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

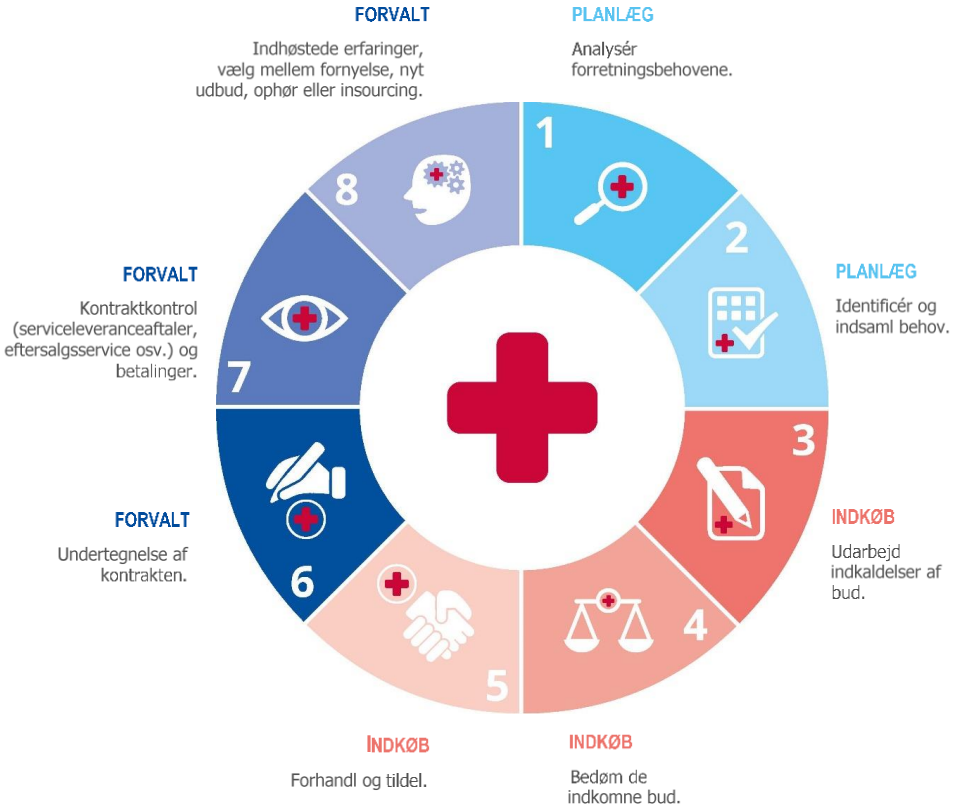
RETNINGSLINJER FOR INDKØB FOR CYBERSIKKERHED PÅ HOSPITALER

Rapporten er udformet som en "håndbog" for sundhedspersoner. Mange af de opstillede praksisser og anbefalinger vil også være nyttige for andre sundhedsorganisationer, da indkøbsprocedurer kan ligne hinanden meget. Rapporten vil være til gavn for sundhedspersonale i tekniske stillinger på hospitaler, dvs. ledere på højt niveau: Investeringschefer (CIO), datasikkerhedsansvarlige (CISO), tekniske chefer (CTO), IT-teams og indkøbere i sundhedsorganisationer. Dette korte dokument gennemgår hovedpunkterne i rapporten — for yderligere detaljer henvises der til ENISA's publikation: ENISA Good Practices for the Security of Healthcare Services, som blev offentliggjort februar 2020.

INDKØBSPROCEDURE

Hospitalers økosystem består af mange forskellige IT-komponenter, og cybersikkerheden bør undersøges særskilt for hver enkelt af dem. Cybersikkerhed bør integreres i alle faser af indkøbsproceduren. I dette afsnit præsenterer vi de trin i indkøbsproceduren, der er fælles for anskaffelse af produkter og tjenesteydelser, herunder medicinsk udstyr, informationssystemer og infrastrukturer.

Figur 1: Indkøbsprocedurens livscyklus for hospitaler



- Planlægningsfasen: Først analyserer hospitalet sine behov og samler behovene fra flere afdelinger internt. Gælder det f.eks. indkøb af en ny cloudtjeneste, bør den tekniske chef fastlægge behovene og sætte sig ind i, hvilke anvendelsesmuligheder tjenesten vil bibringe.

