8 vinkkiä väärinkäytösten välttämiseksi yrityksessäsi

WHISTLEBLOWER PARTNERS

Väärinkäytökset ovat yrityksille merkittävä ja kasvava ongelma globalisaation ja digitalisaation lisääntyessä sekä monien alojen monimutkaistumisen myötä esimerkiksi koronaviruksen vaikutuksesta.

Yritysten sisäiset väärinkäytökset ovat suurempi ongelma kuin moni luuleekaan. Yritys voi menettää jopa viisi prosenttia vuotuisesta liikevaihdostaan sisäisten väärinkäytösten vuoksi. Tämä käy ilmi kansainvälisistä tutkimuksista. Yritykset ovat myös havainneet talousrikollisuuden jyrkkää kasvua, kun työntekijöitä huijataan maksamaan rahaa ulkopuolisille rikollisille.

On selvää, että valvonta on tärkeää. Esimerkiksi tilintarkastustyökaluista voi olla paljon apua, mutta ratkaisu ei ole kokonaisuudessaan aivan näin yksinkertainen. Yhtä tärkeää on hyvä työkulttuuri, jossa työntekijöitä kannustetaan ja ohjataan tekemään oikeita valintoja. Siten he eivät tee tietoisia tai tiedostamattomia virheitä, jotka voivat tulla yritykselle kalliiksi.

Koronaviruspandemian aikana etätöistä on tullut uusi normaali käytäntö, ja suuntaus todennäköisesti jatkuu. Tämä on myös luonut uusia riskejä yrityksille.

Seuraavassa on muutamia seikkoja, jotka on syytä ottaa huomioon väärinkäytösten yhteydessä:

1. **Lisääntynyt valvonta ja tietoisuus menettelytavoista yrityksessä**

Kun työntekijät ovat vähemmän toimistossa, sisäisiä menettelytapoja saatetaan höllentää, jotta päivittäinen elämä onnistuu sujuvammin. Salasanoja voidaan jakaa työtovereiden kesken. On myös olemassa riski, että sama henkilö voi hyväksyä laskuja, muuttaa maksun saajien tietoja ja hyväksyä maksuja.

Tämä tarjoaa otolliset olosuhteet talousrikoksille, joissa huijari voi peittää jälkensä. Jos rikkomuksia tehdään pienimuotoisesti pitkän ajan kuluessa, ne voivat kasvaa melko suuriksi, ennen kuin ne mahdollisesti huomataan.

Yritysten ei siis pitäisi höllentää menettelyjä sisäisesti, vaikka työntekijät saattavat yhä useammin työskennellä kotoa käsin. Valvontatoimia on mukautettava jatkuvasti riskien mukaan.

2. **Tietoisuus hakkeroinnista, tietojenkalastelusta ja muista tietotekniikkahuijauksista**

Rikolliset yrittävät yhä useammin huijata yrityksen työntekijöitä luovuttamaan henkilökohtaisia koodeja tai tietoja puhelimitse (vishing), tekstiviesteillä (smishing) tai sähköpostitse (phishing).

Huijari esiintyy usein esimerkiksi yrityksen pankin tai liikekumppanin, viranomaisten tai Netsin edustajana.

Joidenkin yritysten sähköpostijärjestelmiin murtaudutaan suoraan. Toiset rikolliset taas käyttävät phishing-tekniikkaa, jossa väärennetyn sähköpostin linkkiä tai tiedostoa napsauttava työntekijä antaa heille pääsyn yrityksen IT-järjestelmiin.

On erittäin tärkeää vakuuttaa työntekijöille, että heidän on suhtauduttava epäilevästi odottamattomiin yhteydenottoihin tai epätavallisilta tai oudoilta vaikuttaviin sähköpostiviesteihin. Työntekijöille on vakuutettava, että heidän ei koskaan tule antaa henkilökohtaisia tietoja tai koodeja. Epäselvissä tapauksissa yksittäisten työntekijöiden on aina otettava yhteyttä yrityksensä IT-osastoon – mieluummin liian usein kuin liian harvoin.

3. Ehkäise ”toimitusjohtajahuijaukset”

Toimitusjohtajahuijaus tapahtuu, kun työntekijä huijataan maksamaan väärä lasku tai tekemään luvaton siirto yrityksen tililtä huijarin omistamalle tilille. Huijari esiintyy henkilönä, joka on yrityksessä johtavassa asemassa.

