab küll võimalikke andmerikkeid ära hoida, kuid digidokumendi kadumise korral tekib ikkagi tervikluse kadu. Teine probleem võib olla see, kui andmete kasutamisel ei kontrollita digiallkirja kehtivust.

Digiandmete käideldavuse tagamiseks on oluline

- regulaarne varukoopiate tegemine (varundamine);
- piisav tehniline tugi ja hooldus infosüsteemide töö tagamiseks;
- vajalikele infosüsteemidele juurdepääs arvutivõrgu kaudu.

Digiandmete salajasuse tagavad

- nende hoidmine turvalises kohas ja vastav asjaajamiskord;
- andmete edastamisel ja hoidmisel ebaturvalises kohas nende krüptimine, millele peab lisanduma võtmehaldus.

13.8.1 Digiandmete kaitsmine

Digitaalsetel andmetel on võrreldes muu infoga mõned eripärad, millega on vaja arvestada.

Kaudne väärtus. Andmevara väärtus võib olla suur, kuid seda ei saa hinnata lihtsa peale vaatamisega. Näiteks võib andmeid olla palju, aga võõrale kasutajale ei pruugi neil olla mingit väärtust. Samas võib olla üliväärtuslik mõni üksik infokilluke või pisike andmehulk – mõne inimese isikukood, diagnoos, amet, kodune aadress vmt.

Kergesti liigutatavad. Andmehoidla füüsiline suurus ei peegelda andmete tegelikku väärtust. Kui näiteks paberil infomaterjalide teisaldamiseks on vaja teha teatud jõupingutusi ja see võtab aega, siis digitaalsete andmete liigutamine toimub hetkega ja liigutada saab ülisuuri andmemassiive.

Asukohast sõltumatud. Andmete füüsiline asukoht ja nende kasutamise koht on järjest vähem omavahel seotud. Tänapäeval on täiesti tavaline, et andmed asuvad kuskil pilves ja me isegi ei tea, kus nad siis tegelikult asuvad. Aga me saame andmeid kasutada, kui meil on neile ligipääs ja meil on olemas arvuti/nutiseade, internet, elekter.

Märkamatu kahju. Digiandmete puhul on andmete kahjustamist või väärkasutust keeruline avastada. Kui sahvrist on mõni moosipurk puudu, siis seda on lihtne märgata, kuid kui andmetest on mingi osa puudu, siis seda on raske lihtsalt märgata.

Kuidas kaitstakse paberil olevaid andmeid?

- Käideldavuse tagavad dokumentide säilitamine hävimiskindlas kohas ja korrektne asjaajamiskord.
- Tervikluse tagavad dokumentide füüsiline vorm ja struktuur ning dokumendil olev allkiri, pitsat, kuupäev; samuti õige ligipääsu- ja asjaajamiskord.

Terviseandmete esmase ja teisese kasutamise puhul on oluline arvestada, millisel kujul võib andmeid kasutada. Esmase kasutamise puhul on tegemist isikustatud andmetega ehk andmetega, mis sisaldavad otseseid või kaudseid identifitseerivaid tunnuseid (kindel või kõrge riskiga tuvastamise võimalus).

Teisese kasutamise puhul sõltub juba kasutamise eesmärgist ja õiguslikust alusest, kas andmeid võib kasutada pseudonüümitud kujul, eemaldatud identiteediga andmetena või anonüümsete andmetena.

Pseudonüümitud andmed on andmed, kus identifitseerivad tunnused on asendatud kunstlike võtmetega ehk pseudonüümidega, mille vastavusi hoitakse ja valvatakse eraldi (tuvastamise risk sõltub vastavuste kaitsest).

Eemaldatud identiteediga andmed on andmed, millest otsesed ja kaudsed identifitseerivad tunnused on eemaldatud (tuvastamise jääkrisk).

Anonüümitud andmed. Eemaldatud identiteediga andmed, mida on töödeldud viisil, kus seost isikuga ei ole võimalik taastada (nt koondandmed) (tuvastamise risk puudub).

Kokkuvõte

See peatükk rääkis infoturbest, mille keskmes on informatsioon ehk teave. Need on tähendusega andmed, mis on tähenduse saamiseks töödeldud, korraldatud ja korrigeeritud. Teave ei võrdu andmed, sest teave on sisu, andmed on vorm. Andmed ja info on **väärtuslikud**, sest need aitavad teha paremaid otsuseid. Seetõttu ihaldavad andmeid ja infot ka kurjamid. **Terviseandmed on ühed tundlikumad**, kuna nende põhjal tehakse otsuseid inimese tervise kohta. Igasugused tõrked juurdepääsus ja vead terviseandmetes võivad kujutada ohtu inimeste tervisele. **Terviseandmete kaitse** on tervishoiuvaldkonna ja iga tervishoiuteenuse osutaja **prioriteet** tervishoiuteenuse pakkumisel. Seetõttu on oluline mõista infoturbe olemust ja sellesse panustada nii organisatsiooni kui ka üksikisiku tasandil.

