Centria SecuLab esittää – tietoturvapodcast, osa 7 – Tietojenkalastelu

Ai kauheeta, onko puhelinlasku jäänyt maksamatta…
Miten ne tälleen muistuttavat asiasta sähköpostissa – ja kauheeta mitä seuraamuksia…
…ja vielä just nyt, kun on niin paljon muutakin…
Jaahas, onneksi on kirjautumislinkki suoraan pankin sivulle.

Tietojenkalastelun avulla pyritään vaikuttamaan tietokoneen käyttäjään ja saamaan hänet antamaan sähköpostin tai verkkosivun välityksellä luottamuksellista tietoa. Tietojenkalastelu voi tapahtua esimerkiksi niin, että käyttäjältä pyydetään pankin nimissä sähköpostitse luottokortin numeroa ja tunnuslukua.

Tietojenkalastelu toteutetaan tyypillisesti aidolta näyttävän viestin avulla, jonka tarkoituksena on huijata rahaa tai tietoa – tai esimerkiksi saada pääsy yritysverkkoon. Tietojenkalasteluviestit jäljittelevät oikeiden organisaatioiden ulkoasua, jotta viesti olisi mahdollisimman todentuntuinen. Rikollinen voi jopa ottaa kokonaan haltuunsa toisen käyttäjän tilin. Tällöin viestit tulevat suoraan tuntemasi henkilön tai organisaation sähköpostista. Haitallisia linkkejä liikkuu sähköpostien lisäksi myös sosiaalisessa mediassa ja nettisivuilla. Niitä saatetaan levittää myös tekstiviesteillä.

Kohdennettu tietojenkalastelu on tiettyyn henkilöön tai tietyn organisaation henkilöstöön kohdistuvaa urkintaa. Tällöin kohteelle lähetetään sähköpostiviesti, joka näyttää tulevan pankilta, työkaverilta tai esimieheltä, jolloin urkinnan kohde ei osaa olla varovainen. Tämän avulla työntekijä taivutellaan maksamaan valelasku tai tekemään muu, usein kiireellinen tilisiirto tai palkanmaksu, joka päätyy huijarille.

Tietojenkalastelun uhriksi saattaa joutua kuka tahansa, jolta voi saada rahaa tai arvokasta tietoa – riittää, että pieni osa vastaanottajista hairahtuu vastaamaan viestiin tai klikkaamaan rikollisen luomaa linkkiä.

Kalasteluviestejä lähetetään tyypillisesti massaposteina tuhansille eri ihmisille ja organisaatioille. Vaikka prosentuaalisesti vain pieni osa viestin vastaanottajista avaa haitallisen liitteen tai klikkaa linkkiä, voivat rikolliset kuitenkin saada haltuunsa paljon erilaista tietoa sekä sievoisen summan rahaa.

Tietojenkalastelua tehdään useissa eri kanavissa ja kohteena voivat olla myös erilaiset palvelut. Esimerkiksi sosiaalisen median tilit voivat näin päätyä vääriin käsiin. Tietojenkalastelu on nykyään varsin kehittynyttä ja joistakin viesteistä on erittäin vaikea päätellä, että kyseessä on huijaus. Viesteissä saatetaan esimerkiksi vedota inhimilliseen tekijään, kuten tunteisiin tai kiireeseen, jotta huijaus saadaan onnistumaan.

Sinun kannattaa olla erityisen tarkkana:
- kun saat kiireellisen tilisiirtopyynnön, tai
- kun saat ilmoituksen tilitietojen muutoksesta, tai
- kun saat sähköpostiliitteitä.

Sinun kannattaa myös olla tarkkana:
- mikäli viestissä pyydetään tarkistamaan tai varmistamaan kirjautumistiedot johonkin palveluun, tai
- kun avaat liitteen kirjautumalla tunnuksillasi kyseiseen palveluun.

Jos saat linkin palveluntarjoajalta, ja pyynnön kirjautua sivuille pikaisesti, tarkista aina linkin todenmukaisuus, ja myös, että kirjaudut oikeaan paikkaan. Palveluntarjoajan verkkosivuille tulee aina kirjautua sen oman verkkosivun kautta. Jos et ole varma vastaanottamasi viestin lähettäjästä tai sen sisällöstä, voit aina varmistaa asian soittamalla viestin lähettäjälle. Tällöin yhteystiedot tulee kuitenkin katsoa muualta kuin lähetetystä viestistä.

Nyt on kyllä pakko lopettaa multitaskaaminen, ja ottaa kuppi kahvia.
Kirjaudun sen jälkeen nettipankkiin ja katson, onko tuo lasku oikeasti siellä.