Tervishoiutöötajate Küberturvalisuse Teadlikkuse Tõstmine Eestis: Strateegiline Analüüs ja Soovitused

1. Kokkuvõte

Käesolev aruanne käsitleb Eesti tervishoiusektori küberturvalisuse teadlikkuse tõstmise kriitilist vajadust. Tervishoiutöötajad on küberohtude vastases võitluses eesliinil, arvestades terviseandmete tundlikku olemust ja kasvavat sõltuvust digitaalsetest süsteemidest. Aruandes analüsitakse peamisi ohte, sealhulgas andmelekkeid, lunavararünnakuid ja õngitsuskirju, mis on Eesti tervishoiuasutusi juba märkimisväärselt kahjustanud.[1] Hinnatakse praegust teadlikkuse taset ja olemasolevaid riiklikke ning institutsionaalseid algatusi, tuues esile nii tugevused kui ka potentsiaalsed lüngad. Tuginedes rahvusvahelistele parimatele tavadele ja kohalikule kontekstile, esitatakse aruandes konkreetsed soovitused koolitusstrateegiate, metoodikate ja institutsionaalse pühendumise osas. Rõhutatakse, et küberturvalisuse teadlikkuse tõstmine ei ole ühekordne projekt, vaid pidev protsess, mis nõuab strateegilist lähenemist, piisavaid ressursse ja kõigi osapoolte, alates tippjuhtidest kuni iga üksiku töötajani, aktiivset kaasamist. Aruande eesmärk on pakkuda Eesti tervishoiuasutustele ja poliitikakujundajatele teaduspõhist alust küberturvalisuse kultuuri tugevdamiseks, patsientide andmete kaitsmiseks ja tervishoiusüsteemi tõrgeteta toimimise tagamiseks.

2. Küberturvalisuse Teadlikkuse Tõstmise Imperatiiv Eesti Tervishoius

Eesti tervishoiusektor seisab silmitsi ainulaadsete väljakutsetega küberturvalisuse tagamisel, mis tulenevad nii valdkonna spetsiifikast kui ka riigi kõrgest digitaliseerituse tasemest. Nende väljakutsetega toimetulekuks on tervishoiutöötajate küberturvalisuse teadlikkuse tõstmine möödapääsmatu.

Tervishoiusektori Ainulaadsed Haavatavused

Tervishoiusektor on küberkurjategijatele atraktiivne sihtmärk mitmel põhjusel. Esiteks, terviseandmed, eriti elektroonilised kaitstud terviseandmed (ePHI), on äärmiselt tundlikud ja neil on mustal turul kõrge väärtus, ületades sageli finantsandmete hinda.[4] Teiseks, kaasaegne meditsiin tugineb suurel määral omavahel ühendatud IT-süsteemidele ja meditsiiniseadmetele (IoMT – *Internet of Medical Things*), mis on hädavajalikud patsientide ravimisel ja diagnoosimisel.[4] Nende süsteemide keerukus ja omavaheline seotus loob aga laia rünnakupinna. Kolmandaks, tervishoiuteenuste ööpäevaringne olemus tähendab, et igasugune seisak, olgu see tingitud

turvauuendustest või küberintsidendi lahendamisest, on eriti häiriv ja võib omada otsest mõju patsientide heaolule.[4] Lisaks võivad mõnedes tervishoiuasutustes kasutusel olla vananenud süsteemid, mis on haavatavamad uutele ohtudele.[4] Kõige olulisem on aga see, et küberrünnakud tervishoius ei põhjusta mitte ainult finantsilist või mainekahju, vaid võivad otseselt ohustada patsientide turvalisust ja ravi kvaliteeti.[4]

Tervishoiutöötajate Kriitiline Roll Esimese Kaitseliinina

Tehnoloogilised kaitsemeetmed on küll olulised, kuid inimfaktor mängib küberturvalisuses sageli otsustavat rolli. Uuringud näitavad, et suur osa andmeleketest on tingitud inimlikust eksimusest.[8] Tervishoiutöötajad, alates arstidest ja õdedest kuni administratiivpersonalini, puutuvad igapäevaselt kokku tundlike andmete ja IT-süsteemidega. Nende teadlikkus küberohtudest ja turvalistest töövõtetest on seega kriitilise tähtsusega. Kontseptsioon "inimtulemüürist" rõhutab, et teadlik ja valvas töötaja on sama oluline kaitsemeede kui keerukad tarkvaralahendused.[11]

Eesti, olles tuntud oma eesrindliku digiühiskonna ("e-Eesti") ja arenenud e-tervise süsteemide poolest [5], seisab silmitsi omapärase olukorraga. Ühelt poolt on kõrge digitaliseerituse tase ja avalikkuse usaldus e-teenuste vastu suur tugevus. Teisalt võib see paradoksaalselt luua teatud määral enesega rahulolu või eelduse, et turvalisus on juba eos tagatud. Hiljutised suured andmelekked, nagu Apotheka ja Asper Biogene'i juhtumid [2], on aga valusalt demonstreerinud, et see usaldus võib kergesti kõikuma lüüa, kui küberturvalisuse aluspõhimõtteid, eriti töötajate teadlikkust, ei järgita rangelt igal tasandil. Riikliku infrastruktuuri keerukus ei taga automaatselt turvalisust igas üksikus asutuses või lõpp-punktis. Õiguskantsleri mureküsimused seoses andmehaldusega pärast Asper Biogene'i intsidenti viitavad süsteemsematele probleemidele, mis ulatuvad kaugemale pelgalt tehnilistest vigadest.[3] See rõhutab vajadust pideva valvsuse ja küberturvalisuse integreerimiseks igapäevatöösse, mitte lootma üksnes riigi kui terviku digitaalsele mainele.

Kuigi küberrünnakute finantsilised ja andmekaitsealased tagajärjed on kahtlemata tõsised, on tervishoiutöötajate jaoks sageli kõige mõjuvam argument patsientide ohutus. Otsene oht patsientide turvalisusele – näiteks katkestatud operatsioonid lunavararünnaku tõttu haiglasüsteemidele [1] või kompromiteeritud meditsiiniseadmete põhjustatud ravivigade risk [4] – on ainulaadselt võimas motivaator. Koolitusprogrammid, mis rõhutavad seda seost, suudavad tõenäoliselt tervishoiutöötajaid sügavamalt kõnetada kui abstraktsed andmekaitsekontseptsioonid. Küberrünnakute tagajärgede raamistamine otseste patsientide ohutust mõjutavate teguritena [4] seob küberturvalisuse praktikad nende põhiliste kutse-eetiliste väärtustega, muutes teadlikkuse tõstmise mitte lihtsalt kohustuseks, vaid osaks

kvaliteetse ja turvalise patsiendiravi tagamisest.

3. Küberturvalisuse Ohupilt Eesti Tervishoius

Eesti tervishoiusektor, sarnaselt teiste riikide meditsiiniasutustega, on küberkurjategijate jaoks ihaldusväärne sihtmärk. Sektor puutub kokku mitmesuguste ohtudega, millel võivad olla laastavad tagajärjed nii patsientidele, asutustele kui ka riigi tervishoiusüsteemile tervikuna.

Levinumad Ohud

- **Andmelekked:** Terviseandmete vargus on üks levinumaid ja kahjulikumaid rünnakuliike.
    - Eestis on toimunud mitmeid märkimisväärseid intsidente. Näiteks **Apotheka** juhtumi käigus lekkisid 700 000 inimese andmed.[2] Veelgi tõsisem oli **Asper Biogene'i** küberrünnak 2023. aasta lõpus, mille käigus varastati ligikaudu 10 000 inimese isiku- ja terviseandmed, sealhulgas geneetiliste analüüside tulemused. Seda on nimetatud seni suurimaks terviseandmete lekkeks Eestis.[2] Asper Biogene'i juhtum tõi esile ka küsimusi seoses andmete säilitamise ja vastutava ning volitatud töötleja rollidega.[17] Rahvusvaheline arestimiskäsk on välja antud Venemaa kodaniku suhtes, keda kahtlustatakse selle ründe toimepanemises.[19]
    - Andmelekete peamisteks põhjusteks on sageli ebapiisavad tehnilised ja organisatoorsed turvameetmed [2] ning haavatavused kolmandate osapoolte tarkvaras. Näiteks USA-s toimunud OneTouchPointi intsident, kus postitus- ja printimisteenuse pakkuja kompromiteerimine mõjutas enam kui 30 tervishoiuteenuse osutajat.[1]
    - Euroopa Liidu kontekstis on andmekaitseasutused määranud tervishoiuasutustele, apteekidele ja arstidele kokku 202 trahvi isikuandmete kaitsega seotud rikkumiste eest, peamiselt ebapiisavate turvameetmete tõttu.[2]
- **Lunavara (Ransomware):** See on kasvav oht, mis sihib erinevaid sektoreid, sealhulgas tervishoidu.[4]
    - Lunavara toimib kas failide krüpteerimise (krüpteerijad) või süsteemidele juurdepääsu blokeerimise (lukud) teel.[22] Andmed muudetakse kättesaamatuks ja nende vabastamiseks nõutakse lunaraha, sageli ähvardades andmete avalikustamisega.[23]
    - Lunavararünnakute tagajärjed on tervishoiuasutustele eriti rasked: teenuste katkestused, märkimisväärne finantskahju, pikk taastumisaeg ja potentsiaalne andmete hävimine.[1] Näiteks USA-s toimunud rünnak suurele haiglavõrgule mõjutas 500 000 patsienti ja viis elektrooniliste tervisekaartide (EHR)

