



Tarkistuslista kyberturvallisuuskävelyn tueksi

Huomiona, että käveltävät kohteet ja yksiköt voivat olla hyvin erilaisia, joten tarkistuslista on tarvittaessa räätälöitävä omaan yksikköön sopivaksi. Kyberturvallisuuskävelyn ohjeet suositellaan kertaamaan ennen kävelyn aloittamista.

Kävelyn voi aloittaa esimerkiksi osaston/yksikön pääovilta, jossa voidaan tarkastella seuraavia asioita:

Pääovi ja kulkureitit tiloihin

- Onko osastolle/yksikköön johtavien ovien tarkoitus olla lukossa?
- Jos kyllä, keillä kaikilla on kulkuoikeus ovista? Entä kuinka sisään päästettävät vierailijat otetaan vastaan: Tarkistetaanko rutiininomaisesti, kuka henkilö on ja millä asialla? Tarkistetaanko vierailija- tai henkilökortit ja onko tähän tarvetta?
- Jos ei, onko kulkureiteille näkyvyys (esim. kamerayhteys kansliaan)? Näemmekö ja tiedämmekö, keitä ovesta kulkee? Pitäisikö/tarvitseeko meidän tietää?
- Pohtikaa kävelijöiden kanssa, mihin kaikkialle esimerkiksi heidän omilla avaimillaan voisi päästä myös oman osaston/yksikön ulkopuolella, jos ne päätyisivät väärin käsiin. Entä tunnistekortilla.

Huomiot:

Laitteet

Kiinnittäkää kävellessänne huomiota kaikissa kiertämissänne tiloissa havaitsemiinne laitteisiin ja tarkastelkaa niitä:

- Tiedätkö, ovatko ne päivitettyjä ja kuka päivityksistä vastaa?
- Onko laitteissa organisaation tunnistetarrat?
- Tutki, onko laitteisiin mahdollista liittää ulkoisia laitteita, kuten USB-muistitikkuja huomaamatta?
- Löytyykö laitteiden läheisyydestä kirjautumistietoja?
- Kuinka työpisteiden näytöt on aseteltu? Voiko ulkopuolinen nähdä näytöille? Onko tietokoneissa käytössä näytönsuojakalvo?
- Mitkä ovat käytännöt henkilöstön omien laitteiden käytölle ja noudatetaanko niitä (esim. omien puhelinten lataaminen tietokoneen USB-portista tai omat muistitikut)?

Huomiot:



Käytävät, asiakastilat ja asiakas-/potilashuoneet

Tarkastelkaa esimerkiksi seuraavia asioita:

- Löydätkö tiloista valvomattomia laitteita, joiden ei kuuluisi olla siellä (esim. verkkoon kytkettävät lääkinälliset laitteet, liikuteltavat työasemat, tunnistamattomat laitteet)?
- Millainen on näkyvyys tiloihin, joissa käsitellään arkaluontoista tietoa (esim. kanslian luukulta)? Voitte myös kuulostella tilojen äänieristystä ja havainnoida, ovatko jotkin tilat sopimattomia esimerkiksi raportin antoon.
- Kaapit asiakkaiden/potilaiden henkilökohtaisille tavaroille: ovatko kaapit lukittavat, ovatko lukot ehjiä?
- Havainnoi kävellessäsi löytyykö tiloista unohtuneita dokumentteja, henkilötietoja tai henkilöstön tavaroita tms. kuten unohtuneita muistilappuja, laboratoriotarroja, henkilö- ja varmennekortteja, kirjautumistunnuksia.
- Käykää keskustellen läpi, miten toimisitte, jos yleisistä tiloista, asiakastiloista tai asiakas-/potilashuoneista löytyisi epäilyttävä ulkopuolinen laite, kuten muistitikku, älypuhelin, tabletti tms. Tietääkö henkilöstö, kuinka tällöin toimitaan?

Huomiot:

Varastot, välinehuoltotilat, siivouskaapit

- Mikäli tilat ovat lukitsemattomia, tarkastele löytyykö niistä henkilöstön unohtuneita tavaroita, henkilötietoja, työvuorolistoja, muistilappuja, organisaation omia laitteita tai epäilyttäviä ulkopuolisia laitteita.
- Säilytetäänkö tiloissa organisaation laitteita, joihin ulkopuolinen voi päästä käsiksi ja voisiko tämä olla kyberturvallisuusriski?

Huomiot:

Henkilöstön työtilat, vastaanottohuoneet sekä taukotilat

- Jos osastolla/yksikössä on vastaanotto- tai työhuoneita (esim. lääkärin, osastonhoitajan, sosiaalityöntekijän), onko näihin valvomon pääsy? Jos on, voiko huoneesta löytää henkilötietoja tai muuta arkaluontoista tietoa, kirjautumistunnuksia, lukitsemattomia tietokoneita, henkilöstön tavaroita kuten avaimia, puhelimia tai varmennekortteja?
- Tarkastele henkilöstön työtilojen tietosuojaa: tietokoneiden näyttöjen asettelu ja lukitsemiskäytännöt, suojakalvojen käyttö, asiakas-/potilastaulujen näkyvyys, muistilaput, joissa asiakas- tai kirjautumistietoja, valvomattomat avaimet ja varmennekortit. Tarkastele myös, voisiko tilaan nähdä ulkoikkunoista.
- Kurkkaa myös tilojen roskakoreihin, löytyykö sieltä roskia, jotka kuuluisivat tietosuojaroskikseen?
- Onko henkilökunnan taukotiloihin valvomon pääsy? Tarkastele löytyykö taukotiloista sinne kuulumattomia tavaroita tai asiakas-/potilastietoja.
- Tarkastelkaa myös tilojen äänieristystä ja pohtikaa, millaisia keskusteluja tiloissa käydään. Ovatko tilat soveltuvia esimerkiksi raportin antamiseen? Huolehditäänko ovet kiinni, kun keskustellaan asiakas-/potilasasioista?

Huomiot:

Mahdolliset muut toiminnot ja niiden riskit

- Pohdi, onko tunnistettavissa muita toimintoja, joissa kyberturvallisuus voi olla vaarassa tai arkaluontoista tietoa päätyä väärin käsiin (esim. asiakas-/potilastavaroiden säilytys ja kuljetus yksiköiden välillä, näytteidenotto toiminta tms.).

Huomiot: