Suojaudu sosiaaliselta hakkeroinnilta

Yritysvakoilun ja organisaatioihin tietoverkkojen kautta kohdistuvan rikollisen toiminnan lisääntyessä pyrkivät rikolliset tahot saamaan haltuunsa organisaatioiden tunniste-, rahaliikenne- ja muita luottamuksellisia tietoja. Näitä tietoja pyritään hankkimaan organisaation henkilöstöltä myös ns. sosiaalisella hakkeroinnilla, jossa työntekijään ollaan suoraan yhteydessä (puhelimitse, sähköpostitse tai jopa henkilökohtaisesti). Näissä kontakteissa uhri houkutellaan paljastamaan tärkeitä, salassa pidettäviä tietoja. Tässä yhteydessä on hyvä huomioida erilaisia toimintatapoja, joilla mahdollisia riskejä voidaan pienentää.

Rikollisia kiinnostavat tiedot

Organisaatiossa on paljon tietoja, jotka kiinnostavat rikollisia tai verkkomurtautujia. Tällaisia tietoja ovat esimerkiksi:

- käyttäjätunnukset ja salasanat
- pankkitunnukset
- luotto- ja maksukorttitiedot
- tutkimus- ja tuotekehitystiedot
- prosessivaiheet, tuotteiden ainesosat ja valmistuskaavat
- asiakas- ja henkilötiedot
- tilaus- ja toimittajatiedot sekä vastaavat -hinnat ja -määrät
- työntekijöiden nimitiedot ja sähköpostiosoitteet
- henkilöstön vastuut, loma-ajat ja sijaiset
- organisaation rakenne
- käytössä olevat ohjelmistot ja niiden versionumerot
- palomuuri-, virustorjunta- ja muiden turvallisuusjärjestelmien tiedot
- hälytys- ja valvontajärjestelmien sekä lukituksen ja vartioinnin tiedot.

Luottamuksellisten tietojen määrittely

- Määrittele, mitkä tiedot ovat organisaation kannalta luottamuksellisia. Päätä myös, mitä tietoja voidaan antaa organisaation ulkopuolelle ja mitä ei.
- Luo tiedoille käsittely-, säilytys- ja tuhoamissäännöt.
- Muistuta henkilökuntaa, että myös käytettävät sovellusohjelmat ja niiden versionumerot ovat sisäistä tietoa, jota ei saa kertoa tuntemattomille. Hakkeri voi käyttää näitä tietoja pyrkiessään tunkeutumaan organisaation järjestelmiin.

Sosiaalisen hakkeroinnin tunnistaminen

- Hakkeri luottaa yleensä **ihmisten haluun auttaa, innokkuuteen kertoa omasta työtehtävästään tai auktoriteettien pelkoon**.
- Hakkeroijat ovat taitavia ihmisten manipuloijia. He pystyvät usein muokkaamaan rooliaan ja toimintaansa uhrin käyttäytymisen mukaisesti.
- Tyypillisesti hakkeri esiintyy esimerkiksi ulkoistettujen tukipalvelujen (esim. tietotekniikkatuki tai kirjanpitotoimisto) työntekijänä, jolla on pikaista ratkaisua vaativa ongelma yrityksen tietojärjestelmien kanssa.
- Myös viranomaisen, tyytymättömän asiakkaan tai kiireisen tavarantoimittajan

edustajat ovat suosittuja rooleja.

- Hakkeroinnille tyypillistä on kiire. Tieto on saatava mahdollisimman nopeasti, eikä se voi odottaa uhrin esimiehen tai varsinaisen vastuuhenkilön saapumista.
- Keskustelun sävy on voi olla esimerkiksi yliystävällinen (kohteena kokeneemmat työntekijät) tai uhkaileva/komenteleva (kohteena kokemattomat työntekijät).
- Kehittyneet hakkerit johdattavat keskustelua vähitellen haluamaansa suuntaan: ”Meillä tuli ongelmia taloushallinnon järjestelmissä. Onkos teilläkin tämä XXXX-sovellus käytössä?”
- Hakkerit rakentavat luottamusta viittaamalla yhteisesti tunnettuihin henkilöihin, joiden nimi on saatu organisaation www-sivulta tai puhelunvälittäjältä: ”Meikäläisen Matti IT-tuesta pyysi soittamaan sinulle. Tarvitsisin asennusta varten sen salasanan…”
- Hakkeri on saattanut myös hakea uhrinsa tietoja ja kiinnostuksen kohteita etukäteen esimerkiksi sosiaalisista medioista / internetistä. Yhteydenottotilanteessa hän käyttää näitä tietoja hyväkseen saadakseen uhrin lataamaan saastuneita tiedostoja: ”Minäpä lähetän sinulle yhden hyvän jääkiekkolinkin, josta voit ladata…”
- Käytetyn nimen tai roolin ei tarvitse olla keksitty, vaan hakkeri voi myös esiintyä tietoon oikeutettuna henkilönä.

