European Union Agency
for Cybersecurity
Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

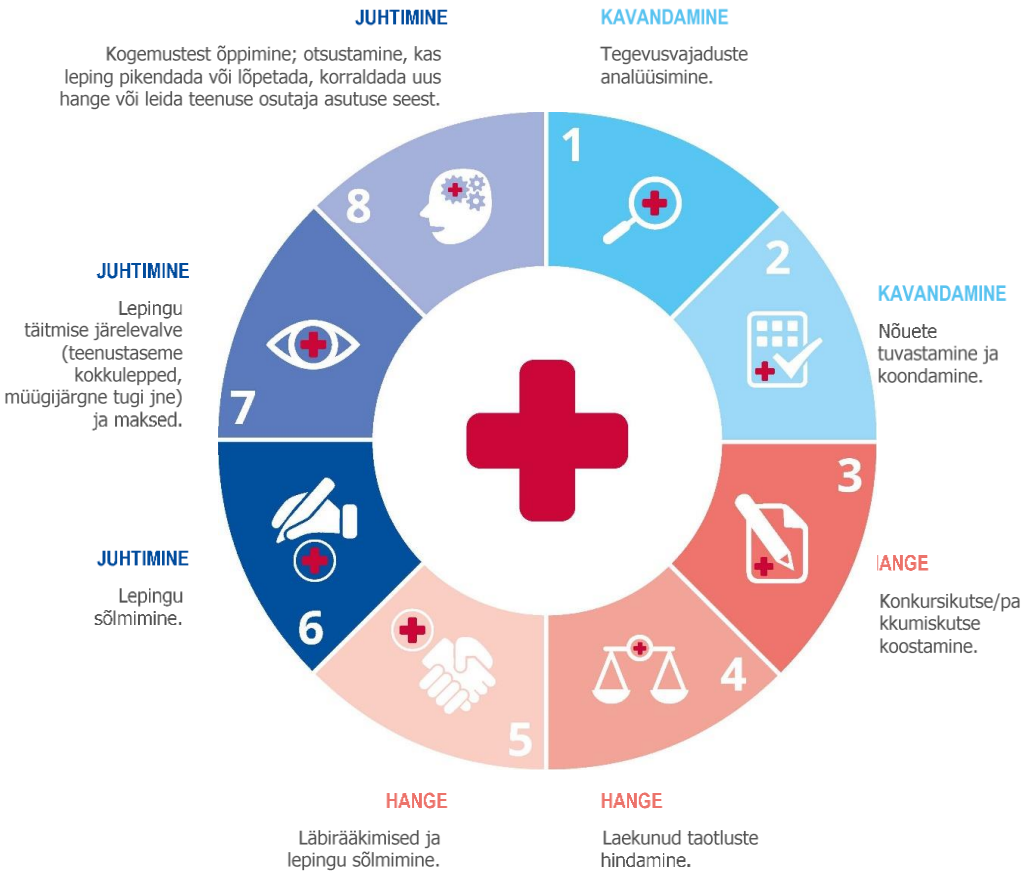
HANKESUUNISED HAIGLATELE KÜBERTURVALISUSE TAGAMISEKS

Aruande eesmärk on anda juhiseid tervishoiutöötajatele. Paljud tavad ja soovitused on kasulikud ka muudele tervishoiuorganisatsioonidele, sest hankeprotsessid võivad olla väga sarnased. Aruandest on kasu tervishoiutöötajatele, kes töötavad haiglates tehnilistel ametikohtadel, st tippjuhtidele (nt infojuhid, infoturbejuhid ja tehnoloogiajuhid), samuti tervishoiuorganisatsioonide IT-töötajatele ja hankeametnikele. Käesolevas lühidokumendis on aruande põhipunktide lühiülevaade. Üksikasjalik teave on ENISA väljaandes „Good Practices for the Security of Healthcare Services“ (Tervishoiuteenuste turvalisuse head tavad), mis avaldati 2020. aasta veebruaris.