Peatükk selgitas infoturbe olulisemaid mõisteid nagu turvalisus ja turve.

Turvalisus on olek, kindlustunne, mis loob aluse kestlikule arengule. **Turve** on tegevuste kogum turvalisuse tagamiseks. **Infoturvalisus, sh küberturvalisus** tähendab info kaitstust ohtude eest inimese turvateadlikkuse ja käitumisharjumuste (sh küberhügieeni) toel.

Kõik organisatsioonid kaitsevad oma äriprotsessidega seotud infot ja vara, et tagada organisatsiooni toimimine. Vara kaitsmiseks on vaja peale sisemiste ohtude tegeleda ka väliste ohtudega. **Infoturve** (ingl k *information security*) keskendub teabe ja sellest sõltuvate äriprotsesside kaitsmisele ning sellest tulenevalt infotöötluse ja infotehnoloogia kaitsmisele. Infoturbe osa on ka andmete kaitse ning selle sees omakorda on küberturve, mis tegeleb küberruumi, sh digiandmete kaitsmisega küberohtude eest. Üle nende kõigi toimib andmekaitse.

Infoturbe eesmärk on andmete käideldavuse, konfidentsiaalsuse ja tervikluse tagamine. Need kolm ongi infoturbe alustalad.

Terviseandmete kogumiseks, töötlemiseks ja jagamiseks kasutavad tervishoiutöötajad mitmesuguseid rakendusi, infosüsteeme, seadmeid, kuid vaja läheb ka ruume ja inimesi, et tervishoiuteenust pakkuda. Kõigil eelnimetatud varadel, mida tervishoiuteenuse osutaja peab kaitsma, on mingid nõrkused, mida võivad rünnata ohud. **Oht** on olukord, kus kedagi/midagi ähvardab **ebasoovitav sündmus** vara või meetme nõrkuse tõttu. Ohu realiseerumise tõenäosus on risk. Tervishoiuteenuse osutaja peab hindama **riske** ja võimalike negatiivsete tagajärgede tekkimise **tõenäosust**.

Organisatsioon loob küll infoturbe meetmestiku ja reeglistiku, kuid **iga üksiku inimese kohustus on nendest reeglitest kinni pidada**. Töötades mingis organisatsioonis, peavad infoturbe reeglid olema paigas ja töötajad koolitatud, kuid eraelus peab iga inimene suutma oma infovara ise kaitsta. Infoturbe ülesanne organisatsioonis on **säilitada** igapäeva töö käigus kasutatava **teabe turvalisus** ja seeläbi **organisatsiooni tõrgeteta toimimine**. Infoturve on pidev protsess, mitte ühekordne tegevus, ja algab juhtkonna pühendumusest.

Iga tegevus ja süsteem on turvaline esimese turvaintsidendini.

Kasutatud kirjandus

Andmekaitse Inspektsioon. (2025a). *Mõisted*. https://www.aki.ee/isikuandmed/kkk/moisted

Andmekaitse Inspektsioon. (2025b). *Tervishoid*. https://www.aki.ee/isikuandmed/kkk/tervishoid

CISCO. (2025). *What Is Information Security?* https://www.cisco.com/site/us/en/learn/topics/security/what-is-information-security-infosec.html?dtid=osscdc000283&linkclickid=srch

Cybernetica AS. (2025a). *AKIT. Andmekaitse*. https://akit.cyber.ee/term/681-data-protection-1

Cybernetica AS. (2025b). *AKIT. Andmete turve, andmete kaitse*. https://akit.cyber.ee/term/4169-data-security

Cybernetica AS. (2025c). *AKIT. Infovara*. https://akit.cyber.ee/

Cybernetica AS. (2025d). *AKIT. Küberruum*. https://akit.cyber.ee/term/568-cyberspace

Cybernetica AS. (2025e). *AKIT. Küberturve, küberturvalisus*. https://akit.cyber.ee/term/676-cybersecurity-1

Cybernetica AS. (2025f). *AKIT. Teabe turvalisus, infoturvalisus, infoturva-*. https://akit.cyber.ee/term/512-information-security-1

DigiriigiAkadeemia.ee. (2025). *Digiriigi Akadeemia õppeplatvorm*. https://digiriigiakadeemia.ee/

Eesti Standardimis- ja Akrediteerimiskeskus. (2024). *ISO/IEC 27001:2022/Amd 1:2024* . https://www.evs.ee/et/iso-iec-27001-2022-amd-1-2024

Euroopa Ülemkogu, & Euroopa Liidu Nõukogu. (2025). *Küberturvalisus: sotsiaalne manipulatsioon*. https://www.consilium.europa.eu/et/policies/cybersecurity-social-engineering/

Google. (2025). *Google Chrome Abi. Inkognito režiimis sirvimine*. https://support.google.com/chrome/answer/95464?hl=et&co=GENIE.Platform%3DDesktop

Küberturvalisuse Seadus. (2024). RT I, 21.06.2024, 15. https://www.riigiteataja.ee/akt/121062024015?

