

Kyberturvallisuuskävely riskien havaitsemiseksi sote-yksikössä



Kyberturvallisuuskävelyn tarkoitus on hoksauttaa sosiaali- ja terveysalan ammattilaisia fyysisen työympäristönsä ja oman toimintansa mahdollisista kyberturvallisuusriskeistä, jotka voivat helposti jäädä huomaamatta työarjen vilkskeessä. Toisaalta kyberturvallisuuskävelyt auttavat tuomaan näkyväksi ne asiat, joissa toimitaan jo hyvin! Säännöllisillä kyberturvallisuuskävelyillä havaitaan ne työarjessa esiintyvät riskit, jotka vaativat toimenpiteitä, sekä seurataan toimenpiteiden toteutumista. Kyberturvallisuuskävelyt vahvistavat organisaation turvallisuuskulttuuria.

Vinkki: KyberSoTe-projektissa kyberturvallisuuskävelyn tarkistuslistan mallia voi hyödyntää käveltävän reitin ja tarkistettavien kohteiden suunnittelussa sekä kävelyn aikana tarkistuslistana ja muistin tukena. Käveltävät kohteet ja yksiköt voivat kuitenkin olla hyvin erilaisia, joten tarkistuslista on tarvittaessa räätälöitävä omaan yksikköön sopivaksi.

► Kyberturvallisuuskävelyn toteuttaminen

1. Suunnittelu

Tavoite: Kyberturvallisuusriskien tunnistaminen ja arviointi, tietoisuuden lisääminen ja työympäristön sekä toimintatapojen kehittäminen kyberturvallisemmaksi. Toimivien ja kyberturvallisuutta edistävien jo olemassa olevien käytäntöjen ja toimintamallien näkyväksi tekeminen.

Osallistujat: Suunnittele osallistujat. Kyberkävely työkaluna on ensisijaisesti suunnattu organisaation kyberagentin roolissa toimiville henkilöille. Kyberagentit voivat suorittaa kävelyn itsenäisesti tai mahdollisuuksien mukaan yksikön esihenkilön ja/tai organisaation tietoturvan asiantuntijan kanssa. Kyberagentit voivat hyödyntää tätä kyberturvallisuuskävelyn runkoa myös fasilitoidakseen kävelyitä yksikön muulle henkilöstölle.

Reitti: Määritä tarvittaessa alue, joka kävellään, sekä reitti. Käveltävä alue voi olla koko osasto/yksikkö, tai vain tietyt osat siitä.

Aikataulu: Sovi aikataulu kävelylle. Kävelyyn on hyvä varata käveltäväksi suunnitellun alueen koko huomioiden noin 30–60 minuuttia. Huomaa varata aikaa havaintojen koonnille ja raportoinnille kävelyn jälkeen.

Valmistelu: Kokoa mahdolliset aiempien kävelyiden dokumentit havainnoista ja niiden perusteella suunnitelluista toimenpiteistä. Varaa muistiinpanovälineitä ja tarkistuslista.





2. Kävelyn suorittaminen

Orientaatio: Jos kävely suoritetaan ryhmässä, muistutetaan mieleen kävelyn tavoitteet ja suunnitelma; käydään läpi, mikä alue kävellään ja ohjeistetaan kävelyllä tehtyjen huomioiden kirjaus ja purkaminen kävelyn päätteeksi. On hyvä muistuttaa osallistujia kirjaamaan ylös myös positiivisia huomioita asioista, jotka ovat jo hyvin.

Kyberturvallisuuskävely ja ympäristön havainnointi: Kävellään suunniteltu reitti rauhallisesti ja mahdollisen ryhmän kanssa keskustellen. Tehdään edetessä muistiinpanoja huomioista.

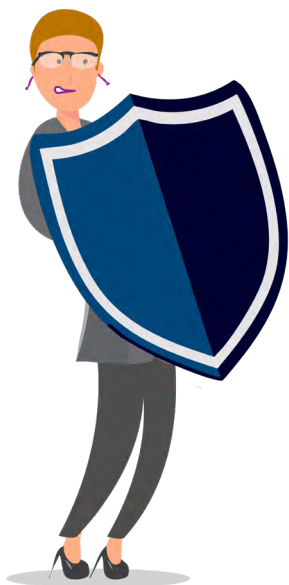
3. Yhteenveto, raportointi ja seuranta

Huomioiden koonti ja analysointi: Kävelyn päätteeksi kootaan havainnot yhteen. Jaotellaan huomiot riskeihin, jotka vaativat välittömiä toimenpiteitä, kehityskohteisiin ja asioihin, jotka ovat hyvin. Tässä kohtaa on hyvä myös pohtia mahdollisia ratkaisuja ja kehitysehdotuksia.

Raportointi ja palaute: Kyberagentti raportoi kootuista huomioista yksikön johdolle, jonka vastuulla on suunnitella jatkotoimenpiteet. Kyberagentti raportoi huomioista myös henkilöstölle esimerkiksi tiimipalaverissa tai osastokokouksessa. On tärkeää kiittää henkilöstöä niistä asioista ja toimintatavoista, joissa on onnistuttu hyvin kyberturvallisuuden näkökulmasta.

Toimenpiteet ja seuranta: Toteutetaan yksikön johdon linjaamia toimenpiteitä ja kehitystoimia havaittujen riskien ja kehityskohteiden korjaamiseksi. Sovitaan seuraavan kyberturvallisuuskävelyn ajankohta, jolloin kiinnitetään tarkistuslistan kohtien lisäksi huomiota toimenpiteiden ja kehitystoimien toteutumiseen.

► Vaihtoehtoinen toteutustapa kokoneemmille ryhmille:



Kun kyberturvallisuuskävelystä on tullut tuttu ja kävelijät osaavat jo omatoimisesti kiinnittää huomiota mahdollisiin kyberturvallisuushälytyksiin, voidaan kävelystä suorittaa haastavampi versio. Tässä versiossa kävelijät asettuvat kyberrikollisen rooliin ja pyrkivät löytämään ympäristöstä haavoittuvuuksia, joita hyödyntämällä voisi päästä käsiksi arkaluontoiseen tietoon, kirjautumistietoihin tai tiloihin, joihin heillä ei pitäisi ulkopuolisina olla pääsyä. Kyberrikollisen roolissa vain mielikuvitus on rajana ja keinot hyödyntää haavoittuvuuksia saavat olla erikoisiakin*. Kävelyn jälkeen voidaan pohtia yhdessä, olisivatko keksityt skenaariot oikeasti mahdollisia.

***Esimerkki. Kansliaan voisi mahdollisesti päästä aiheuttamalla yhteen tai useampaan asiakas-/potilashuoneeseen hälytyksen tai osastolle palohälytyksen, joka saa henkilökunnan kansliassa liikkeelle. Aiheutuneessa hälyssä joku voi ehtiä saamaan jalan sulkeutuvan kanslian oven väliin ja päästä kansliaan.**