HANKEPROTSESS

Haiglate ökosüsteem koosneb mitmest IT-komponendist ja seega tuleb uurida kõigi nende eri komponentide küberturvet eraldi. Küberturve peab olema hankeprotsessi kõigi etappide osa. Selles jaotises tutvustatakse hankeprotsessi ühisetappe toodete ja teenuste, sealhulgas meditsiiniseadmete, infosüsteemide ja taristu hankimisel.

Joonis 1. Haiglate hankeprotsessi olelusring



- Kavandamisetapp: kõigepealt analüüsib haigla oma vajadusi ja kogub kokku osakondade nõuded. Näiteks uue pilveteenuse hankimisel peab tehnoloogiajuht tuvastama vajadused ja uurima, mis kasutusvõimalusi teenus pakub.

- Hankeetapp: seejärel koostatakse nõuete põhjal tehnilised kirjeldused ja koostöös hankeüksusega algab hankemenetlus (nt avaldatakse pakkumiskutse). Haigla saab pakkumused, mida hindab komitee (sealhulgas tehnoloogiajuht, infoturbejuht ja/või IT-rühm), kes valib kõige sobivamad tooted. Töövõtjaga peetakse läbirääkimisi ja sõlmitakse leping.

- Juhtimisetapp: lõpuks antakse leping (juhtimine ja järelevalve) haiglas teatud projektijuhi vastutusalasse. Tema ülesanne on hankemenetlus lõpetada ja käsitleda kasutajate tagasisidet seadmete, süsteemi või teenuse tegeliku toimimise kohta.

HAIGLATES KORRALDATAVATE HANGETE LIIGID

Tabel 1. Hankeliigid (varade taksonoomia)

Hanke liik	Liigi kirjeldus
Kliinilise info süsteemid	Hõlmab meditsiiniteenuste osutamiseks vajaliku mis tahes liiki tarkvara hankimist
Meditsiiniseadmed	Mis tahes riistvara, mis on ette nähtud haiguste raviks, tõrjeks või diagnostikaks
Võrguseadmed	Võrguliinid (koaksiaalsed, optilised), lüüsid, ruuterid, lülitid, tulemüürid, VPNid, IPS, IDS jne.
Kaugtervishoiusüsteemid	Vahendid või seadmed, millega pakutakse tervishoiuteenuseid väljaspool haiglakeskkonda, eelkõige teenuseid, mida tänapäeval nimetatakse haiglapõhisteks koduhooldusteenusteks.
Mobiilsed klientseadmed	Tarkvara, mis pakub tervishoiuabi või võimaldab koguda meditsiinilisi andmeid ja mis ei ole otseselt ühendatud haigla võrguga, näiteks telemeditsiini rakendused.
Tuvastussüsteemid	Patsientide või meditsiinitöötajate tuvastamise süsteemid (biomeetrilised skannerid, kaardilugerid jne) ning IT-süsteemidele juurdepääsuks vajaliku tuvastamise ja/või volitamise tagamise süsteemid.
Hoonehaldussüsteemid	Mis tahes ehitis, milles võidakse osutada meditsiiniteenuseid.
Tehnojuhtimissüsteemid	Süsteemid, millega juhitakse keskuste kõiki füüsilisi aspekte, näiteks elektrireguleerimissüsteemid, ukselukusüsteemid ja valvesüsteemid.
Kutselised teenused	Mis tahes teenused, mida osutavad spetsialistid või ettevõtted, sh allhankena: meditsiiniteenused, transport, raamatupidamine, tehnikateenused, IT, õigusteenused, hooldusteenused, puhastusteenused, toitlustamine jne.
Pilveteenused	Mis tahes side- ja infosüsteem või muu infosüsteem mujal kui meditsiiniasutuses või andmekeskuses ja mis on meditsiinikeskuse IT-osakonna täieliku kontrolli all.

OHUTAKSONOOMIA

Eri liiki hangetega võivad kaasneda mitmesugused ohud haigla IKT-keskkonnale. Et tuvastada, mis ohud on teie organisatsiooni jaoks kõige asjakohasemad, uurige koos oma IT-, turbe- või riskijuhtimisosakonnaga käesolevas jaotises esitatud ohutaksonoomiat. See peaks kuuluma haigla IT-ülesannete hulka olenemata hanke potentsiaalist.