Politsei- ja Piirivalveamet. (2025). *Teata kuriteost*. https://cyber.politsei.ee/

Riigi Infosüsteemi Amet. (2018). *Küberturvalisuse infomaterjalid*. https://www.ria.ee/kuberturbe-nouanded/infomaterjalid-ja-kirjutised/kuberturvalisuse-infomaterjalid

Riigi Infosüsteemi Amet. (2022). *Nutitelefoni turvaline kasutamine*. https://www.ria.ee/kuberturbe-nouanded/nouanded-internetikasutajale/nutitelefon

Riigi Infosüsteemi Amet. (2024a). *AKIT. Autentimine*. https://akit.cyber.ee/term/14-authentication

Riigi Infosüsteemi Amet. (2024b). *AKIT. Biomeetrik*. https://akit.cyber.ee/term/12

Riigi Infosüsteemi Amet. (2024c). *Eesti infoturbestandard*. https://eits.ria.ee/et/abimaterjalid/seletav-soonaraamat

Riigi Infosüsteemi Amet. (2024d). *Eesti Infoturbestandard. CON.1: Krüptokontseptsioon*. https://eits.ria.ee/et/versioon/2024/eits-poohidokumendid/etalonturbe-kataloog/con-kontseptsioonid-ja-metoodikad/con1-krueptokontseptsioon/2-ohud

Riigi Infosüsteemi Amet. (2024e). *Eesti Infoturbestandard. CON.2: Isikuandmete kaitse*. https://eits.ria.ee/et/versioon/2024/eits-poohidokumendid/etalonturbe-kataloog/con-kontseptsioonid-ja-metoodikad/con2-isikuandmete-kaitse/2-ohud

Riigi Infosüsteemi Amet. (2024f). *Eesti Infoturbestandard. INF.8: Kodutöökoht*. https://eits.ria.ee/et/versioon/2024/eits-poohidokumendid/etalonturbe-kataloog/inf-taristu/inf8-kodutoeoekoht/3-meetmed/33-standardmeetmed/inf8m4-kodutoeoekoha-ooige-korraldus

Riigi Infosüsteemi Amet. (2024g). *Eesti Infoturbestandard. ISMS.1: Turbehaldus*. https://eits.ria.ee/et/versioon/2024/eits-poohidokumendid/etalonturbe-kataloog/isms-turbehaldus/isms1-turbehaldus/2-ohud

Riigi Infosüsteemi Amet. (2024h). *Eesti Infoturbestandard. OPS.2.2: Pilvteenuste kasutamine*. https://eits.ria.ee/et/versioon/2024/eits-poohidokumendid/etalonturbe-kataloog/ops-kaeidutoeoed/ops2-kaeidutoeoed-teenusena/ops22-pilvteenuste-kasutamine/2-ohud

Riigi Infosüsteemi Amet. (2024i). *Eesti Infoturbestandard. ORP.2: Personal*. https://eits.ria.ee/et/versioon/2024/eits-poohidokumendid/etalonturbe-kataloog/orp-organisatsioon-ja-personal/orp2-personal/2-ohud/21-personali-piisamatus

Riigi Infosüsteemi Amet. (2024j). *Eesti Infoturbestandard. SYS.3.3: Mobiiltelefon*. https://eits.ria.ee/et/versioon/2024/eits-poohidokumendid/etalonturbe-kataloog/sys-itsuesteemid/sys3-mobiilseadmed/sys33-mobiiltelefon/2-ohud

Riigi Infosüsteemi Amet. (2024k). *Eesti Infoturbestandardi põhidokumendid*. https://eits.ria.ee/

Riigi Infosüsteemi Amet. (2024l). *Küberturvalisuse aastaraamat 2024*. https://www.ria.ee/sites/default/files/documents/2024-02/RIAkuberturvalisuse-aastaraamat-2024.pdf

Riigi Infosüsteemi Amet. (2024m). *Küberturvalisuse ABC* . https://www.ria.ee/kuberturbe-nouanded/nouanded-internetikasutajale/kuberturvalisuse-abc

Riigi Infosüsteemi Amet. (2024n). *Pahavara, õngitsuslehed ja libaloosimised*. https://www.ria.ee/kuberturbe-nouanded/nouanded-internetikasutajale/pahavara-ongitsuslehed-ja-libaloosimised

Riigi Infosüsteemi Amet. (2025). *Teavita küberintsidendist*. https://www.ria.ee/kuberturvalisus/kuberintsidentide-kasitlemine-cert-ee/kuberintsidendist-teavitamine