- Indkøbsfasen: Derefter omsættes kravene til tekniske specifikationer, og selve udbudsproceduren iværksættes i samarbejde med indkøbsafdelingen (f.eks. offentliggørelse af et udbud). Hospitalet modtager de designerede bud, og udvalget (herunder den tekniske chef/den IT-sikkerhedsansvarlige og/eller et medlem af IT-teamet) bedømmer buddene og udvælger de bedst egnede produkter. Der forhandles med kontrahenten, og kontrakten tildeles.

- Forvaltningsfasen: Til slut overdrages kontrakten (kontraktforvaltningen og -overvågningen) til den medarbejder, der har ansvaret for aktivitetsområdet på hospitalet. Den pågældende medarbejder er ansvarlig for at afslutte udbudsproceduren og tage imod feedback fra brugerne om udstyrets/systemets/tjenestens faktiske performance.

INDKØBSTYPER FOR HOSPITALER

Tabel 1: Indkøbstyper (klassificering af aktiver)

Indkøbstype	Typebeskrivelse
Kliniske informationssystemer	Omfatter indkøb af software af enhver art til brug i forbindelse med lægebehandling
Medicinsk udstyr	Hardware af enhver art til brug i forbindelse med behandling, regulering eller diagnosticering af sygdomme
Netværksudstyr	Netværkslinjer (koaksiale, optiske), gateways, routere, switches, firewalls, VPN (virtuelle private netværk), IPS (systemer til forebyggelse af indtrængen), IDS (systemer til afsløring af indtrængen) mv.
Fjernbehandlingssystemer	Faciliteter eller udstyr til behandling uden for hospitalsmiljøet, navnlig det, der i dag betegnes "hospitalsbaseret hjemmepleje".
Mobile klientenheder	Software, der yder sundhedsstøtte eller indsamler sundhedsoplysninger og ikke er direkte forbundet med hospitalsnetværket, f.eks. telemedicinske apps
Identifikationssystemer	Systemer, der entydigt identificerer patienter eller sundhedspersonale (biometriske scannere, kortlæsere mv.) og sikrer identifikation og/eller adgangstilladelse til IT-systemerne
Systemer til bygningsforvaltning	Enhver type bygning, der kan rumme hospitalsfaciliteter.
Industrielle kontrolsystemer	Systemer, der styrer alle de fysiske aspekter af centrene, bl.a. strømreguleringssystemer, dørlåsesystemer og sikkerhedssystemer for lukkede kredsløb.
Professionelle tjenester	Alle former for tjenesteydelser, også outsourcede, som ydes af fagfolk eller virksomheder: lægetjenester, transport, bogføring, tekniske tjenester, IT, juridiske tjenester, vedligeholdelse, rengøring, catering mv.
Cloudtjenester	Alle IT-baserede informationssystemer og andre informationssystemer, der ikke er placeret i hospitalsbygningerne eller i et datacenter under fuld kontrol af hospitalets IT-afdeling.

KLASSIFICERING AF TRUSLER

Der er forskellige indkøbstyper knyttet til forskellige trusler mod et hospitals IKT-miljø. Gennemgå trusselsklassificeringen, som præsenteres i dette afsnit, sammen med din IT-, sikkerheds- eller risikoafdeling for at fastlægge, hvilke trusler der er mest relevante for din organisation. Denne aktivitet bør være en del af IT-opgaverne på hospitalet, uanset indkøbspotentialet.

