RIIGI INFOSÜSTEEMI AMET

Riskid meditsiinisektoris küberturvalisuse tagamisel

Sissejuhatus

Hetkeolukorras, kus maailmas toimuv mõjutab väga palju digikeskkonda, tuleb küberturvalisuse peale mõelda rohkem kui kunagi varem. Asutused peaksid veenduma, et organisatsioon ja nende poolt pakutavad teenused oleksid turvanõutele vastavad. Eriti oluline on see meditsiinisektoris, kus delikaatseid isiku- ja terviseandmeid käsitleb suur osa töötajatest igapäevaselt seejuures tihti selle peale mõtlemata.

Selleks, et omada head ülevaadet millised riskid asutuses on või milliseid turvameetmeid riskide leevendamiseks kasutatakse, on vajalik põhjaliku riskianalüüsi olemasolu, mis peaks hõlmama ka riskisõltuvuste kaardistust ja riskikäsitluskava. Riskianalüüsis tuleks käsitleda nii organisatsiooniga seotud riske kui ka võrgu-ja infosüsteemide seotud riske, millele tuleb rakendada vastavalt organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid.

2018. aastal jõustus Eestis küberturvalisuse seadus, mis seadis küberturvalisuse nõuded sellistele ettevõtetele ja asutustele, mille tegevus on elutähtis, sealhulgas ka meditsiinisektorile. Lisaks peavad meditsiinisektori asutused arvestama ka isikuandmete kaitse üldmääruse ja isikuandmete kaitse seadusega, hädaolukorra seadusega ja muude valdkondlike regulatsioonidega kust tulevad erinevad nõuded teenuste pakkumisele.

Käesolevas dokumendis on toodud välja erinevad riskid, millele tuleks esmajärjekorras mõelda ja riskianalüüsis riske kaardistades arvesse võtta.

Riskide kirjeldused

1. **Infoturbepoliitika vähene korraldus organisatsioonis**
   Infoturbe korraldamine asutuses annab aluse asutuse turvateadlikkusele. Ka meditsiinsektoris, kus käsitletakse igapäevaselt kriitilised isiku-ja terviseandmeid tuleks luua organisatsiooniülene infoturbepoliitika ning strateegilised põhimõtted ja suunised infoturbe korraldamiseks. Organisatsiooni infoturbe korraldamise seisukohalt on infoturbe poliitika kehtestamisel ja personalile teatavaks tegemisel väga oluline roll. Kui puuduvad infoturvet reguleerivad eeskirjad ja juhendid, siis puudub ka teadmus, mille järgi saab asutuses juhinduda. Kui infoturbe meetmeid ei ole kehtestatud või meetmete rakendamise juhised ei ole arusaadavalt dokumenteeritud, siis pole ka võimalik kontrollida turvameetmete olemasolu. Ebapiisavad eeskirjad või eeskirjade eest vastutavate isikute puudumise tõttu on asutusel otsene oht kahjudele, eriti olukordade puhul, mis nõuavad aegkriitilist tegutsemist.

2. **Infoturbe eest vastutav isik ja tema roll asutuses on puudu**
   Olenevalt asutuse suurusest peaks asutuses juhtkonna poolt olema määratud isik koos rolli ja ülesannetega, kes tegeleb infoturbe korraldamisega. Ülesannete kirjeldamata jätmine võib tekitada olukorra, kus ohustav tegevus võib jääda märkamata. Vastutav isik peaks omama ülevaadet kogu organisatsiooni tegevusprotsesside nõrkadest ja kriitilistest aspektidest sealhulgas ITga seotud nüanssidest ning regulatsioonidest ning juhtima juhtkonna tähelepanu nendele.

3. **Vähene infoturbeteadlikkus ja selle korraldus asutuses**
   Regulaarsete infoturbeteadlikkuse koolituste puudumisel või personali liiga pika aja tagant koolitades võivad meditsiinisektori töötajad, kelle põhirõhk on meditsiiniabi pakkumisel, unustada igapäevatöö kõrvalt baasteadmised infoturbest (nt e-mailide õngitsuse oht, liiga lühikesed ja lihtsad paroolid, arvuti välja logimine laua tagant lahkudes, paroolid märkmepaberitel jne). Personali tuleks koolitada pidevalt ja kontrollida ka nende teadmisi, mis kinnistavad infot (nt testidega). Personali infoturbeteadlikkuse hoidmine on pidev protsess ja see omakorda on üheks organisatsiooni alaliseks infoturbemeetmeks, millega tuleb aktiivselt ja regulaarselt tegeleda. Kui töötajad ei ole infoturbe meetmetest piisavalt teadlikud, kannatab organisatsiooni turvakultuur ja turvaeesmärkide täitmine. Töötajal on keeruline luua konkreetseid seoseid oma töökeskkonnaga, sest neile ei ole selgitatud turvameetmete olulisust. Sageli on inimtegevusest tingitud turvaintsidendi tekkepõhjuseks turvanõuete puudulik tundmine ja/või nende järgimata jätmine. See omakorda võib mõjutada pakutava teenuse toimimist või tuua kaasa haldusalas olevate eriliigiliste isikuandmete konfidentsiaalsuse, tervikluse või käideldavuse nõuete rikkumise ja nende andmete sattumise kolmandate isikute valdusesse.