süsteemid rivist välja.[13]
- **Õngitsuskirjad (Phishing) ja Sotsiaalne Manipulatsioon:** Need ründed põhinevad inimeste petmisel eesmärgiga saada kätte konfidentsiaalset informatsiooni (paroolid, krediitkaardiandmed) või paigaldada pahavara.[4]
    - Meetodid hõlmavad pahatahtlikke e-kirja manuseid, kloonitud veebilehti, hüpikaknaid ja kellegi teisena esinemist.[26]
    - Eesti kontekstis on teada Emotet pahavara levik usaldusväärsetena näivate e-kirjade kaudu, millega on nakatunud ka tervishoiusektor.[25] Samuti on Tervisekassa nime kasutatud õngitsuskampaaniates.[25]
    - Rahvusvaheliselt on haiglaid rünnatud õngitsuskirjadega, eriti COVID-19 pandeemia ajal, püüdes ära kasutada kõrgendatud stressi ja infovajadust.[18]
- **Rünnakud Kolmandate Osapoolte Teenusepakkujate Kaudu:** Tervishoiuasutused kasutavad sageli väliste teenusepakkujate tarkvara (nt raamatupidamistarkvara), mis võib osutuda ründevektoriks, kui teenusepakkuja süsteemid kompromiteeritakse.[1] OneTouchPointi juhtum on siin heaks näiteks.[1]

Ohtude Mõju

Küberohtude realiseerumisel võivad olla tervishoiusektorile laiaulatuslikud ja tõsised tagajärjed:

- **Patsientide ohutus ja ravi järjepidevus:** Rünnakud võivad häirida haiglate tavapärast töökorraldust, põhjustada operatsioonide edasilükkamist ja takistada juurdepääsu kriitilisele patsiendiinfole, seades otseselt ohtu patsientide tervise ja elu.[1]
- **Andmete terviklikkuse ja konfidentsiaalsuse kaotus:** Patsientide tundlikud terviseandmed võivad lekkida, neid võidakse muuta või hävitada.[1]
- **Finantskahjud:** Need võivad hõlmata lunaraha maksmist (kuigi seda üldiselt ei soovitata), süsteemide taastamise kulusid, saamata jäänud tulu teenuste katkestuste tõttu ja trahve andmekaitsenõuete rikkumise eest.[1] Tervishoiu andmelekke keskmine kulu oli 2024. aastal 9.77 miljonit dollarit.[4]
- **Maine kahjustumine ja avalikkuse usalduse kaotus:** Edukad küberrünnakud võivad tõsiselt kahjustada tervishoiuasutuse mainet ja õõnestada patsientide usaldust digitaalsete tervishoiuteenuste vastu.[3]
- **Operatiivsed häired:** Süsteemide rikked ja andmetele juurdepääsu takistamine võivad halvata asutuse igapäevatöö.[1]

Asjakohane Statistika ja Trendid Eestist ning Euroopa Liidust

Küberturvalisuse olukord on pingeline nii Eestis kui ka laiemalt Euroopas:

- Riigi Infosüsteemi Amet (RIA) on oma aastaraamatutes teatanud mõjuga

intsidentide arvu kahekordistumisest Eestis.[20]

- 2024. aastal tuvastati rekordarv turvanõrkusi.[20]
- Eelmisel aastal petsid kurjategijad Eesti inimestelt välja vähemalt 8.3 miljonit eurot.[21]
- Venemaa luureteenistuste kübersurve lääneriikidele, sealhulgas Eestile, on kasvav.[20]
- Euroopa Liidu Küberturvalisuse Ameti (ENISA) hinnangul on ELi tervishoiusektori küberturvalisuse küpsus mõõdukas ja liikmesriikide ning asutuste vahel esineb suuri erinevusi. Ligi pooled tervishoiuasutustest ei ole kunagi riskianalüüsi teinud.[29]

Eesti tervishoiusüsteemi, nagu paljude kaasaegsete süsteemide, toimimine sõltub omavahel ühendatud teenuste ja kolmandate osapoolte tarnijate võrgustikust. Näiteks haldab Tervise ja Heaolu Infosüsteemide Keskus (TEHIK) keskseid süsteeme [5] ja paljud asutused kasutavad väliste tarkvaraarendajate tooteid.[1] Kuigi selline ülesehitus võimaldab tõhusust ja andmete liikumist [30], loob see ka doominoefekti riski. Haavatavus ühes ökosüsteemi osas, näiteks tarkvaratarnija juures, nagu näitas OneTouchPointi juhtum [1], võib kaugeleulatuvaid tagajärgi omada mitmele tervishoiuteenuse osutajale. Seetõttu peab küberturvalisuse teadlikkus hõlmama ka tarneahela riskide mõistmist ja maandamist, ulatudes kaugemale vaid sisemistest praktikatest.

RIA nending "Veel üks rekordiaasta, mida polnud vaja" ja mõjuga intsidentide arvu kahekordistumine [20] viitavad sellele, et küberrünnakud on muutumas üha tavapärasemaks. Selline kõrge sagedus, kui seda korrektselt ei kontekstualiseerita, võib tervishoiutöötajate seas tekitada "häireväsimust" või paratamatuse tunnet, mis võib omakorda vähendada nende valvsust. Teadlikkusprogrammid peavad sellele vastu töötama, rõhutades, et kuigi ohud on püsivad, on ennetavatel meetmetel ja individuaalsetel tegevustel siiski oluline roll rünnakute ärahoidmisel või nende mõju leevendamisel.

Allolev tabel annab ülevaate peamistest küberturvalisuse ohtudest Eesti tervishoius:

Tabel 1: Peamised Küberturvalisuse Ohud Eesti Tervishoius

Ohu Tüüp	Kirjeldus	Spetsiifilised Eesti Näited/Kontekst	Potentsiaalne Mõju Tervishoiule (Patsiendi Ohutus,

			Andmed, Operatsioonid, Finants)
Andmelekked	Tundlike isiku- ja terviseandmete volitamata avalikustamine, muutmine või hävitamine.	Apotheka (700 000 inimese andmed) [2]; Asper Biogene (10 000 inimese geeni- ja terviseandmed).[2] Põhjuseks sageli ebapiisavad turvameetmed.[2]	Patsiendi privaatsuse rikkumine, identiteedivargus, usalduse kaotus, finantskahjud (trahvid, kohtukulud), operatiivsed häired uurimise ajal.
Lunavara (Ransomware)	Pahavara, mis krüpteerib andmed või lukustab süsteemid, nõudes nende vabastamiseks lunaraha.	Rünnakud koolidele, hambaravikeskustele [20]; üldine oht ettevõtetele.[21] Tervishoiusektor on eriti haavatav.[4]	Patsientide ravi katkestused, operatsioonide edasilükkamine, juurdepääsu kaotus kriitilistele andmetele, märkimisväärne finantskulu (lunaraha, taastamine), andmete püsiv kaotus.[1]
Õngitsuskirjad (Phishing) / Sotsiaalne Manipulatsioon	Kasutajate petmine konfidentsiaalse info (paroolid, finantsandmed) väljameelitamiseks või pahavara paigaldamiseks.	Emotet pahavara levik tervishoiusektoris [25]; Tervisekassa nime all saadetud õngitsuskirjad [25]; rünnakud haiglatele COVID-19 ajal.[18]	Volitamata juurdepääs süsteemidele ja andmetele, finantsvargused, pahavara levik organisatsioonis, süsteemide kompromiteerimine.
Kolmandate Osapoolte / Tarneahela Rünnakud	Rünnakud, mis toimuvad tervishoiuasutuse partnerite või teenusepakkujate (nt tarkvaraarendajad) kaudu.	Välise teenusepakkuja tarkvara (nt raamatupidamine) võib olla ründevektoriks.[1] OneTouchPointi juhtum USA-s.[1]	Sarnane otseste rünnakute mõjuga: andmelekked, teenusekatkestused, finantskahju, sõltuvalt kompromiteeritud teenuse ulatusest.