Tabel 2: Trusselstyper (trusselsklassificering)

Trussel	Eksempler
Naturkatastrofer	Brand, oversvømmelse og jordskælv
Svigt i leverandørkæden	Manglende levering fra cloudtjenesteudbydere og netværksleverandører, strømsvigt, manglende levering eller manglende overholdelse fra producenter af medicinsk udstyr
Menneskelige fejl	Konfigurationsfejl i medicinske systemer, manglende revisionslog, manglende eller svigtende processer til kontrol med uautoriseret adgang, manglende overensstemmelse af BYOD-enheder ("Bring Your Own Device"), fejl fra sundhedspersonales/patienters side
Ondsindede angreb	Malware (virus, ransomware (afpresningsprogrammer), BYOD), hijacking (kryptojacking (kapring for at generere kryptovaluta) og medjacking (kapring af medicinsk udstyr)), social manipulation (phishing (webfiskeri efter adgangskoder), baiting (franarring med "madding") og enhedskloning (device cloning)), tyveri af data eller udstyr, manipulation af medicinsk udstyr, skimming (ulovlig kopiering), denial-of-service (servicenægtelse), angreb på webbaserede applikationer, interne trusler, fysisk manipulation/beskadigelse, identitetstyveri, cyberspionage, mekanisk afbrydelse af komponenter
Systemfejl	Softwarefejl, forældet firmware, enhedssvigt, netværkskomponentsvigt, utilstrækkelig vedligeholdelse

GOD PRAKSIS FOR CYBERSIKKERHED VED INDKØB

Følgende liste over god praksis er på ingen måde udtømmende, men den er særdeles nyttig for den sundhedsteknologiske IT-medarbejder, der har ansvar for indkøb af udstyr på et hospital. Listen er det samlede resultat af al input fra de interviewede sundhedspersoner. Læseren kan tilpasse listen efter sin organisations prioriteter.

GOD PRAKSIS 1. Inddrag IT-afdelingen i de forskellige indkøbsfaser for at sikre, at der tages højde for ekspertviden inden for cybersikkerhed.

Indkøbsfaser: Alle

Relaterede indkøbstyper: Alle

Relaterede trusler: Alle

GOD PRAKSIS 2. Implementér en proces for sårbarhedsidentifikation og -styring, der sikrer, at sårbarheder tages i betragtning, før der indkøbes nye produkter eller tjenester, og at sårbarheder i eksisterende produkter/tjenester overvåges i hele deres livscyklus.

Indkøbsfaser: Alle

Relaterede indkøbstyper: Kliniske informationssystemer, medicinsk udstyr, netværksudstyr, fjernbehandlingssystemer, mobile klientenheder, identifikationssystemer, industrielle kontrolsystemer, cloudtjenester

Relaterede trusler: Alle

GOD PRAKSIS 3. Fastlæg en politik for hardware- og softwareopdatering, der sikrer, at de seneste patches til dit operativsystem og din software bliver taget i brug, og at antivirussoftwaren er ajour.

Indkøbsfaser: Alle

Relaterede indkøbstyper: Medicinsk udstyr, kliniske informationssystemer, netværksudstyr, fjernbehandlingssystemer, mobile klientenheder, identifikationssystemer, industrielle kontrolsystemer, cloudtjenester

Relaterede trusler: Ondsindede angreb, svigt i leverandørkæden, systemsvigt

GOD PRAKSIS 4. Forbedr sikkerhedskontrollen for trådløs kommunikation, så adgangen til hospitalets wi-fi-netværk er begrænset og strengt kontrolleret.

Indkøbsfaser: Alle

Relaterede indkøbstyper: Medicinsk udstyr, klienters fjernenheder, identifikationssystemer, cloudtjenester

Relaterede trusler: Ondsindede angreb, menneskelige fejl

GOD PRAKSIS 5. Fastlæg politikker for afprøvning, der sikrer, at nyerhvervede eller nykonfigurerede produkter penetrationstestes, og at der træffes afhjælpende foranstaltninger i overensstemmelse med de operationelle parametre for det faktiske miljø.

Indkøbsfaser: Alle

Relaterede indkøbstyper: Kliniske informationssystemer, medicinsk udstyr, netværksudstyr, fjernbehandlingssystemer, mobile klientenheder, identifikationssystemer, systemer til bygningsforvaltning, industrielle kontrolsystemer, cloudtjenester

Relaterede trusler: Ondsindede angreb, systemsvigt, menneskelige fejl

GOD PRAKSIS 6. Udarbejd planer for forretningskontinuitet, der sikrer, at et systemsvigt ikke medfører afbrydelse i hospitalets kerneydelser, og at leverandørens rolle er veldefineret.