4. **Puudulik turvaline kanal andmevahetuseks (e-kirjavahetuseks)**
   Meditsiinitöötajate suhtlus/andmevahetus igapäevaselt peaks käima läbi turvalise kanali, kuna tervishoiu asutused käitlevad isikuandmeid ja terviseandmeid. Näiteks e-kirjavahetus peaks olema krüpteeritud. Ebaturvalise e-posti serveri kasutamisega, mis on asutuse üks peamisi ründevektoreid, kaasneb oht eriliigilistele isikuandmetele ning ohustatud on asutuse käsutuses olevate andmete tervikluse ning konfidentsiaalsuse kaitse.

5. **Puudulik ülevaade võrgus osalevatest infovaradest, süsteemidest ja tarkvaradest (sh meditsiiniseadmed ja tarkvara)**
   Arvutivõrgu turvalisuse kaitseks on vaja pidada ajakohast infovaranimekirja ja võrgu IT-taristu arhitektuurilist kirjeldust (skeemi) kõikide võrku ühendatud süsteemide, võrguseadmete ja tarkvarade ning nendevaheliste ühenduste kohta sealhulgas ka meditsiinitarkvara ja meditsiiniseadmete kohta. Nimekirja puudumisel tekib oht, et asutusel puudub ülevaade millised infovarad asutuses on ja sellepealt ei ole infot milliseid infovarasid tuleks nt välja vahetada või uuendada. Tuleks tuvastada ja arvestust pidada kõikide võrku ühendatavate seadmete üle, olenemata sellest, kas need kuuluvad asutusele endale või mitte. IT-taristus osalevate infovarade inventuur ja haldus peaks olema korraldatud nii, et see annaks võrgu administraatorile ajakohase info infovarade (arvutite, serverite, võrguseadmete, tarkvarade jne) staatuse, eluea, kasutajate kohta ning kirjeldaks ära infovarade omavahelised seosed, sõltuvused,

vastutajad ja rollijaotused alates kasutajast kuni infosüsteemi ja võrgu lõpp-seadmeteni välja.

6. **Riistvara ja tarkvara ei hoita ajakohasena**
   IT-taristu halduses avaldab olulist mõju turvalisusele asutuse teenuseid käitavate operatsioonisüsteemide ja tööjaamas kasutavate tarkvarade turvapaikade ja värskenduste kontrollimine ja paigaldamine. Tarkvarauuenduste õigeaegne tegemata jätmine toob endaga kaasa suurenenud riski edukaks rünnakuks. Meditsiiniasutustes, kus on töötajaid palju, võiks tööjaamade ja võrguseadmete tarkvara uuendamine käia automatiseeritult. Uuendusi peaks enne tööjaamadesse paigaldamist testima ja paigaldada tuleks need esimesel võimalusel. Samuti peaks tööjaama ja võrguseadmete uuendamine olema dokumenteeritud. See loob järjepidevuse olulise turvameetme rakendamisel, mis aitaks tagada turvapaikade ja uuenduste õigeaegse korraldamise võimalike küberintsidentide ennetamiseks. Siinkohal tulekski kaaluda keskhalduse kasutuselevõttu, kuna see võimaldab seadmeid ja tarkvara paremini hallata.

7. **Puudulikud taasteplaanid ja varundamine**
   Üheks IT-taristu halduse rajamise ja käigus hoidmise alaliseks turvameetmeks on infosüsteemide andmevarunduse ja taastetestimise kontseptsiooni olemasolu. Määratud peaks olema andmevarunduse eest vastutaja ning kehtestama reeglid mida, kui tihti, kuhu varundada tuleb ja kui tihti tuleb taasteteste teha, et aru saada, kas varundussüsteem toimib korrektselt. Andmevarunduse puudumisel võib andmekadu (nt kahjurvara, tehniliste tõrgete või tulekahju tõttu) organisatsioonile kaasa tuua korvamatut kahju. Kui varundusprotseduuride jaoks ei ole koostatud andmevarunduskontseptsiooni või kontseptsioonist ei peeta kinni (nt varundatakse andmeid liiga harva või on andmete reaalne taasteaeg suurem kui organisatsioonis kokku lepitud), on andmete taastamine raskendatud. Organisatsioonipõhiselt tuleks luua asutusele oluliste süsteemide jaoks taasteplaanid, mis aitavad kriitilises olukorras süsteemid kiiresti ja tõhusalt taastada.

8. **Puudulik kaugtöö korraldus asutuses (sh isiklike tööjaamade kasutamine)**
   Kaugtöö korraldamisel meditsiiniasutuses tuleks eelkõige mõelda VPN lahendusele ja kontrollitud riistavarale (sülearvutid, nutitelefonid). Kontrolli alt väljas olevates seadmetes võib esineda teadmata ründevektoreid, mis suurendavad ohtu meditsiinisektoris asutuste arvutivõrgu ja infosüsteemide korrektsele toimimisele ja turvalisusele. Iga asutuse IT teenistuse kontrolli alt väljas olev sülearvuti või muu seade on kõrgendatud risk IT-taristule, mille kaudu on avatud erinevad ründevektorid sisevõrgu ressurssidele. Tuleks võtta kasutusele lisa turvameetmed isiklike arvutite, nutitelefonide kasutamise kontrolli alla saamiseks isegi olukorras, kui neid kasutatakse vaid e-teenustes, milledesse autentimine käib kaheastmelise autentimisega.