4. Küberturvalisuse Teadlikkuse ja Valmisoleku Praeguse Seisundi

Hindamine Eestis

Eesti tervishoiusektori küberturvalisuse teadlikkuse ja valmisoleku tase on mitmetahuline, peegeldades nii riigi üldist digitaalset arengut kui ka spetsiifilisi väljakutseid tervishoiuvaldkonnas.

Tuvastatud Lüngad Teadmistes ja Praktikas

Kuigi Eestis on tehtud märkimisväärseid jõupingutusi küberturvalisuse edendamiseks, viitavad mitmed asjaolud olemasolevatele lünkadele teadmistes ja praktikas. Edukad küberrünnakud, sealhulgas ulatuslikud andmelekked nagu Apotheka ja Asper Biogene [1], annavad tunnistust sellest, et teadlikkus või parimate tavade järgimine ei ole alati piisaval tasemel. ENISA aruanne, mis näitab, et ligi pooled Euroopa Liidu tervishoiuasutustest ei ole kunagi riskianalüüsi teinud [29], viitab fundamentaalsele lüngale, mis tõenäoliselt mõjutab ka Eesti asutusi ja nende teadlikkust spetsiifilistest haavatavustest. Korduv vajadus rõhutada küberhügieeni põhitõdesid [4] viitab sellele, et praegused praktikad võivad olla puudulikud. Samuti on probleemiks tarkvara uuendamisega viivitamine, mis jätab süsteemid haavatavaks [20] – see on käitumuslik probleem, mis on seotud riskide alahindamise või teadmatusest.

Ülevaade Olemasolevatest Riiklikest Strateegiatest ja Institutsionaalsetest Jõupingutustest

Eestis on mitmeid algatusi ja institutsioone, mis tegelevad küberturvalisuse, sealhulgas teadlikkuse tõstmisega:

- **E-tervise strateegia:** See dokument mainib küberturvalisust osana laiematest arengukavadest ning sisaldab tegevuskavasid ja sidusrühmadega suhtlemist.[14]
- **Riigi Infosüsteemi Amet (RIA):**
    - Avaldab iga-aastaseid küberturvalisuse aastaraamatuid, mis pakuvad ohuhinnanguid ja intsidentide statistikat.[20]
    - Korraldab teavituskampaaniaid ja ennetustegevusi erinevatele sihtrühmadele.[20]
    - Pakub tasuta küberturbealast õppeplatvormi Kübertest, millega liitus esimese aasta jooksul üle 15 000 inimese.[21]
    - Annab juhiseid ja võib pakkuda otsest nõustamist organisatsioonidele, näiteks koolidele [36], mida saaks laiendada ka tervishoiusektorile.
    - Tegeleb küberintsidentide käsitlemisega (CERT-EE) ja kriitilise infrastruktuuri küberkaitsega.[20]
    - On pakkunud küberturvalisuse taseme kaardistamise ja arendamise toetust, mis, kuigi hetkel suletud, näitab mehhanismi olemasolu parenduste rahastamiseks.[37]

- **Tervise ja Heaolu Infosüsteemide Keskus (TEHIK):**
  - Haldab kriitilisi terviseinfosüsteeme ja andmebaase 1.3 miljoni Eesti elaniku kohta.[5]
  - Arendab e-teenuseid tervise, sotsiaalkindlustuse ja töö valdkonnas ning on nende valdkondade e-teenuste kompetentsikeskus.[5]
  - Kuigi TEHIKu otsene roll küberturvalisuse koolituste pakkumisel või üksikasjalike avalike juhiste andmisel tervishoiuasutustele ei ole materjalides selgelt välja toodud [38], on tema keskne positsioon teeb temast olulise partneri parimate tavade levitamisel.
- **Health-ISAC (Health Information Sharing and Analysis Center):** Mainitud kui organisatsioon ohuteabe jagamiseks.[12] Eesti tervishoiuasutuste osalemine oleks kasulik.
- **Euroopa Liidu tasandi algatused:**
  - ENISA roll üleeuroopalise küberturvalisuse tugikeskuse loomisel haiglatele, pakkudes juhiseid, tööriistu, teenuseid ja koolitusi.[29]
  - ELi tegevuskava tervishoiu küberturvalisuse tugevdamiseks.[29]
  - NIS2 direktiiv, mis seab olulistele ja tähtsamatele teenuseosutajatele, sealhulgas tervishoius, kohustusi küberturvalisuse meetmete, sh koolituste osas.[41]

Kuigi ressursid nagu Kübertest [21] on olemas ja RIA viib läbi teavituskampaaniaid [20], viitab suhteliselt lihtsate rünnakute (nt õngitsuskirjad [25], uuendamata tarkvara ärakasutamine [20]) jätkuv edu nn "teadmise-tegemise lõhele". Tervishoiutöötajad võivad olla üldisel tasandil mõningatest ohtudest teadlikud, kuid ei pruugi seda teadmist oma igapäevatöös järjepidevalt ja korrektselt rakendada. Selle põhjuseks võib olla töökoormus, ebamugavus või oma isikliku rolli alahindamine. Seega ei piisa pelgalt teadmiste levitamisest; koolitus peab olema praktilisem ja käitumisele orienteeritud.

Samal ajal kui RIA-l on lai riiklik mandaat [20] ja TEHIK haldab keskseid tervise IT-süsteeme [5], tundub esmane vastutus töötajate küberturvalisuse teadlikkuse eest lasuvat üksikutel tervishoiuasutustel. See võib viia koolituste kvaliteedi ja järjepidevuse varieeruvuseni, sarnaselt koolide "kõikuva" tasemega küberturvalisuses.[20] Sarnane varieeruvus eksisteerib tõenäoliselt ka erinevate tervishoiuasutuste vahel (suured haiglad vs. väikesed kliinikud). Siin avaneb võimalus koordineeritumaks lähenemiseks. Võib-olla saaks TEHIK või spetsiaalne tervishoiu küberturvalisuse organ pakkuda standardiseeritud, kvaliteetseid ja Eesti tervishoiu konteksti jaoks kohandatud koolitusmooduleid ja ressursse, võttes eeskuju ENISA üleeuroopalistest püüdlustest.[29] See tagaks ühtlasema teadlikkuse baastaseme kogu sektoris.

5. Tõhusa Küberturvalisuse Teadlikkusprogrammi Alustalad Tervishoiutöötajatele

Tervishoiutöötajate küberturvalisuse teadlikkuse tõstmiseks on vaja terviklikku lähenemist, mis hõlmab nii spetsiifilisi teadmisi kui ka turvalisust väärtustava kultuuri kujundamist.

Põhilised Teadmiste Valdkonnad (Koolituse Sisu)

- **Õngitsus- ja Sihitud Õngitsusrünnakute Mõistmine ja Tuvastamine:**
  - Pahatahtlike e-kirjade, linkide ja manuste äratundmine.[4]
  - Taktikate mõistmine, nagu saatja identiteedi võltsimine, kiireloomulisuse rõhutamine ja kahtlased päringud.[26]
  - Saatja identiteedi kontrollimine enne tegutsemist.[7]
  - Kahtlastest e-kirjadest teavitamine.[7]
  - Teadlikkus tehisintellektil põhinevatest õngitsusrünnakutest ja süvavõltsingutest (*deepfakes*), mis muudavad pettused realistlikumaks.[7]
- **Lunavararünnakute Äratundmine ja Maandamine:**
  - Lunavara toimimispõhimõtted (krüpteerimine, lunarahanõuded).[4]
  - Lunaraha mittemaksmise olulisus (sageli ei garanteeri andmete tagastamist ja rahastab kuritegevust).
  - Varukoopiate roll taastamisel.[12]
  - Kuidas esmane nakatumine sageli toimub (õngitsuskirjad, uuendamata tarkvara).[20]
- **Tugeva Paroolihügieeni ja Mitmeastmelise Autentimise (MFA) Praktiseerimine:**
  - Tugevate, unikaalsete paroolide loomine erinevate kontode jaoks.[4]
  - Paroolihaldurite kasutamine.[31]
  - MFA olulisus ja rakendamine.[4]
  - Paroolide jagamise riskid.
- **Patsiendiandmete Turvaline Käsitlemine (Konfidentsiaalsus, Terviklikkus, Kättesaadavus) ja GDPR/Andmekaitse Nõuete Järgimine:**
  - Konfidentsiaalsuse, terviklikkuse ja kättesaadavuse põhimõtete mõistmine.[4]
  - Seadusest tulenev kohustus tagada andmete salastatus.[47]
  - GDPR-i nõuded, mis on asjakohased igapäevatöös.[2]
  - Andmete turvaline säilitamine, edastamine (TLS/SSL, VPN) ja hävitamine.[7]
  - Ekraanide ja kontode lukustamine töökohalt lahkudes.[7]
  - Patsiendiandmete arutamise vältimine avalikes kohtades.[7]
- **Meditsiiniseadmete ja Meditsiiniseadmete Interneti (IoMT) Turvaline Kasutamine:**

