HE 63/2024 Lausunto

Etäyhteyksien käytön edistämistä oikeudenkäynneissä

Antti Laatikainen

Johtava tietoturvakonsultti, WithSecure Consulting

Taustoitusta muistiosta

- Nykyajan digitalisaatio muokkaa yhteiskuntaamme ja vaikuttaa kaikkiin elämänalueisiin, mukaan lukien oikeuskäytännöt. Teknologian kehitys tuo mukanaan joustoa, mutta myös uusia uhkia ja riskejä, jotka vaativat huolellista harkintaa
- Oikeudenkäynnit ovat oikeusvaltion perusta, ja niihin liittyy vahvoja odotuksia arvokkuudesta, perinteistä, sääntöjenmukaisuudesta ja luotettavuudesta. Asianomaisen kokemukseen vaikuttaa suuresti, miten käsittelyprosessi on toteutettu ja miten hän kokee tulevansa kuulluksi ja kohdatuksi.
- WithSecuren lausunto käsittelee teknisen tietoturvan, tietojärjestelmien käytettävyyden ja toimintaan liittyvän riskienhallinnan näkökulmia.



Sisällys

- Päätelaitteiden tietoturva ja luotettavuus
- Video- ja äänivirran kiistämättömyys
- Tilaturvallisuus ja vaikuttamisen estäminen
- Riskienhallinta ja tekninen ymmärrys
- Yhteensopivuus ja käytettävyys



Päätelaitteiden tietoturva ja luotettavuus

Yksityisten henkilöiden omistamien päätelaitteiden tietoturvallisuutta ei voida taata, mikä heikentää oikeudenkäyntiin osallistujan tunnistautumisen luotettavuutta ja lisää salakuuntelun sekä luvattoman tallentamisen riskiä.

WithSecuren suosittelee videoyhteyden yli oikeuden istuntoon osallistumisen sallimista toimintamallin ensivaiheessa vain viranomaisten hyväksymillä ja ylläpitämillä ratkaisuilla.







Video- ja äänivirran kiistämättömyys

Yksityisten laitteiden video- ja äänivirran kiistämättömyyttä ei voida taata ilman erityisiä prosesseja.

Tekoälyn avulla voidaan jo nyt muokata ja väärentää kuvaa ja ääntä, mikä vaikeuttaa luotettavaa todentamista.

Deep fake -huijausten tai generatiivisella tekoälyllä toteutettujen video- tai ääniyhteyksien väärentämisen tunnistamiseen ei ole vielä luotettavia teknisiä ratkaisuja.



Tilaturvallisuus ja vaikuttamisen estäminen

Etänä tapahtuvan lausunnon antamisen tilaturvallisuutta ei voida taata, sillä henkilö voi olla painostuksen tai uhkailun kohteena.

Fyysisessä istuntosalissa tällaisen vaikuttamisen mahdollisuus on helpompi minimoida







Riskienhallinta ja tekninen ymmärrys

Etäyhteyden turvallisuuden, käytettävyyden ja soveltuvuuden varmistamiseksi on tärkeää, että harkintaa toteuttavilla henkilöillä on tekninen ymmärrys videoneuvottelun riskeistä ja uhista.

Turvallisten laitteiden saatavuus tulee suunnitella tasa-arvoisesti, niin että tarveharkinta on sama kaikille, eikä sitä ohjaa kustannustehokkuus tai helppous.

WithSecure suosittelee kattavia ja uhkamallinnukseen perustuvia toimintaohjeita tarveharkinnan tueksi.



Yhteensopivuus ja käytettävyys

Suunniteltaessa etäosallistumista tulee huomioida muiden viranomaisten tarpeet ja harmonisoida laitteistot ja toimintatavat.

Järjestelmien käytön helppous ja saatavuus vaikuttavat kansalaisten vastaanottoon ja yleiseen mielipiteeseen.








WITH®
secure