Tabel 2. Ohuliigid (ohutaksonoomia)

Oht	Näited
Loodusnähtused	Tulekahjud, üleujutused, maavärinad
Tarneahela tõrge	Tõrge pilveteenuste osutamisel, tõrge võrguteenuse osutamisel, elektrikatkestus, meditsiiniseadmete tootja hooletus või vastutuse puudumine.
Inimeksimused	Meditsiinisüsteemi konfiguratsiooniviga, auditilogide puudumine, loata juurdepääsu kontroll (puudumine või protsessid), mittevastavus (isiklike seadmete kasutamine), meditsiinitöötajate või patsiendi viga
Pahatahtlik tegevus	Kahjurvara (viirus, lunavara, isiklike seadmete kasutamine), kaaperdusrünne (kaevekaaperdus, meditsiiniseadmetesse häkkimine), suhtlusrünne (andmepüük, söötpüük, seadmete kloonimine), vargus (andmed, seadmed), meditsiiniseadmetega manipuleerimine, andmete kopeerimine, teenusetõkestus, veebipõhised ründed, veebirakenduste ründed, siseoht, füüsiline manipuleerimine/kahjustamine, identiteedivargus, küberspionaaž, komponentide mehaaniline halvang
Süsteemirikked	Tarkvararike, aegunud püsivara, seadme rike, võrgukomponentide rike, ebapiisav hooldus

KÜBERTURBE HEAD TAVAD HANGETES

Järgmine heade tavade loetelu ei ole ammendav, kuid annab siiski tugeva eelise tervishoiuasutuse IT-spetsialistile, kes vastutab haiglas seadmete ostmise eest. See heade tavade loetelu koostati teabe põhjal, mis saadi tervishoiutöötajaid küsitledes. Lugeja saab loetelu kohandada oma organisatsiooni prioriteetide järgi.

1. hea tava. Kaasata IT-osakond hangete eri etappidesse, et arvestataks asjatundmust seoses küberturbeaspektidega.

Hankeetapid: kõik

Seotud hankeliigid: kõik

Seotud ohud: kõik

2. hea tava. Tagada nõrkuste tuvastamise ja juhtimise protsessiga, et enne uute toodete või teenuste hankimist kaalutletakse nõrkusi ning olemasolevate toodete ja teenuste nõrkusi jälgitakse kogu nende olelusringi jooksul.

Hankeetapid: kõik

Seotud hankeliigid: kliinilise info süsteemid, meditsiiniseadmed, võrguseadmed, kaugtervishoiusüsteemid, mobiilsed klientseadmed, tuvastussüsteemid, tehnojuhtimissüsteemid, pilveteenused

Seotud ohud: kõik

3. hea tava. Koostada riistvara- ja tarkvarauuenduste poliitika, et tagada operatsioonisüsteemi ja tarkvara uusimate paikade rakendamine ning viirustõrjetarkvara ajakohastamine.

Hankeetapid: kõik

Seotud hankeliigid: meditsiiniseadmed, kliinilise info süsteemid, võrguseadmed, kaugtervishoiusüsteemid, mobiilsed klientseadmed, tuvastussüsteemid, tehnojuhtimissüsteemid, pilveteenused

Seotud ohud: pahatahtlik tegevus, tarneahela tõrge, süsteemirikked

4. hea tava. Tõhustada juhtmeta side turbemeetmeid, et juurdepääs haigla Wi-Fi-võrkudele oleks piiratud ja rangelt ohjatud.

Hankeetapid: kõik

Seotud hankeliigid: meditsiiniseadmed, kaug-klientseadmed, tuvastussüsteemid, pilveteenused

Seotud ohud: pahatahtlik tegevus, inimeksimused

5. hea tava. Kehtestada testimispoliitika, millega tagatakse, et äsja hangitud või äsja konfigureeritud tooted läbivad läbistustestimise ja võetud parandusmeetmed on kooskõlas tegeliku keskkonna tööparameetritega.

Hankeetapid: kõik

Seotud hankeliigid: kliinilise info süsteemid, meditsiiniseadmed, võrguseadmed, kaugtervishoiusüsteemid, mobiilsed klientseadmed, tuvastussüsteemid, hoonehaldussüsteemid, tehnojuhtimissüsteemid, pilveteenused

Seotud ohud: pahatahtlik tegevus, süsteemirikked, inimeksimused

6. hea tava. Koostada talitluspidevuse kavad tagamaks, et süsteemirike ei katkesta haigla põhiteenuseid ja teenuseosutaja roll on täpselt määratletud.

Hankeetapid: kõik

Seotud hankeliigid: meditsiiniseadmed, kliinilise info süsteemid, võrguseadmed, kaugtervishoiusüsteemid, mobiilsed klientseadmed, tuvastussüsteemid, tehnojuhtimissüsteemid, pilveteenused

Seotud ohud: pahatahtlik tegevus, tarneahela tõrge, süsteemirikked

7. hea tava. Arvestada koostalitlusvõime probleeme, et tagada turbelünkade puudumine juba olemasolevates komponentides (pärandsüsteemides).

Hankeetapid: kõik

Seotud hankeliigid: kliinilise info süsteemid, meditsiiniseadmed, kaugtervishoiusüsteemid, mobiilsed klientseadmed, tuvastussüsteemid, tehnojuhtimissüsteemid, pilveteenused

Seotud ohud: süsteemirikked, inimeksimused, pahatahtlik tegevus

8. hea tava. Võimaldada kõigi komponentide testimine, et tagada lubatud tulemuste saavutamine: kontrollida kasutuslihtsust, kontrollida tulemuste õigsust koormuse tingimustes ja turbedefektide olemasolu (nõrga salasõna poliitika, SQL-süst).

Hankeetapid: kõik

Seotud hankeliigid: kliinilise info süsteemid, meditsiiniseadmed, kaug-klientseadmed, tuvastussüsteemid, pilveteenused, tehnojuhtimissüsteemid, kaugtervishoiusüsteemid, hoonehaldussüsteemid, mobiilsed klientseadmed

Seotud ohud: pahatahtlik tegevus, inimeksimused, süsteemirikked, tarneahela tõrge

9. hea tava. Võimaldada auditeerimine ja logimine, et jälitada süsteemi murdmisel ründajaid ja leida, kui palju teavet on kadunud või varastatud.

Hankeetapid: kõik

Seotud hankeliigid: meditsiiniseadmed, kaugtervishoiusüsteemid, mobiilsed klientseadmed, tuvastussüsteemid, tehnojuhtimissüsteemid

Seotud ohud: pahatahtlik tegevus, tarneahela tõrge, süsteemirikked

10. hea tava. Krüptida jõudeolekus ja liikvel tundlikud isikuandmed, määratledes poliitika süsteemide, teenuste ja seadmete jaoks, mis töötlevad isikuandmete kaitse üldmääruse artikli 9 kohaseid isikuandmete eriliike.

Hankeetapid: kõik

Seotud hankeliigid: meditsiiniseadmed, kliinilise info süsteemid, võrguseadmed, kaugtervishoiusüsteemid, mobiilsed klientseadmed, tuvastussüsteemid, tehnojuhtimissüsteemid, pilveteenused

Seotud ohud: pahatahtlik tegevus, tarneahela tõrge, süsteemirikked

11. hea tava Teha riskihindamine hankeprotsessi osana.

Hankeetapid: kavandamine

Seotud hankeliigid: kõik

Seotud ohud: kõik

12. hea tava. Eelkavandada võrgu-, riistvara- ja litsentsinõuded, et määrata, kas enne uue süsteemi paigaldamist on vaja teha veel uuendusi ja/või oste.

Hankeetapid: kavandamine

Seotud hankeliigid: kliinilise info süsteemid, võrguseadmed, tuvastussüsteemid, tehnojuhtimissüsteemid

Seotud ohud: tarneahela tõrge, süsteemirikked, loodusnähtused, inimeksimused

13. hea tava. Tuvastada hangitavate toodete või teenustega seotud ohud ning tagada, et ohte tuvastatakse hanke olelusringi jooksul pidevalt.

Hankeetapid: kavandamine, juhtimine

Seotud hankeliigid: kõik

Seotud ohud: kõik

14. hea tava. Eraldada oma võrk, et tagada võrguliikluse isoleerimine ja/või filtreerimine, et piirata ja/või takistada juurdepääsu võrgualadele.