    - Teadlikkus IoMT seadmete haavatavustest (vananenud tarkvara, krüpteerimise puudumine, nõrk autentimine).[4]
    - Vajadusel tarkvara paikamise ja uuenduste olulisus.[4]
    - Meditsiiniseadmete turvaline võrgukonfiguratsioon (segmenteerimine).[12]
    - Kahtlasest seadmekäitumisest teavitamine.[4]
- **Sotsiaalse Manipulatsiooni Taktikate Tuvastamine ja Nendele Reageerimine:**
    - Erinevate manipulatsioonitehnikate mõistmine (mõjutamine, veenmine, petmine).[4]
    - Ründajate infokogumiskatsete äratundmine.[26]
    - Ettevaatlikkus soovimatu abi või ebatavaliste palvete suhtes.[26]
    - Rünnakute "inimlik element" – usalduse ja abivalmiduse ärakasutamine.[26]
- **Turvalised Kaugtöö Praktikad:**
    - VPN-ide turvaline kasutamine.[7]
    - Koduste Wi-Fi võrkude turvamine.
    - Avaliku Wi-Fi vältimine tundlike ülesannete täitmisel.[7]
    - Isiklike või haigla poolt antud seadmete turvalisus kaugtööl.[7]
    - Turvalisus telemeditsiini konsultatsioonide ajal.[7]
- **Intsidentidele Reageerimise Alused Lõppkasutajatele:**
    - Teadmine, kellega ühendust võtta ja millist infot anda kahtlustatava intsidendi korral.[7]
    - Kohese teavitamise olulisus laiema kahju vältimiseks.[25]

Turvateadliku Kultuuri Arendamine

Efektiivne küberturvalisus ulatub kaugemale tehnilistest meetmetest ja regulatiivsest vastavusest; see nõuab turvalisust väärtustava kultuuri loomist.[10] See tähendab, et iga töötaja mõistab oma rolli ja vastutust organisatsiooni küberturvalisuse tagamisel. Juhtkonna eeskuju ja pühendumus on siin võtmetähtsusega.[53] Oluline on julgustada intsidentidest ja peaaegu-intsidentidest avatult teavitama, ilma hukkamõistu kartmata. Küberturvalisus peaks olema pidev dialoog, mitte ühekordne koolitusüritus.[13]

Meditsiiniseadmete internet (IoMT) ei ole enam nišitehnoloogia IT-osakondadele, vaid igapäevane töövahend paljudele kliinilistele töötajatele. Samas jääb teadlikkus nende seadmete spetsiifilistest haavatavustest [6] sageli maha. Standardne küberturvalisuse koolitus võib katta e-posti õngitsust, kuid mitte uuendamata infusioonipumba või kompromiteeritud patsiendimonitori riske. On kriitilise tähtsusega integreerida IoMT turvalisuse teadlikkus kõigi asjassepuutuvate tervishoiutöötajate põhikoolituskavva, mitte ainult IT-personali jaoks. Rõhutada tuleb, kuidas nende seadmete haavatavused võivad otseselt mõjutada patsientide ravi, näiteks kantavatelt seadmetelt andmete

pealtkuulamise [6] või püsivara ärakasutamise [6] kaudu.

Paljud koolitusprogrammid keskenduvad olemasolevate, teadaolevate ohtude äratundmisele (nt konkreetset tüüpi õngitsuskiri). Ohumaastik areneb aga kiiresti.[20] Tõhus teadlikkus peaks kasvatama ka ennetava ohu tuvastamise mõtteviisi – õpetama töötajaid ära tundma anomaalset käitumist või kahtlasi mustreid, *isegi kui need ei vasta tuntud rünnakusignatuurile*. See hõlmab kriitilist mõtlemist ja rünnakute *põhimõtete* mõistmist, mitte ainult näidete meeldejätmist. Selline lähenemine soodustab vastupidavamat kaitset, mis suudab kohaneda tekkivate, ettenägematute ohtudega, mitte ainult reageerida vanadele.

Allolev tabel esitab tervishoiutöötajate küberturvalisuse koolituse põhiteemad:

Tabel 2: Tervishoiutöötajate Küberturvalisuse Koolituse Põhiteemad

Teemavaldkond	Peamised Õpieesmärgid	Spetsiifiline Olulisus/Näited Tervishoiurollidele
Õngitsuskirjad ja Sotsiaalne Manipulatsioon	Oskus tuvastada ja vältida õngitsuskirju, kahtlasi linke/manuseid. Sotsiaalse manipulatsiooni taktikate äratundmine. Teavitamisprotseduurid.	**Kliinikud:** Patsiendiandmeid või juurdepääsu nõudvad petukirjad. **Administraatorid:** Arvete või finantsinfoga seotud pettused. **IT-tugi:** Kasutajate abistamine kahtlaste kirjade tuvastamisel.
Lunavara	Lunavara toimimispõhimõtete mõistmine. Nakatumisviiside (nt õngitsus, uuendamata tarkvara) teadmine. Varukoopiate olulisus. Lunaraha mittemaksmise põhjendused.	**Kõik rollid:** Mõistmine, kuidas lunavara võib halvata kogu haigla töö ja ohustada patsientide ravi.
Andmekäitlus ja GDPR	Konfidentsiaalsuse, terviklikkuse, kättesaadavuse põhimõtted. GDPR-i nõuded. Patsiendiandmete turvaline säilitamine, edastamine, hävitamine. Andmete salastatuse kohustus.	**Kliinikud:** Patsiendiandmete korrektne dokumenteerimine ja jagamine. **Administraatorid:** Juurdepääsuõiguste haldamine, andmekaitse dokumentatsioon.
IoMT Turvalisus	Meditsiiniseadmete	**Kliinikud:** Igapäevaselt

	haavatavuste teadvustamine. Turvalise kasutamise praktikad (nt vaikeparoolide muutmine, kui võimalik). Kahtlase seadmekäitumise raporteerimine.	kasutatavate seadmete (monitorid, pumbad) riskide mõistmine. **Tehnikud/IT:** Seadmete turvaline konfigureerimine ja hooldus.
Paroolid ja Autentimine	Tugevate, unikaalsete paroolide loomise ja haldamise oskus. Mitmeastmelise autentimise (MFA) vajalikkuse ja kasutamise mõistmine.	**Kõik rollid:** Turvaline sisselogimine kõikidesse tööalastesse süsteemidesse ja andmebaasidesse.
Intsidentidest Teavitamine	Teadmine, kuidas ja kellele teatada turvaintsidendist või selle kahtlusest. Kiire reageerimise olulisus.	**Kõik rollid:** Võimaldades IT-osakonnal või turvameeskonnal kiiresti reageerida, et piirata kahju.

6. Strateegilised Lähenemisviisid Küberturvalisuse Koolitusele ja Teadlikkusele

Efektiivse küberturvalisuse teadlikkuse saavutamiseks tervishoiusektoris on vaja strateegilist ja mitmekülgset lähenemist koolitusele, mis arvestab nii valdkonna eripärasid kui ka kaasaegseid õppemeetodeid.

Kohandatud Koolitussisu

Koolituse sisu peab olema asjakohane ja sihipärane. See tähendab rollipõhiste koolitusmoodulite arendamist.[4] Kliinilistel töötajatel, administratiivpersonalil, IT-spetsialistidel ja juhtkonnal on erinev kokkupuude andmete ja süsteemidega ning seega ka erinevad riskiprofiilid ja õpivajadused. Tervishoiuspetsiifiliste stsenaariumide ja näidete kasutamine suurendab koolituse asjakohasust ja kaasatust.[4]

Kaasavad Koolitusmetoodikad

Traditsioonilistest loengutest sageli ei piisa püsiva teadlikkuse ja käitumismuutuste saavutamiseks. Seetõttu tuleks rakendada kaasavamaid meetodeid:

- **Interaktiivsed E-õppe Moodulid:** Staatiliste esitluste asemel tuleks kasutada mooduleid, mis sisaldavad viktoriine, hargnevaid stsenaariume ja interaktiivseid elemente.[11]
- **Mängustamine (Gamification) ja Tõsimängud:** Mängumehaanika (punktid,

märgid, edetabelid, väljakutsed) kasutamine motivatsiooni, kaasatuse ja teadmiste kinnistumise suurendamiseks.[9] Näideteks on õngitsussimulatsioonimängud ja küberturvalisuse põgenemistoad.[57] Mängustamise kasudeks on tugevam turvakultuur, reaalsete olukordade harjutamine ja mõõdetav tulemuslikkus.[57]
- **Realistlikud Õngitsussimulatsioonid ja Intsidentidele Reageerimise Õppused:** Töötajate regulaarne testimine simuleeritud õngitsuskirjadega aitab hinnata teadlikkust ja kinnistada õpitut.[4] Samuti on oluline läbi viia intsidentidele reageerimise lauaharjutusi või õppusi.[12] ENISA toetab riiklikke küberturvalisuse õppusi.[29]
- **Töötoad ja Kolleegidelt Õppimine (Peer-to-Peer Learning):** Arutelude ja teadmiste jagamise soodustamine töötajate vahel.[54] See võib hõlmata kogemuste jagamist tegelike või simuleeritud intsidentidega (süüdistamiseta keskkonnas).
- **Mikroõpe:** Informatsiooni edastamine väikeste, kergesti seeditavate osadena, et sobituda kiire töögraafikuga.