9. **Logimise halb korraldus**
   Meditsiinisektoris nii nagu ka muudes sektorites tuleks infosüsteemide ja sisevõrgu sündmuste kohta pidada logi. Kui logimist ei ole üksikasjalikult plaanitud (dokumenteeritud) ega viida läbi pistelisi kontrolle ega analüüse logiandmete osas, on IT-süsteemide logiandmete haldus kontrollita ning IT-süsteemidega seotud turvasündmuste tekkepõhjused võivad seetõttu jääda tuvastamata. Samuti tuleks ära määratleda, kes ja kuidas logidele ligi pääseb. Logimise kontseptsioonita puudub

kindlus, et vajalikud logiandmed tegeliku turvasündmuse tuvastamisel ja lahendamisel soovitud ajal on olemas.

10. Puudulik intsidentide haldus ja süsteemide seire

Hea infoturbekorraldusega meditsiiniasutustes peaks olema intsidentide käsitlemise ja haldamise protsess (turvaintsidentide määratlus, käsitlus protseduurid, teavitamiskanalid, turvaintsidentide käsitlemise eest vastutavad isikud jm). Olulised IT-süsteemid peaksid olema monitooringusüsteemi taga, mis teavitab esinevatest probleemidest ja veasituatsioonidest. Intsidente tuleks registreerida ja põhjuseid uurida ja analüüsida. Tuleks juurutada majasisene toimiv intsidentide haldussüsteem, mis sisaldab mõjutatud osapoolte teavitamast (töötajaid, asutusi, koostööpartnereid), sealhulgas küberintsidendi korral CERT-ee teavitamist. Intsidentide käsitlemise ja haldamise protsessi puudumisel tekib oht, et mõni intsident jääb märkamata/registreerimata ja seetõttu võib teenuse taastamine võtta kauem aega ja intsidendi põhjus jääda teadmata ja analüüsimata.

NB! Küberintsidentidest teavitamine CERT-EE-le on küberturvalisuse seaduse järgi meditsiiniasutustel kohustus, mis tuleb oma tegevusprotsessidega 24 tunni jooksul intsidendi teatavaks tulemisest alates tagada.

11. IT-taristule kasutajate juurde- ja ligipääsuõiguste puudulik haldamine

Meditsiiniasutuse IT-taristu infoturbes on väga oluline roll kasutajate haldusel, sinna sisse kuulub ka IT ressurssidele pääsuõiguste andmine ja ära võtmine. Kasutajakonto tuleks luua ja pääsuõigused tagada üksnes vajaduse põhiselt. Kasutajakontode üle tuleks pidada ajakohast ülevaadet ning omada reegleid kasutajaõiguste andmiseks ja äravõtmiseks. Kehtestamata reeglitega pole tagatud kindlus, et asutuses oleks turvaline, õiguspärane ja järjepidev kasutajate haldus.

12. Väljast tellimise halb korraldus

Väljastpoolt asutust teenuste tellimisel tuleks veenduda, et IT-taristule küberturvalisust tagavad teenusleppetingimused oleks kokkulepitud nii, et osutamiseks vajalik kaitsetarve - teenuse käideldavus, konfidentsiaalsus ja terviklus oleks tagatud. Tuleks veenduda, et on teadmus, et millisel juhul vastutab välispartner teenuse kättesaadavuse eest ja millistel tingimustel. Otsus kasutada väljast tellimist võib viia organisatsiooni teenuseandjast täielikku sõltuvusse, põhjustades oskusteabe kaotust ja väljast tellitud teenuse üle kontrolli kadumist. Klient ei pruugi puudujääke teenuseandja infoturbes ise märgata.

Kokkuvõte

Kuna uusi turvanõrkusi avastatakse digitaalses keskkonnas, sealhulgas meditsiinisektoris tegutsevates asutuste teenuseid käitavates süsteemides igapäevaselt, siis tuleb korraldada asutuse infoturvet süsteemselt ja regulaarselt. Esmajärjekorras tuleks teadvustada juhtkonna tasemel ohtudest ja probleemidest ning luua tõhus infoturbepoliitika, mis kohandub kogu organisatsioonile. Väljatoodud riskide hindamisel tuleks seetõttu lähtuda eelkõige asutusest endast, kuid antud punktid kohanduvad kõikidele meditsiinisektoris tegutsevatele (samuti ka muude valdkondade) asutustele, kes tegutsevad digikeskkonnas.

Dokumendis väljatoodud punktide kohta loetleb Eesti infoturbestandard E-ITS hulga võimalikke ohtusid, millega soovitame kindlasti tutvuda https://eits.ria.ee/.