Hankeetapid: kavandamine, hange

Seotud hankeliigid: meditsiiniseadmed, kliinilise info süsteemid, võrguseadmed, kaugtervishoiusüsteemid, mobiilsed klientseadmed, tuvastussüsteemid, tehnojuhtimissüsteemid, pilveteenused

Seotud ohud: pahatahtlik tegevus, tarneahela tõrge, süsteemirikked

15. hea tava. Määrata võrgunõuded, et tagada pärast võrgu ja komponentide topoloogia loomist koostalitlusvõime ja vältida lünki.

Hankeetapid: kavandamine

Seotud hankeliigid: kliinilise info süsteemid, võrguseadmed, tuvastussüsteemid, tehnojuhtimissüsteemid, pilveteenused, kaugtervishoiusüsteemid, mobiilsed klientseadmed

Seotud ohud: tarneahela tõrge, süsteemirikked, loodusnähtused

16. hea tava. Kehtestada põhilised turbenõuded ja lisada need tarnijate valimisel sobivuskriteeriumide hulka.

Hankeetapid: kavandamine, hange

Seotud hankeliigid: meditsiiniseadmed, kliinilise info süsteemid, võrguseadmed, kaugtervishoiusüsteemid, mobiilsed klientseadmed, tuvastussüsteemid, tehnojuhtimissüsteemid, pilveteenused

Seotud ohud: pahatahtlik tegevus, tarneahela tõrge, süsteemirikked

17. hea tava. Koostada pilveteenuste hankimiseks spetsiaalne konkursikutse, arvestades regulatiivseid ja poliitikanõudeid.

Hankeetapid: kavandamine, hange

Seotud hankeliigid: pilveteenused

Seotud ohud: pahatahtlik tegevus, tarneahela tõrge

18. hea tava. Prioriseerida selliste varade hankimist, mis on sertifitseeritud küberturbekavade/-standardite alusel.

Hankeetapid: hange

Seotud hankeliigid: meditsiiniseadmed, kliinilise info süsteemid, võrguseadmed, kaugtervishoiusüsteemid, mobiilsed klientseadmed, tuvastussüsteemid, tehnojuhtimissüsteemid, pilveteenused

Seotud ohud: pahatahtlik tegevus, tarneahela tõrge, süsteemirikked

19. hea tava. Teha uue süsteemi või teenuse hanget kavandades andmekaitsele avalduva mõju hindamine.

Hankeetapid: hange

Seotud hankeliigid: kliinilise info süsteemid, meditsiiniseadmed, võrguseadmed, kaugtervishoiusüsteemid, mobiilsed klientseadmed, tuvastussüsteemid, erialateenused, pilveteenused

Seotud ohud: pahatahtlik tegevus, inimeksimused

20. hea tava. Luua lüüsid, mis võimaldavad hoida olemasolevad süsteemid/seadmed ühendatuna ja reguleerida pääsu nendes rühmades esinevate probleemide korral.

Hankeetapid: hange, juhtimine

Seotud hankeliigid: meditsiiniseadmed, kaugtervishoiusüsteemid, mobiilsed klientseadmed, tuvastussüsteemid, tehnojuhtimissüsteemid

Seotud ohud: pahatahtlik tegevus, tarneahela tõrge, süsteemirikked

21. hea tava. Pakkuda küberturbekoolitust organisatsiooni turbetavade kohta, et tagada sisetöötajate ning väliste töövõtjate ja konsultantide asjakohane väljaõpe.

Hankeetapid: hange, juhtimine

Seotud hankeliigid: kõik

Seotud ohud: pahatahtlik tegevus, inimeksimused

22. hea tava. Koostada intsidentidele reageerimise kavad, mis hõlmavad äsja hangitud tooteid või süsteeme.

Hankeetapid: hange, juhtimine

Seotud hankeliigid: meditsiiniseadmed, kliinilise info süsteemid, võrguseadmed, kaugtervishoiusüsteemid, mobiilsed klientseadmed, tuvastussüsteemid, tehnojuhtimissüsteemid, pilveteenused

Seotud ohud: pahatahtlik tegevus, tarneahela tõrge, süsteemirikked

23. hea tava. Kaasata müüja/tootja intsidendihaldusesse ja kehtestada konkursikutses selged tingimused.