Pidev Kinnistamine

Küberturvalisuse teadlikkus ei ole ühekordne sündmus, vaid nõuab pidevat pingutust.[13] See hõlmab regulaarseid uuendusi, uudiskirju, plakateid ja lühikesi meeldetuletusi.[51] Küberturvalisuse näpunäiteid saab integreerida ka regulaarsetesse töökoosolekutesse.

Rahvusvaheliste Parimate Tavade ja Ressursside Kasutamine

Oluline on tugineda olemasolevatele rahvusvahelistele standarditele ja ressurssidele:

- **NIST Küberturvalisuse Raamistik:** Selle funktsioonide (Tuvasta, Kaitse, Avasta, Reageeri, Taasta, Halda) kasutuselevõtt teadlikkuse ja laiema küberturvalisuse töö struktureerimiseks.[53] NIST SP 800-66 on spetsiifiliselt HIPAA turvareegli jaoks.[68]
- **ENISA Juhised ja Tugi:** Euroopa Liidu Küberturvalisuse Ameti ressursside, sealhulgas kavandatava üleeuroopalise haiglate küberturvalisuse tugikeskuse kasutamine.[29] ENISA terviseohu maastiku aruanne on samuti väärtuslik allikas.[41]
- **Tasuta Koolitusmaterjalid:** Ressursside, nagu HSCC "Cybersecurity for the Clinician" videoseeria [69] või CISA tasuta koolituste [58] kasutamine.

Paljud küberturvalisuse koolitused keskenduvad hirmule, ebakindlusele ja kahtlustele (FUD – *Fear, Uncertainty, and Doubt*), rõhutades negatiivseid tagajärgi. Kuigi riskide mõistmine on oluline, võib FUD-i liigne rõhutamine olla kahjulik, põhjustades ärevust või passiivsust. Tõhusam lähenemine hõlmab "positiivset turvalisust", mis annab töötajatele jõudu, näidates, kuidas nende tegevus *aitab kaasa* ohutusele ja vastupidavusele, ning tunnustades häid turvatavasid, mitte ainult karistades vigu. See tasakaal riskiteadlikkuse ja ennetavate, positiivsete sammude vahel, mida töötajad

saavad astuda [44], võib olla motiveerivam. Mängustamine sisaldab sageli positiivseid preemiaid [57], mis toetab seda lähenemist.

Selle asemel, et tugineda üksnes kesksele IT-osakonnale või välistele koolitajatele, võiksid tervishoiuasutused tuvastada ja koolitada "küberturvalisuse eestvedajaid" erinevates osakondades. Need kolleegid saaksid pakkuda lokaliseeritud, kontekstispetsiifilist nõu, kinnistada koolitussõnumeid igapäevastes töövoogudes ja olla kättesaadavamaks esmaseks kontaktisikuks turvaküsimustes. Selline lähenemine kasutab ära olemasolevat sotsiaalset dünaamikat ja usaldust. Kolleegidevaheline õpe on näidanud oma väärtust ka teistes koolituskontekstides.[54]

Allolev tabel võrdleb erinevaid küberturvalisuse teadlikkuse koolitusmetoodikaid:

Tabel 3: Küberturvalisuse Teadlikkuse Koolitusmetoodikate Võrdlus

Metoodika	Kirjeldus	Eelised	Puudused	Sobivus/Näited Tervishoius
Interaktiivne E-õpe	Veebipõhised moodulid, mis sisaldavad multimeediat, viktoriine, stsenaariume.	Paindlik ajakasutus, skaleeritav, järjepidev sisu, jälgitav progress.	Võib nõuda esialgset investeeringut sisu loomisse/hankimisse, võib olla vähem kaasahaarav kui otsene interaktsioon.	Sobib põhikoolituseks, GDPR-i, andmekaitse teemadeks. Ressursid nagu Kübertest.[21]
Mängustamine (Gamification)	Mänguelementide (punktid, tasemed, auhinnad) kasutamine õppeprotsessis.	Kõrge kaasatus, parem teadmiste kinnistumine, positiivne õpikogemus, käitumuslik muutus.	Nõuab läbimõeldud disaini, võib olla kulukas arendada, ei pruugi sobida kõigile õppijatele.	Õngitsussimulatsioonimängud, turvalisuse "põgenemistoad", teadlikkuse tõstmise väljakutsed.[57]
Õngitsussimulatsioonid	Regulaarselt saadetavad võlts-õngitsuskirjad töötajate	Praktiline, mõõdetav, aitab tuvastada haavatavaid	Võib tekitada frustratsiooni, kui seda halvasti hallata, nõuab	Oluline osa igas tervishoiuasutuse programmis, et testida

	testimiseks ja õpetamiseks.	töötajaid, realistlik.	pidevat haldamist.	reaktsiooni petukirjadele.[4]
Töötoad / Kolleegidelt Õppimine	Interaktiivsed sessioonid, arutelud, rühmatööd, kogemuste jagamine.	Soodustab arutelu, praktiliste oskuste arendamist, meeskonnatööd, kontekstipõhist õpet.	Ajanõudlik, raskem skaleerida, sõltub moderaatori oskustest.	Intsidentide analüüs (anonüümselt), parimate praktikate jagamine osakondades.[54]
Mikroõpe	Lühikesed, keskendunud õppetükid (nt 5-10 min videod, lühikesed artiklid).	Sobib kiire graafikuga töötajatele, kergesti omastatav, hea teadmiste värskendamiseks.	Ei pruugi sobida keerukate teemade süvitsi õppimiseks, vajab head struktureerimist.	Kiired meeldetuletused paroolihügieenist, uutest ohtudest teavitamine kliinilisele personalile.
Traditsioonilised Loengud	Informatsiooni edastamine esitluse vormis.	Lihtne organiseerida suurele grupile, madalad tehnilised nõuded.	Sageli passiivne, madal kaasatus, teadmiste halb kinnistumine.	Võib olla osa sissejuhatavast koolitusest, kuid peaks olema kombineeritud interaktiivsemate meetoditega.

7. Väljakutsete Ületamine Teadlikkusprogrammide Rakendamisel

Küberturvalisuse teadlikkusprogrammide edukas rakendamine tervishoiusektoris nõuab mitmete väljakutsete teadvustamist ja nendele strateegiliste lahenduste leidmist.

Ajaliste Piirangute ja Ressursside Nappuse Lahendamine

Tervishoiutöötajate töögraafikud on sageli pingelised, jättes vähe aega täiendkoolitusteks. Ressursinappus, nii rahaline kui ka personalialane, on samuti levinud probleem.[73]

- **Strateegiad:** Lahenduseks võivad olla mikroõppe moodulid, mis edastavad infot lühikeste, kontsentreeritud osadena.[57] Koolitusi saab integreerida olemasolevatesse koosolekutesse või pakkuda paindlike veebikursustena, mida

saab läbida endale sobival ajal.[72] Mängustatud lühiseansid võivad samuti olla tõhusad.
- **Ressursid:** Oluline on ära kasutada tasuta või madala kuluga ressursse, mida pakuvad näiteks RIA (Kübertest), HSCC ("Cybersecurity for the Clinician") [69] ja CISA.[58]
- **Välzeressursid:** Kaaluda võib koolituste või hallatud turvateenuste sisseostmist, kui asutusesisene ekspertiis puudub.[66]
- **ROI:** Investeeringu õigustamiseks on oluline keskenduda koolituse tasuvusanalüüsile (ROI), näidates, kuidas see aitab vähendada andmeleketega seotud kulusid.[55]

Juhtkonna Nõusoleku ja Toe Tagamine

Juhtkonna toetus on iga eduka teadlikkusprogrammi aluseks.

- **Kommunikatsioon:** Juhtkonnale tuleb selgelt kommunikeerida küberintsidentide riske ja potentsiaalset mõju patsientide ohutusele, finantsidele ja mainele.[53]
- **Kohustused:** Rõhutada tuleb seadusest tulenevaid ja regulatiivseid kohustusi (NIS2, GDPR).[2]
- **Investeering, mitte kulu:** Teadlikkuskoolitust tuleb esitleda investeeringuna, millel on tõestatav tasuvus, mitte kuluna.[55]
- **Eeskuju:** Juhtkond peab olema kaasatud küberturvalisuse kultuuri edendamisse ja olema ise eeskujuks.[53]

Koolitusprogrammide Tõhususe Mõõtmine

Ilma mõõtmiseta on raske hinnata programmi edukust ja teha vajalikke parandusi.