Indkøbsfaser: Alle

Relaterede indkøbstyper: Medicinsk udstyr, kliniske informationssystemer, netværksudstyr, fjernbehandlingssystemer, mobile klientenheder, identifikationssystemer, industrielle kontrolsystemer, cloudtjenester

Relaterede trusler: Ondsindede angreb, svigt i leverandørkæden, systemsvigt

GOD PRAKSIS 7. Tag hensyn til interoperabilitetsproblemer, så der undgås sikkerhedsmangler ved de eksisterende IT-komponenter.

Indkøbsfaser: Alle

Relaterede indkøbstyper: Kliniske informationssystemer, medicinsk udstyr, fjernbehandlingssystemer, mobile klientenheder, identifikationssystemer, industrielle kontrolsystemer, cloudtjenester

Relaterede trusler: Systemfejl, menneskelige fejl, ondsindede angreb

GOD PRAKSIS 8. Muliggør afprøvning af alle komponenter med henblik på at sikre, at de yder det, der er lovet: efterprøv brugervenligheden, kontrollér korrektheden af resultaterne under belastning, og kontrollér for sikkerhedsmangler (politik for svage adgangskoder, angreb på databaser (SQL-injection).

Indkøbsfaser: Alle

Relaterede indkøbstyper: Kliniske informationssystemer, medicinsk udstyr, klienters fjernenheder, identifikationssystemer, cloudtjenester, industrielle kontrolsystemer, fjernbehandlingssystemer, systemer til bygningsforvaltning, mobile klientenheder

Relaterede trusler: Ondsindede angreb, menneskelige fejl, systemfejl, svigt i leverandørkæden

GOD PRAKSIS 9. Muliggør revision og logning med henblik på at spore angribere og anslå omfanget af mistede/stjålne oplysninger, hvis systemet kompromitteres.

Indkøbsfaser: Alle

Relaterede indkøbstyper: Medicinsk udstyr, fjernbehandlingssystemer, mobile klientenheder, identifikationssystemer, industrielle kontrolsystemer

Relaterede trusler: Ondsindede angreb, svigt i leverandørkæden, systemsvigt

GOD PRAKSIS 10. Kryptér følsomme personoplysninger, som er i hvile eller under videregivelse, ved at fastlægge en politik for systemer, tjenester og

enheder, der behandler særlige kategorier af personoplysninger i henhold til databeskyttelsesforordningens artikel 9.

Indkøbsfaser: Alle

Relaterede indkøbstyper: Medicinsk udstyr, kliniske informationssystemer, netværksudstyr, fjernbehandlingssystemer, mobile klientenheder, identifikationssystemer, industrielle kontrolsystemer, cloudtjenester

Relaterede trusler: Ondsindede angreb, svigt i leverandørkæden, systemsvigt

GOD PRAKSIS 11. Foretag en risikovurdering som led i indkøbsproceduren.

Indkøbsfaser: Planlæg

Relaterede indkøbstyper: Alle

Relaterede trusler: Alle

GOD PRAKSIS 12. Planlæg netværks-, hardware- og licensbehov på forhånd med henblik på, om der skal foretages yderligere opgraderinger og/eller indkøb, for at det nye system kan installeres.

Indkøbsfaser: Planlæg

Relaterede indkøbstyper: Kliniske informationssystemer, netværksudstyr, identifikationssystemer, industrielle kontrolsystemer.

Relaterede trusler: Svigt i leverandørkæden, systemfejl, naturkatastrofer, menneskelige fejl

GOD PRAKSIS 13. Identificer trusler relateret til produkter eller tjenesteydelser, der skal indkøbes, og sørg for løbende trusselsidentifikation i hele indkøbscyklussen.

Indkøbsfaser: Planlæg, forvalt

Relaterede indkøbstyper: Alle

Relaterede trusler: Alle

GOD PRAKSIS 14. Opdel dit netværk, så trafikken på det kan isoleres og/eller filtreres med henblik på at begrænse og/eller hindre adgang mellem netværksområder.