Hankeetapid: hange, juhtimine

Seotud hankeliigid: meditsiiniseadmed, kliinilise info süsteemid, võrguseadmed, kaugtervishoiusüsteemid, mobiilsed klientseadmed, tuvastussüsteemid, tehnojuhtimissüsteemid, pilveteenused

Seotud ohud: pahatahtlik tegevus, tarneahela tõrge, süsteemirikked

24. hea tava. Kavandada ja jälgida kõigi seadmete hooldustoiminguid, et tagada nende piisav toimivus ja otsustada uuendamine või paikamine.

Hankeetapid: hange, juhtimine

Seotud hankeliigid: kliinilise info süsteemid, võrguseadmed, meditsiiniseadmed, hoonehaldussüsteemid, kaugtervishoiusüsteemid, mobiilsed klientseadmed, tuvastussüsteemid, tehnojuhtimissüsteemid, pilveteenused

Seotud ohud: inimeksimused, süsteemirikked, loodusnähtused

25. hea tava. Kaugjuurdepääsu tuleb minimeerida ja hallata nii, et välissuhtlus tarnijaga piirduks üksnes tema kontrolli all oleva seadmega.

Hankeetapid: hange, juhtimine

Seotud hankeliigid: meditsiiniseadmed, kliinilise info süsteemid, võrguseadmed, kaugtervishoiusüsteemid, mobiilsed klientseadmed, tuvastussüsteemid, tehnojuhtimissüsteemid, pilveteenused

Seotud ohud: pahatahtlik tegevus, tarneahela tõrge, süsteemirikked, inimeksimused

26. hea tava. Nõuda kõigi komponentide paikamist ja lisada see teave konkursikutsesse.

Hankeetapid: hange, juhtimine

Seotud hankeliigid: meditsiiniseadmed, kliinilise info süsteemid, võrguseadmed, kaugtervishoiusüsteemid, mobiilsed klientseadmed, tuvastussüsteemid, tehnojuhtimissüsteemid, pilveteenused

Seotud ohud: pahatahtlik tegevus, tarneahela tõrge, süsteemirikked

27. hea tava. Teadvustada töötajatele küberturvet, et nad tunneksid äsja hangitud toodete või teenuste riske.

Hankeetapid: juhtimine

Seotud hankeliigid: kõik

Seotud ohud: kõik

28. hea tava. Hallata varade loetelu ja konfiguratsiooni, et tagada varaloetelu asjakohane ajakohastamine mis tahes komponendi lisamisel IKT-keskkonda või sealt eemaldamisel ning IKT-komponentide põhiliste turbekonfiguratsioonide olemasolu ja asjakohane haldamine.

Hankeetapid: juhtimine

Seotud hankeliigid: kliinilise info süsteemid, meditsiiniseadmed, võrguseadmed, kaugtervishoiusüsteemid, mobiilsed klientseadmed, tuvastussüsteemid

Seotud ohud: pahatahtlik tegevus, inimeksimused, süsteemirikked

29. hea tava. Luua spetsiaalsed juurdepääsu reguleerimise mehhanismid meditsiiniseadmetega rajatistele, mis peavad olema ka füüsiliselt kaitstud ja juurdepääsuga üksnes eritöötajatele.

Hankeetapid: juhtimine

Seotud hankeliigid: meditsiiniseadmed, hoonehaldussüsteemid, tuvastussüsteemid

Seotud ohud: pahatahtlik tegevus, inimeksimused

30. hea tava. Korraldada sageli või pärast arhitektuuri/süsteemi muutust läbistustestimine ja lisada vastavad tingimused konkursikutsesse.

Hankeetapid: hange, juhtimine

Seotud hankeliigid: meditsiiniseadmed, kliinilise info süsteemid, võrguseadmed, kaugtervishoiusüsteemid, mobiilsed klientseadmed, tuvastussüsteemid, tehnojuhtimissüsteemid, pilveteenused

Seotud ohud: pahatahtlik tegevus, tarneahela tõrge, süsteemirikked