- **Mõõdikud:** Jälgida tuleks selliseid näitajaid nagu õngitsussimulatsioonide klikkimise määrad, viktoriinide tulemused, intsidentidest teavitamise sagedus ja teatud tüüpi turvaintsidentide vähenemine.[8]
- **Hindamine:** Läbi viia koolitusjärgseid hindamisi ja küsitlusi.
- **Uuendamine:** Programmi tuleb regulaarselt üle vaadata ja uuendada, tuginedes mõõdikutele ja arenevale ohupildile.[53] Kirkpatricku mudel või sarnased raamistikud võivad olla abiks koolituse tulemuslikkuse hindamisel.[8]

Vastuseisu Muutustele või Rahuloluga Tegelemine

Uute praktikate juurutamine võib kohata vastuseisu või ükskõiksust.

- **Kaasamine:** Koolitus tuleb muuta kaasahaaravaks ja asjakohaseks, kasutades tervishoiuspetsiifilisi näiteid.[7]
- **Isiklik vastutus:** Rõhutada tuleb isiklikku mõju ja vastutust, näidates, kuidas iga

töötaja tegevus loeb.[67]
- **Näited:** Kasutada reaalseid näiteid ja edulugusid ennetustööst.

Koolitussisu Ajakohasena Hoidmine Arenevate Ohtudega

Küberohud muutuvad pidevalt, seega peab ka koolitussisu olema dünaamiline.

- **Ohuteave:** Tellida ohuteabe vooge (nt Health-ISAC).[12]
- **Regulaarne ülevaatus:** Koolitusmaterjale tuleb regulaarselt üle vaadata ja värskendada.[7]
- **Partnerlus:** Kaasata uuenduste tegemisse küberturvalisuse ettevõtteid või eksperte.

Tervishoius, kus eelarved on sageli piiratud ja kliinilised prioriteedid domineerivad, võib olla keeruline õigustada kulutusi "pehmetele" valdkondadele nagu teadlikkuskoolitus. Selge tasuvusanalüüsi (ROI) demonstreerimine – sidudes koolituse vähenenud intsidentide kuludega, välditud trahvidega ja paranenud operatiivse tõhususega [55] – on kriitilise tähtsusega vajalike ressursside ja juhtkonna pühendumuse tagamiseks. See muudab koolituse tajumist kuluallikast väärtust lisavaks kaitsemeetmeks.

Tõhus küberturvalisuse teadlikkus on enamat kui perioodiline koolitus; see seisneb vastupidava küberturvalisuse kultuuri kinnistamises.[10] See on märkimisväärne väljakutse, sest nõuab sisseharjunud käitumisviiside muutmist ja turvalisuse muutmist igaühe töö intuitiivseks osaks. See hõlmab pidevat kinnistamist, juhtkonna poolt õigete käitumisviiside modelleerimist ja turvakaalutluste integreerimist kõikidesse protsessidesse, mitte käsitledes seda isoleeritud IT-probleemina.

8. Peamised Soovitused Eesti Tervishoiuasutustele

Eesti tervishoiuasutuste küberturvalisuse teadlikkuse ja vastupanuvõime tõstmiseks on vajalikud sihipärased ja järjepidevad sammud. Järgnevalt on esitatud peamised soovitused, mis tuginevad käesoleva aruande analüüsile.

- **Arendada ja Rakendada Terviklikke, Pidevaid Küberturvalisuse Teadlikkusprogramme:**
    - Muuta regulaarne küberturvalisuse koolitus kohustuslikuks kõigile töötajatele, sealhulgas kliinilisele personalile, administratiivtöötajatele ja juhtkonnale.
    - Kohandada koolituse sisu vastavalt spetsiifilistele rollidele ja riskidele tervishoiukeskkonnas.
    - Kasutada kombineeritud õppemeetodeid, mis ühendavad interaktiivset e-õpet, mängustamist, simulatsioone ja töötubasid.
    - Tagada, et programmid kataksid kõik 5. peatükis tuvastatud põhiteadmiste

valdkonnad.

- **Investeerida Sobivatesse Koolitusressurssidesse ja Platvormidesse:**
  - Eraldada eelarve professionaalsete koolitusmaterjalide, simulatsioonivahendite või ekspertkoolitajate jaoks.
  - Uurida ja kasutada olemasolevaid tasuta ressursse, mida pakuvad riiklikud (nt RIA Kübertest [21]) ja rahvusvahelised (nt HSCC [69], CISA [72]) organid.
  - Kaaluda partnerlust spetsialiseerunud küberturvalisuse koolituspakkujatega, kui asutusesisene ekspertiis on piiratud.[78]
- **Edendada Tugevat Küberturvalisuse Kultuuri Tippjuhtkonnast Alates:**
  - Juhtkond peab nähtavalt toetama küberturvalisuse algatusi ja eraldama vajalikud ressursid.[53]
  - Edendada süüdistamiseta keskkonda intsidentidest või peaaegu-intsidentidest teavitamiseks, et julgustada läbipaistvust.
  - Integreerida küberturvalisus töötajate sisseelamisprogrammidesse ja regulaarsetesse tulemusvestlustesse.
- **Regulaarselt Hinnata ja Uuendada Teadlikkusalgatusi:**
  - Pidevalt jälgida koolituse tõhusust mõõdikute abil, nagu õngitsustestide tulemused ja teatatud intsidentide arv.[53]
  - Uuendada koolitussisu sageli, et see kajastaks uusimaid ohte, haavatavusi ja institutsionaalseid kogemusi.[7]
  - Viia läbi perioodilisi küberturvalisuse riskihindamisi, mis teavitavad teadlikkusprogrammi prioriteete.[4]
- **Teha Koostööd Riiklike ja Rahvusvaheliste Organitega:**
  - Aktiivselt suhelda RIA-ga juhiste, ressursside ja riiklikes küberturvalisuse algatustes osalemise osas.[20]
  - Teha koostööd TEHIKuga, et mõista ja maandada kesksete terviseinfosüsteemidega seotud riske ning uurida võimalusi sektoripõhiste teadlikkusressursside loomiseks.[5]
  - Kaaluda liitumist või ressursside kasutamist Health-ISACilt ohuteabe jagamiseks.[12]
  - Järgida ELi direktiive (nt NIS2 [43]) ja kasutada ENISA tuge.[29]
- **Spetsiifilised Meetmed IoMT Turvalisuse Osas:**
  - Arendada spetsiifilisi koolitusmooduleid meditsiiniseadmete turvalise kasutamise ja haldamise kohta kliinilisele personalile.
  - Rakendada tugevaid IoMT turvapraktikaid, sealhulgas seadmete inventuuri, tarkvara paikamist ja võrgu segmenteerimist, ning tagada, et personal oleks nendest meetmetest teadlik.[4]

Soovitustes tuleks rõhutada tagasisideahela loomist, kus tegelikest intsidentidest (nii

sisemistest kui ka avalikult teatatud Eesti juhtumitest nagu Asper Biogene [2]) saadud õppetunnid anonüümitakse ja integreeritakse koolitusstsenaariumidesse. See muudab koolituse väga asjakohaseks ja demonstreerib teadlikkuse põhimõtete reaalset rakendatavust. See eeldab protsessi, kus intsidentide järelanalüüsid annavad sisendit õppekavade arendusse, tagades, et koolitus areneb koos tegeliku ohumaastikuga, millega asutus silmitsi seisab.[56]

9. Järeldused

Küberturvalisuse teadlikkuse ennetav ja pidev tõstmine kõigi Eesti tervishoiutöötajate seas on kriitilise tähtsusega. See ei ole pelgalt IT-osakonna ülesanne, vaid kogu organisatsiooni hõlmav strateegiline prioriteet. Tugevam teadlikkus on otseselt seotud küberintsidentide arvu vähenemisega, patsientide ohutuse paranemisega ja Eesti tervishoiusüsteemi üldise vastupanuvõime suurenemisega digitaalajastu ohtudele.

Käesolev aruanne kutsub tervishoiuasutusi, poliitikakujundajaid ja iga üksikut tervishoiutöötajat üles seadma esikohale küberturvalisuse teadlikkuse ja investeerima sellesse valdkonda. Küberturvalisus ei ole enam eraldiseisev tehniline küsimus, vaid kvaliteetse tervishoiuteenuse lahutamatu osa.