Sosiaalisen hakkeroinnin ehkäiseminen – ohjeet ja koulutus

- Tiedota ja kouluta henkilökuntaa säännöllisesti sosiaalisen hakkeroinnin mahdollisuudesta organisaatiossa.
- Laadi ja jaa henkilöstölle kirjalliset ohjeet siitä, mitkä ovat luottamuksellisia tietoja ja mitä tietoja saa luovuttaa organisaation ulkopuolelle.
- Ohjeista myös tietojen turvallinen säilytys, kuljetus ja tuhoaminen.
- Jos ennestään tuntematon henkilö väittää tarvitsevansa luottamuksellista tietoa, ohjeista henkilökunta varmistamaan asia esimieheltään aina ennen luovutusta.

Sosiaalisen hakkeroinnin ehkäiseminen – tekniset ja tietotekniset ratkaisut

- Rajoita henkilökunnan pääsy yrityksessä vain työtehtävissä tarvittaviin tietoihin ja järjestelmiin. Sulje muut hakemistot ja järjestelmät henkilöiltä, jotka eivät niitä työtehtävissään tarvitse.
- Pidä yllä ajantasaista palomuuri- ja virustorjuntajärjestelmää. Huolehdi myös kaikkien käytettyjen ohjelmien ja niiden liitännäisten toimivista turvapäivityksistä.
- Käytä luottamuksellisen tiedon välityksessä lähtevän sähköpostin salausta. Toimita salauksen purkuun tarvittava koodiavain toista kanavaa (tekstiviesti, soitto, kirjeposti, henkilökohtainen tapaaminen) pitkin vastaanottajalle.
- Huolehdi, että järjestelmien salasanoja vaihdetaan säännöllisesti. Salasanojen tulee olla riittävän pitkiä ja vaikeita. Vanhoja salasanoja ei saa käyttää uudelleen.
- Jos epäilet, että salasanasi ovat paljastuneet, vaihda välittömästi järjestelmien salasanat.
- Työasemat tulee lukita itse tai automaattisesti järjestelmän toimesta, kun työpisteessä ei oleskella.
- Estä vierailijoiden kytkeytyminen yrityksen sisäverkkoon, äläkä päästä heitä omalle työasemallesi.
- Kytke yrityksen tietoteknisiin laitteisiin vain tietohallinnon toimittamia tietovälineitä (USB-muistit, romput) tai laitteita (hiiret, kamerat), ei ulkopuolisilta saatuja.
- Luo toimitiloihin eriasteisia kulunvalvontavyöhykkeitä. Estä asiattomien / vieraiden pääsy vyöhykkeeltä toiselle esimerkiksi lukituilla ovilla.

Sosiaalisen hakkeroinnin ehkäiseminen – henkilöstön toiminta

- Sovi palveluntarjoajien ja tavarantoimittajien kanssa nimetyt yhteyshenkilöt, jotka ovat yhteydessä organisaation omiin yhteyshenkilöihin. Sovi myös näiden henkilöiden varahenkilöt poissaolotapauksissa.
- Pyydä ennestään tuntemattomalta huolto- tai korjaushenkilökunnalta nähtäväksesi henkilökortti ja/tai työmääräys ennen kuin

päästät heidät käsiksi tietojärjestelmiin tai tietoteknisiin laitteisiin.

- Säilytä luottamukselliset paperit lukituissa kaapeissa, kun et ole työpisteessä.
- Hävitä tarpeeton tietomateriaali turvallisesti. Hävittäminen tulee tehdä silppuamalla paperit, murskaamalla tai ylikirjoittamalla magneettinen media tai käyttämällä hävityksessä palveluntarjoajan lukittuja tietosuoja-astioita.
- Jos tietoja pyydetään puhelimitse, varmista ennen tietojen antamista, että puhelinnumero on tietoon oikeutetun henkilön. Varmistuksen voi tehdä soittajan numerotiedolla puhelinluettelosta tai vastasoitolla pyytäjän organisaation puhelinkeskuksen kautta.
- Pidä neuvottelut vieraiden kanssa ainoastaan tarkoitukseen varatuissa neuvotteluhuoneissa. Siivoa neuvotteluhuoneista etukäteen edellisen kokouksen muistiinpanot sekä tilaisuuden jälkeen myös omat esitysmateriaalisi.
- IT-tuki ei tarvitse salasanaasi. Salasanaa ei pidä koskaan lähettää sähköpostilla tai antaa puhelimitse. Jos tukihenkilö haluaa kirjautua tunnuksillasi koneellesi, tee se itse salasana peittäen. Vaihda heti korjaustoimien jälkeen salasana uuteen.
- Pidä luottamukselliset työasiat organisaation sisäisinä tietoina. Vältä keskustelua näistä asioista ulkopuolisten, tuttavien tai perheenjäsenten kanssa.
- Vältä työasioista keskustelua julkisella paikalla, yleisissä kulkuvälineissä tai puhelimessa muiden kuullen.
- Jos aiemman yhteistyökumppanin sähköpostin nimikenttä on muuttunut tai kumppani vaihtaa viestissä käytettyä kieltä (esim. suomi → englanti), viestin kieliasua tai vastausosoitetta, varmista puhelimella, että viesti on oikealta taholta.
- Käytä vastausviestien osoitteena mieluiten omaa osoitelistaasi, ei ”reply”-osoitetta.