Indkøbsfaser: Planlæg, indkøb

Relaterede indkøbstyper: Medicinsk udstyr, kliniske informationssystemer, netværksudstyr, fjernbehandlingssystemer, mobile klientenheder, identifikationssystemer, industrielle kontrolsystemer, cloudtjenester

Relaterede trusler: Ondsindede angreb, svigt i leverandørkæden, systemsvigt

GOD PRAKSIS 15. Fastsæt netværkskrav med henblik på at sikre interoperabilitet og undgå mangler efter fastlæggelsen af netværks- og komponenttopologien.

Indkøbsfaser: Planlæg

Relaterede indkøbstyper: Kliniske informationssystemer, netværksudstyr, identifikationssystemer, industrielle kontrolsystemer, cloudtjenester, fjernbehandlingssystemer, mobile klientenheder.

Relaterede trusler: Svigt i leverandørkæden, systemfejl, naturkatastrofer

GOD PRAKSIS 16. Fastsæt grundlæggende sikkerhedskrav, og omsæt dem til udvælgelseskriterier ved valget af leverandører.

Indkøbsfaser: Planlæg, indkøb

Relaterede indkøbstyper: Medicinsk udstyr, kliniske informationssystemer, netværksudstyr, fjernbehandlingssystemer, mobile klientenheder, identifikationssystemer, industrielle kontrolsystemer, cloudtjenester

Relaterede trusler: Ondsindede angreb, svigt i leverandørkæden, systemsvigt

GOD PRAKSIS 17. Lav en dedikeret indkaldelse af bud ved indkøb af cloudtjenester under hensyntagen til regulatoriske krav og politikkrav.

Indkøbsfaser: Planlæg, indkøb

Relaterede indkøbstyper: Cloudtjenester

Relaterede trusler: Ondsindede angreb, svigt i leverandørkæden

GOD PRAKSIS 18. Prioritér indkøb af aktiver, der er certificeret ud fra cybersikkerhedsordninger/-standarder.

Indkøbsfaser: Indkøb

Relaterede indkøbstyper: Medicinsk udstyr, kliniske informationssystemer, netværksudstyr, fjernbehandlingssystemer, mobile klientenheder, identifikationssystemer, industrielle kontrolsystemer, cloudtjenester

Relaterede trusler: Ondsindede angreb, svigt i leverandørkæden, systemsvigt

GOD PRAKSIS 19. Foretag konsekvensanalyser af databeskyttelse ved planlægningen af indkøb af et nyt system eller en ny tjeneste.

Indkøbsfaser: Indkøb

Relaterede indkøbstyper: Kliniske informationssystemer, medicinsk udstyr, netværksudstyr, fjernbehandlingssystemer, mobile klientenheder, identifikationssystemer, professionelle tjenester, cloudtjenester

Relaterede trusler: Ondsindede angreb, menneskelige fejl

GOD PRAKSIS 20. Opret gateways, der opretholder forbindelsen med eksisterende systemer/maskiner, og sørg for grænsekontrol i tilfælde af problemer inde i disse grupper.

Indkøbsfaser: Indkøb, forvalt

Relaterede indkøbstyper: Medicinsk udstyr, fjernbehandlingssystem, mobile klientenheder, identifikationssystemer, industrielle kontrolsystemer

Relaterede trusler: Ondsindede angreb, svigt i leverandørkæden, systemsvigt

GOD PRAKSIS 21. Giv cybersikkerhedskurser i organisationens sikkerhedspraksis for at sikre tilstrækkelig uddannelse af internt personale og eksterne kontrahenter/konsulenter, der arbejder på stedet.

Indkøbsfaser: Indkøb, forvalt

Relaterede indkøbstyper: Alle

Relaterede trusler: Ondsindede angreb, menneskelige fejl

GOD PRAKSIS 22. Udarbejd beredskabsplaner for hændelser, der omfatter nyerhvervede produkter eller systemer.

Indkøbsfaser: Indkøb, forvalt

Relaterede indkøbstyper: Medicinsk udstyr, kliniske informationssystemer, netværksudstyr, fjernbehandlingssystemer, mobile klientenheder, identifikationssystemer, industrielle kontrolsystemer, cloudtjenester

Relaterede trusler: Ondsindede angreb, svigt i leverandørkæden, systemsvigt

GOD PRAKSIS 23. Inddrag sælger/producent i at håndtere hændelser og opstil klare betingelser i udbuddet.

