Aloita visuaalisen tietosuojakäytännön kehittäminen

Tekniikan kehityksen myötä työtä tehdään yhä useammin julkisissa tiloissa, ja tietoturvaa ja tietosuojaa koskevan säätelyn määrä kasvaa. Organisaatioiden on nyt entistä tärkeämpää laatia käytännöt, joilla puututaan visuaalisen hakkeroinnin muodostamaan uhkaan.

Olemme laatineet yrityksille oheisen Visuaalisen tietosuojavalmiuden tarkistuslistan, jonka avulla ne voivat tiedottaa henkilöstölleen paremmin visuaalisesta hakkeroinnista sekä visuaalisen tietosuojan merkityksestä. Tavoitteena on pitää yksityiset, luottamukselliset ja arkaluontoiset tiedot poissa näkyviltä, jolloin ne eivät altistu visuaaliselle hakkeroinnille.

Visuaalisen tietosuojavalmiuden tarkistuslista

Visuaalisen tietosuojavalmiuden tarkistuslistassa käydään läpi kolme keskeistä osa-aluetta: visuaalisen hakkeroinnin uhasta sekä visuaalisen tietosuojan merkityksestä tiedottaminen henkilöstölle, käytäntöjen luominen ongelmiin puuttumiseksi sekä ratkaisujen ja ehdotusten tarjoaminen rikkomusten estämiseksi.

√ Aloita henkilöstön kouluttaminen.

❑ Sisällytä tietoturvakoulutukseen visuaalista tietosuojaa ja visuaalista hakkerointia koskevat moduulit.

❑ Ota visuaalista tietosuojaa ja visuaalista hakkerointia koskeva koulutus osaksi uusien työntekijöiden perehdytystä.

❑ Järjestä ylimmälle johdolle sekä riskeille alttiille työntekijöille erillinen visuaalista tietosuojaa ja visuaalista hakkerointia koskeva koulutus.

√ Laadi asianmukaiset käytännöt.

❑ Tunnista riskeille alttiit työntekijät seuraavien ehtojen mukaan:

- matkustustarve (esim. liike- ja työmatkat)
- käsiteltävien tietojen arkaluontoisuus (esim. rahoitustiedot, henkilöstötiedot tai asiakastiedot)
- toimiston ulkopuoliseen työskentelyyn käytetty aika (sähköpostin ja muiden viestien käyttö, arkaluontoisten tietojen käsittely)
- organisaatiotaso (liikesalaisuuksia tai luottamuksellisia tietoja käsittelevä ylin johto voi olla alttiina riskeille).

❑ Vaadi tietoturvasuojien käyttöä:

- toimiston sisällä kaikissa laitteissa, joilla riskeille alttiit työntekijät käsittelevät arkaluontoisia tietoja (kuten henkilöstö- ja asiakastietoja)
- kaikissa laitteissa, joilla arkaluontoisia tietoja käsitellään julkisissa tiloissa (esim. luottamukselliset potilas- tai asiakastiedot)
- kaikissa laitteissa, joita työntekijät käyttävät toimiston ulkopuoliseen työskentelyyn.

❑ Estä tarvittaessa työskentely vilkkaissa korkean riskin kohteissa (esim. liikennevälineet, ravintolat ja kahvilat).

❑ Valvo, että työntekijät noudattavat puhtaan pöydän periaatetta, eli että he sammuttavat näytöt eivätkä jätä asiakirjoja näkyviin poistuessaan työpisteeltä.

❑ Määritä sovellukset piilottamaan korkean riskin tiedot urkinnalta seuraavilla tavoilla (vaihtoehdot on lueteltu vahvimmasta heikoimpaan):

- Syötteen ja sen pituuden piilottaminen.
- Syötteen piilottaminen merkki kerrallaan (esim. mobiililaitteilla salasanojen syöttämisen yhteydessä).
- Syötteen piilottaminen vain aktiivisissa tietokentissä.

√ Varmista vaatimusten noudattaminen tarjoamalla ratkaisuja

❑ Hanki tietoturvasuojat kaikkiin kannettaviin laitteisiin (esim. kannettavat tietokoneet, tabletit ja älypuhelimet), joilla käytetään arkaluontoisia tietoja julkisissa tiloissa.

❑ Käytä tietoturvasuojia näytöissä, joilla käytetään luottamuksellisia tietoja työpaikan sisällä.

❑ Käytä aikakatkaisuja ja näytönsäästäjiä kannettavissa ja pöytätietokoneissa valvomattomien näyttöjen visuaalisen tietosuojan parantamiseksi.