Eesti tervishoiusüsteem tugineb suuresti digitaaltehnoloogiatele ja e-tervise lahendustele.[5] Avalikkuse usaldus on sellise süsteemi eduka toimimise alustala. Andmelekked ja küberrünnakud, nagu hiljutised kõrgetasemelised juhtumid [2], ei põhjusta mitte ainult otsest kahju, vaid õõnestavad ka usaldust, mis on vajalik patsientide ja spetsialistide jaoks digitaalsete tervishoiulahenduste täielikuks omaksvõtmiseks. Seetõttu ei ole küberturvalisuse teadlikkusesse investeerimine mitte ainult tehniline või vastavusküsimus, vaid strateegiline imperatiiv e-Eesti tervishoiumudeli pikaajalise elujõulisuse ja aktsepteerimise tagamiseks. Tugev küberturvalisuse kultuur, mille keskmes on teadlikud töötajad, on digitaalse tervise usalduse üks olulisemaid tugisambaid.

Viidatud allikad

1. TERVISHOIUSEKTORI KÜBERRISKIANALÜÜS - RIA, juurdepääs juuni 12, 2025, https://www.ria.ee/sites/default/files/documents/2024-03/tervishoiusektori-eelanaluus.pdf
2. Andmelekked tervishoius – lühiülevaade trahvidest. | GDPR24.ee, juurdepääs juuni 12, 2025, https://gdpr24.ee/andmelekked-tervishoius-luhiulevaade-trahvidest/
3. Õiguskantsleri aastaülevaade 2023/2024, juurdepääs juuni 12, 2025, https://www.oiguskantsler.ee/ylevaade2024/e-eesti
4. A Comprehensive Guide to Healthcare Cybersecurity - Netwrix Blog, juurdepääs juuni 12, 2025, https://blog.netwrix.com/healthcare-cybersecurity

5. TEHIK: Home page, juurdepääs juuni 12, 2025, https://www.tehik.ee/en
6. Cybersecurity and Frequent Cyber Attacks on IoT Devices in Healthcare: Issues and Solutions - arXiv, juurdepääs juuni 12, 2025, https://arxiv.org/html/2501.11250v1
7. Cybersecurity Awareness Training for Healthcare Staff: 2025 Edition - CyOp Security, juurdepääs juuni 12, 2025, https://cyopsecurity.com/insights/cybersecurity-awareness-training-for-healthcare-staff-2025-edition/
8. The Effectiveness of Cybersecurity Training - Scholars Archive, juurdepääs juuni 12, 2025, https://scholarsarchive.library.albany.edu/cgi/viewcontent.cgi?article=1105&context=etd
9. How Gamification Closes The Cybersecurity Skills Gap - Forbes, juurdepääs juuni 12, 2025, https://www.forbes.com/councils/forbestechcouncil/2025/02/26/the-growing-cybersecurity-skills-gap-a-breach-waiting-to-happen/
10. Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review, juurdepääs juuni 12, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC8059789/
11. Küberturvalisuse e-kursus - Äripäeva E-pood, juurdepääs juuni 12, 2025, https://pood.aripaev.ee/koolitus-kuberturvalisus
12. Cybersecurity Hygiene Checklist for Healthcare Organizations - Omega Systems, juurdepääs juuni 12, 2025, https://email.omegasystemscorp.com/hubfs/Healthcare%20Cybersecurity%20Checklist.pdf
13. Healthcare Cybersecurity Challenges & Threats - 2025 | Rubrik, juurdepääs juuni 12, 2025, https://www.rubrik.com/insights/healthcare-cybersecurity-challenges-threats-2025
14. E-tervise strateegia - Sotsiaalministeerium, juurdepääs juuni 12, 2025, https://sm.ee/sites/default/files/documents/2025-02/E-tervise%20strateegia.pdf
15. Cybernetica, juurdepääs juuni 12, 2025, https://cyber.ee/
16. Estonian e-Health Records - e-Estonia, juurdepääs juuni 12, 2025, https://e-estonia.com/solutions/e-health-2/e-health-records/
17. Asper Biogene OÜ andmeleke | Andmekaitse Inspektsioon, juurdepääs juuni 12, 2025, https://www.aki.ee/uudised/asper-biogene-ou-andmeleke
18. Olukord küberruumis – märts 2020 - RIA, juurdepääs juuni 12, 2025, https://www.ria.ee/sites/default/files/documents/2022-11/Olukord-kuberruumis-marts-2020.pdf
19. Police suspect Moroccan national of downloading Apotheka customer data - Estonian news, juurdepääs juuni 12, 2025, https://news.postimees.ee/8255999/police-suspect-moroccan-national-of-downloading-apotheka-customer-data
20. Küberturvalisuse aastaraamat 2025 | RIA, juurdepääs juuni 12, 2025, https://www.ria.ee/kuberturvalisuse-aastaraamat-2025

21. RIA küberturvalisuse aastaraamat 2024, juurdepääs juuni 12, 2025, https://www.vm.ee/sites/default/files/documents/2024-04/RIA%20k%C3%BCberturvalisuse%20aastaraamat%202024.pdf
22. Mis on lunavara ja kuidas end selle eest kaitsta - Netsec.ee, juurdepääs juuni 12, 2025, https://netsec.ee/mis-on-lunavara-ja-kuidas-end-selle-eest-kaitsta/
23. Mis on lunavara? | Microsofti turbeteenus, juurdepääs juuni 12, 2025, https://www.microsoft.com/et-ee/security/business/security-101/what-is-ransomware
24. SEKTORIAALSE KÜBERRISKIANALÜÜSI KOOSTAMISE JUHEND, juurdepääs juuni 12, 2025, https://www.ria.ee/sites/default/files/documents/2024-11/Kuberriskianaluuside-koostamise-metoodika.pdf
25. Eestis levib pahavaravõrgustik Emotet - Pettused.ee, juurdepääs juuni 12, 2025, https://pettused.ee/eestis-levib-pahavaravorgustik-emotet/?noamp=mobile
26. Sotsiaalne-manipulatsioon-kuidas-seda-suua.doc - Targalt Internetis -, juurdepääs juuni 12, 2025, https://www.targaltinternetis.ee/wp-content/uploads/2015/12/Sotsiaalne-manipulatsioon-kuidas-seda-suua.doc
27. KÜBERTURVALISUS - Tööstuslikud infovõrgud ja IT turvalisus, juurdepääs juuni 12, 2025, https://ikt.tthk.ee/kuberturvalisus/
28. TARTU ÜLIKOOL SOTSIAALTEADUSTE VALDKOND NARVA KOLLEDŽ ÕPPEKAVA „ETTEVÕTLUS JA DIGILAHENDUSED" Valeri Jakovlev KÜBERPE - DSpace, juurdepääs juuni 12, 2025, https://dspace.ut.ee/bitstreams/82e0605b-ab72-4d75-b6b5-d4a93c550552/download
29. New EU action plan set to protect hospitals, healthcare providers against rising cybersecurity threats - Industrial Cyber, juurdepääs juuni 12, 2025, https://industrialcyber.co/medical/new-eu-action-plan-set-to-protect-hospitals-healthcare-providers-against-rising-cybersecurity-threats/
30. Isiku terviseandmete vaba liikumise tõkete kaardistamine EL digitaalse ühisturu eesmärkide valguses - Sotsiaalministeerium, juurdepääs juuni 12, 2025, https://www.sm.ee/sites/default/files/content-editors/final_etervise_uuring.pdf
31. Andmekaitse – kas tüütu lisakohustus igapäevatöös?, juurdepääs juuni 12, 2025, https://www.aki.ee/uudised/andmekaitse-kas-tuutu-lisakohustus-igapaevatoos
32. 5426/25 JAI.2 Euroopa Liidu Nõukogu Käesolevaga edastatakse delegatsioonidele dokument COM(2025) 10 final. Lisatud - Data, juurdepääs juuni 12, 2025, https://data.consilium.europa.eu/doc/document/ST-5426-2025-INIT/et/pdf
33. Cybersecurity Hygiene for the Healthcare Industry: The basics in Healthcare IT, Health Informatics and Cybersecurity for the Health Sector by James Scott MD, Paperback | Barnes & Noble®, juurdepääs juuni 12, 2025, https://www.barnesandnoble.com/w/cybersecurity-hygiene-for-the-healthcare-industry-james-scott-md/1122957660
34. KÜBER- TURVALISUSE AASTARAAMAT 2023 - RIA, juurdepääs juuni 12, 2025, https://www.ria.ee/sites/default/files/documents/2023-02/RIA_kyberturvalisuse_aastaraamat_2023.pdf