Indkøbsfaser: Indkøb, forvalt

Relaterede indkøbstyper: Medicinsk udstyr, kliniske informationssystemer, netværksudstyr, fjernbehandlingssystemer, mobile klientenheder, identifikationssystemer, industrielle kontrolsystemer, cloudtjenester

Relaterede trusler: Ondsindede angreb, svigt i leverandørkæden, systemsvigt

GOD PRAKSIS 24. Planlæg og overvåg vedligeholdelsen af alt udstyr med henblik på at sikre et tilstrækkeligt funktionsniveau, og træf afgørelse om opdateringer/patches osv.

Indkøbsfaser: Indkøb, forvalt

Relaterede indkøbstyper: Kliniske informationssystemer, netværksudstyr, medicinsk udstyr, systemer til bygningsforvaltning, fjernbehandlingssystemer, mobile klientenheder, identifikationssystemer, industrielle kontrolsystemer, cloudtjenester

Relaterede trusler: Menneskelig fejl, systemfejl, naturkatastrofer

GOD PRAKSIS 25. Fjernadgang bør minimeres og administreres på en måde, så ekstern kommunikation med leverandøren begrænses alene til den enhed, leverandøren skal kontrollere.

Indkøbsfaser: Indkøb, forvalt

Relaterede indkøbstyper: Medicinsk udstyr, kliniske informationssystemer, netværksudstyr, fjernbehandlingssystemer, mobile klientenheder, identifikationssystemer, industrielle kontrolsystemer, cloudtjenester

Relaterede trusler: Ondsindede angreb, svigt i leverandørkæden, systemsvigt, menneskelige fejl

GOD PRAKSIS 26. Kræv patching for alle komponenter, og medtag oplysninger herom i indkaldelsen af bud.

Indkøbsfaser: Indkøb, forvalt

Relaterede indkøbstyper: Medicinsk udstyr, kliniske informationssystemer, netværksudstyr, fjernbehandlingssystemer, mobile klientenheder, identifikationssystemer, industrielle kontrolsystemer, cloudtjenester

Relaterede trusler: Ondsindede angreb, svigt i leverandørkæden, systemsvigt

GOD PRAKSIS 27. Styrk personalets kendskab til cybersikkerhed, så det er klar over risiciene ved nyerhvervede produkter eller tjenester.

Indkøbsfaser: Forvalt

Relaterede indkøbstyper: Alle

Relaterede trusler: Alle

GOD PRAKSIS 28. Opstil en liste over aktiver og foretag en konfigurationsstyring, der sikrer, at listen bliver korrekt ajourført, når der tilføjes eller fjernes komponenter i IKT-miljøet, at der forefindes basiskonfigurationer for sikkerheden af IKT-komponenterne, og at de forvaltes hensigtsmæssigt.

Indkøbsfaser: Forvalt

Relaterede indkøbstyper: Kliniske informationssystemer, medicinsk udstyr, netværksudstyr, fjernbehandlingssystemer, mobile klientenheder, identifikationssystemer

Relaterede trusler: Ondsindede angreb, menneskelige fejl, systemfejl

GOD PRAKSIS 29. Indfør særlige adgangskontrolsystemer for faciliteter med medicinsk udstyr, som også bør være fysisk beskyttet og kun tilgængeligt for specialiseret personale.

Indkøbsfaser: Forvalt

Relaterede indkøbstyper: Medicinsk udstyr, systemer til bygningsforvaltning, identifikationssystemer

Relaterede trusler: Ondsindede angreb, menneskelige fejl

GOD PRAKSIS 30. Skemalæg penetrationstests (simulerede angreb), så de udføres hyppigt eller efter arkitektur-/systemændringer, og anfør betingelserne i indkaldelsen af bud.

Indkøbsfaser: Indkøb, forvalt

Relaterede indkøbstyper: Medicinsk udstyr, kliniske informationssystemer, netværksudstyr, fjernbehandlingssystemer, mobile klientenheder, identifikationssystemer, industrielle kontrolsystemer, cloudtjenester

Relaterede trusler: Ondsindede angreb, svigt i leverandørkæden, systemsvigt