35. Küberturvalisuse aastaraamat 2021 - RIA, juurdepääs juuni 12, 2025, https://www.ria.ee/sites/default/files/documents/2022-11/RIA-kuberturvalisuse-aastaraamat-2021.pdf
36. Eesti koolid küberturvaliseks! - RIA, juurdepääs juuni 12, 2025, https://www.ria.ee/eesti-koolid-kuberturvaliseks
37. Küberturvalisuse taseme kaardistamise ja arendamise toetus - EIS, juurdepääs juuni 12, 2025, https://eis.ee/toetused/kybertoetus/
38. TEHIK: Avaleht, juurdepääs juuni 12, 2025, https://www.tehik.ee/
39. Health-ISAC Avaleht – Tervis-ISAC – Tervisealase teabe jagamise ja analüüsi keskus, juurdepääs juuni 12, 2025, https://health-isac.org/et/
40. Tervishoiu küberturvalisus vajab kontrolli - Health-ISAC, juurdepääs juuni 12, 2025, https://health-isac.org/et/tervishoiu-k%C3%BCberjulgeolek-vajab-kontrolli/
41. Proposed ENISA role to safeguard cybersecurity of health sector - European Union, juurdepääs juuni 12, 2025, https://www.enisa.europa.eu/news/proposed-enisa-role-to-safeguard-cybersecurity-of-health-sector
42. Tervishoiusektori küberturvalisuse suurendamine - Euroopa Komisjon, juurdepääs juuni 12, 2025, https://commission.europa.eu/news/bolstering-cybersecurity-healthcare-sector-2025-01-15_et
43. EU direktiiv NIS2 - juriidilised küsimused ja soovitused - kohustused ja vastutus - OIXIO, juurdepääs juuni 12, 2025, https://oixio.eu/et/artiklid/nis2-juriidilised-kohustused-ja-vastutus/
44. Küberturvalisuse koolitus, juurdepääs juuni 12, 2025, https://www.bcskoolitus.ee/koolitus/kuberturvalisuse-koolitus/
45. Emerging Cyber Attack Risks of Medical AI Agents - arXiv, juurdepääs juuni 12, 2025, https://arxiv.org/html/2504.03759v1
46. [2504.03759] Emerging Cyber Attack Risks of Medical AI Agents - arXiv, juurdepääs juuni 12, 2025, https://arxiv.org/abs/2504.03759
47. PKL-194 / Isikuandmete töötlemise üldtingimused 1 / 9 - Tartu Ülikooli Kliinikum, juurdepääs juuni 12, 2025, https://www.kliinikum.ee/wp-content/uploads/2023/10/pkl-194_isikuandmete_tootlemise_uldtingimused_04.pdf
48. Tööstus 4.0 ja võrgud - Tööstuslikud infovõrgud ja IT turvalisus, juurdepääs juuni 12, 2025, https://ikt.tthk.ee/toostus-4-0-ja-vorgud/
49. Nutilinn (Smart city) ja asjade internet (IoT) - ICO wiki, juurdepääs juuni 12, 2025, https://wiki.itcollege.ee/index.php/Nutilinn_(Smart_city)_ja_asjade_internet_(IoT)
50. A Review on the Security Vulnerabilities of the IoMT against Malware Attacks and DDoS, juurdepääs juuni 12, 2025, https://arxiv.org/html/2501.07703v1
51. Social Engineering Awareness Kit | Free Resources - Terranova Security, juurdepääs juuni 12, 2025, https://www.terranovasecurity.com/resources/guides/social-engineering-training-kit
52. Top 10 Tips for Cybersecurity in Health Care, juurdepääs juuni 12, 2025, https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

53. Guide to Adopting the NIST Cybersecurity Framework in Healthcare - Compliancy Group, juurdepääs juuni 12, 2025, https://compliancy-group.com/adopting-the-nist-cybersecurity-framework-in-healthcare/
54. Cybersecurity in Healthcare (Hospitals & Care Centres) - Coursera, juurdepääs juuni 12, 2025, https://www.coursera.org/learn/cybersecurity-in-healthcare
55. Strengthening Cybersecurity in Healthcare: Key Strategies for Data Protection, juurdepääs juuni 12, 2025, https://www.cohnreznick.com/insights/strengthening-cybersecurity-healthcare-strategies-data-protection-operational-integrity
56. Enhancing Cybersecurity Measures in Healthcare: A Case Study - ECS Infotech, juurdepääs juuni 12, 2025, https://www.ecsinfotech.com/case-study/cybersecurity-healthcare-case-study-enhancements/
57. Gamified Cybersecurity Training - Security Compass, juurdepääs juuni 12, 2025, https://www.securitycompass.com/blog/gamified-cybersecurity-training/
58. Product: Cybersecurity Awareness Essentials Training for Healthcare, juurdepääs juuni 12, 2025, https://marketplace.healthstream.com/s/product/cybersecurity-awareness-essentials-training-for-healthcare/01t30000006HBzvAAG
59. Gamification: Revolutionising Healthcare Training for Leaders and Professionals, juurdepääs juuni 12, 2025, https://healthmanagement.org/c/healthmanagement/IssueArticle/gamification-revolutionising-healthcare-training-for-leaders-and-professionals
60. Case Study for Gamification for Cybersecurity | IEEE Thompson Okanagan Section, juurdepääs juuni 12, 2025, http://www.okanagan.ieee.ca/case-study-for-gamification-for-cybersecurity/
61. How Gamification Can Improve Cybersecurity Awareness Training, juurdepääs juuni 12, 2025, https://www.cm-alliance.com/cybersecurity-blog/how-gamification-can-improve-cybersecurity-awareness-training
62. Perspectives of Learning and Training Practitioners on Gamification - CORALS LLC, juurdepääs juuni 12, 2025, https://journal.coralsllc.com/index.php/CJAR/article/view/12
63. Workplace gamification using Cultural Historical Activity Theory: three case studies - MyUC Student Portal - University of Canberra, juurdepääs juuni 12, 2025, https://researchsystem.canberra.edu.au/ws/portalfiles/portal/45330208/Oberprieler_Kerstin.pdf
64. secure.ipex.eu, juurdepääs juuni 12, 2025, https://secure.ipex.eu/IPEXL-WEB/download/file/082d290892218c90019228b9e70a0470
65. secure.ipex.eu, juurdepääs juuni 12, 2025, https://secure.ipex.eu/IPEXL-WEB/download/file/082d290894d3d7d80194d5d381400275
66. How Healthcare Can Reduce Cybersecurity Response Times from Hours to

Minutes, juurdepääs juuni 12, 2025, https://medcitynews.com/2025/06/how-healthcare-can-reduce-cybersecurity-response-times-from-hours-to-minutes/
67. Phishing Awareness Boosts Hospital Cyber Security - BlueOrange Compliance, juurdepääs juuni 12, 2025, https://www.blueorangecompliance.com/phishing-awareness-boosts-hospital-cyber-security/
68. NIST Updates Guidance For Healthcare Security - PurpleSec, juurdepääs juuni 12, 2025, https://purplesec.us/breach-report/nist-healthcare-security-guidance/
69. healthsectorcouncil.org, juurdepääs juuni 12, 2025, https://healthsectorcouncil.org/hscc-cybersecurity-training-video-series/#:~:text=%E2%80%9CCybersecurity%20for%20the%20Clinician%E2%80%9D%20is,the%20government%20to%20identify%20and
70. Free “Cybersecurity for the Clinician” Training Video - Anna Nurse, juurdepääs juuni 12, 2025, https://www.annanurse.org/free-cybersecurity-for-the-clinician-training-video/
71. HSCC Cybersecurity Training Video Series - Health Sector Council, juurdepääs juuni 12, 2025, https://healthsectorcouncil.org/hscc-cybersecurity-training-video-series/
72. Cybersecurity Training & Exercises - CISA, juurdepääs juuni 12, 2025, https://www.cisa.gov/cybersecurity-training-exercises
73. Tulevikuvaade tööjõu- ja oskuste vajadusele: tervishoid - Oska Kutsekoda, juurdepääs juuni 12, 2025, https://oska.kutsekoda.ee/wp-content/uploads/2016/04/tervishoiu_uuringu_tervik tekst.pdf
74. Vaimse tervise tegevuskava 2023–2026 - Sotsiaalministeerium, juurdepääs juuni 12, 2025, https://www.sm.ee/media/2998/download
75. Avaleht | RIA, juurdepääs juuni 12, 2025, https://www.ria.ee/
76. Healthcare Cybersecurity Challenges: A Complete Guide - ER Tech Pros, juurdepääs juuni 12, 2025, https://www.ertech.io/blog/healthcare-cybersecurity-challenges-a-complete-guide
77. What Is the ROI of Investing in Cybersecurity Awareness Programs? - MetaCompliance, juurdepääs juuni 12, 2025, https://www.metacompliance.com/blog/cyber-security-awareness/roi-of-cybersecurity-awareness-programs
78. SANS Tallinn September 2025 | Cyber Security Training, juurdepääs juuni 12, 2025, https://www.sans.org/cyber-security-training-events/tallinn-september-2025/
79. The Best Cyber Security Course in Estonia | EyeQ Dot Net, juurdepääs juuni 12, 2025, https://www.eyeqdotnet.com/cyber-security-course-in-estonia