On tärkeää, että yrityksessä otetaan käyttöön menettelytavat laskujen maksamista ja varojen siirtämistä varten ja että kaikkien tavanomaisesta poikkeavien pyyntöjen jälkeen tehdään tarkistus, vaikka sähköpostitse saapunut tieto rahansiirrosta olisi kuinka kiireellinen. Puhelu toimitusjohtajalle voi usein paljastaa huijauksen ja pelastaa yrityksen valtavilta tappioilta.

4. Ehkäise laskuhuijaukset

Laskuhuijauksissa tai -petoksissa rikollinen teeskentelee edustavansa yrityksen asiakasta tai liikekumppania ja pyytää, että tulevat laskut maksetaan uudelle pankkitilille, joka kuuluu huijarille.

On tärkeää varmistaa, että maksutietoja käsittelevät työntekijät ovat tietoisia tämäntyyppisistä huijauksista ja siitä, miten ne voidaan välttää. Siksi on tärkeää ohjeistaa laskujen maksamisesta vastaavaa henkilöstöä tarkastamaan laskut aina epäjohdonmukaisuuksien varalta, laatimaan selkeät menettelytavat maksujen manuaalista käsittelyä varten ja tarkistamaan maksupyyntöjen laillisuus.

Automaattisen maksujärjestelmän käyttäminen on eduksi, jotta manuaalisten maksujen määrä voidaan pitää mahdollisimman pienenä.

5. **Ole tietoinen huijauksista, kun muutat pankkitietoja**

On tärkeää olla tietoinen siitä, että pankkitietojen muuttamiseen liittyviä huijauksia sattuu. Tämä tieto on jaettava niiden yrityksen toimintojen kanssa, joihin saattaa kohdistua yrityksiä muuttaa pankkitietoja.

Jos yritys saa sähköpostiviestin pankkitietojen muutoksesta, liikekumppaniin on aina otettava yhteyttä, jotta sen tavanomainen yhteyshenkilö voi vahvistaa tilimuutoksen voimaantulon.

6. **Ehkäise ALV-petokset**

ALV-karuselleihin liittyvässä kaupankäynnissä on merkittävä riski, että yritykset altistuvat ALV-petoksille. ALV-karuselleille on ominaista tavaroiden tai palvelujen kauppa yli kansallisten rajojen. Tyypillisesti tavarat myydään bulvaanin kautta, joka ei ilmoita tai tilitä arvonlisäveroa, kun tavarat myydään edelleen. Tämän jälkeen tavarat myydään yhden tai useamman välittäjän kautta, ennen kuin ne lähetetään jälleen pois maasta ja karuselli jatkuu.

Välittäjät voivat olla aitoja suomalaisia yrityksiä. Yritykset voivat siten helposti joutua ansaan, joka johtaa taloudellisiin tappioihin esimerkiksi menetettyjen arvonlisäverovähennysten, huonolaatuisten tavaroiden, huonon maineen tai kilpailusääntöjen rikkomisen muodossa. Joissain tapauksissa koko markkinat voivat kärsiä, ennen kuin petos havaitaan.
Jos on pienintäkään epäilystä liikekumppanista tai tuotteista, joita yritys on ostamassa, kannattaa pidättäytyä kaupasta. On myös aina suositeltavaa tarkistaa, että liikekumppanit, joiden kanssa yritys käy kauppaa, ovat rekisteröityneet arvonlisäverovelvollisiksi. Yritys tekee tämän etsimällä toimittajan ALV-numeron.

Verottajan sivustolla luetellaan myös useita erityiskohtia, jotka on syytä ottaa huomioon arvioitaessa kauppakumppanin luotettavuutta.

7. **Varo tulostimia**

Yritysten tulostimet voivat aiheuttaa yritykselle merkittävän turvallisuusriskin, jos varovaisuutta ei noudateta.

Tulostinteknologian kehitys, mukaan lukien se, että tulostimissa on samat laitteistokomponentit kuin tietokoneissa, kuten asema, ohjauspaneeli ja näppäimistö, tarkoittaa, että yritysten olisi suojattava tulostimet hyökkäyksiltä samalla tavoin kuin tietokoneet. Tämä jätetään usein huomiotta, vaikka yritykset ovat yleensä hyvin tietoisia verkkouhista.

8. **Ota yhteyttä pankkiin ja ilmoita huijauksesta tai sen yrityksestä poliisille**

Jos huijaukseen liittyvä maksu on tehty yrityksen pankin kautta, pankkiin on aina otettava yhteyttä summan perimiseksi takaisin. Ota myös aina yhteyttä poliisiin, jos kyseessä on huijaus tai huijausyritys, vaikka et olisikaan joutunut sen uhriksi. Muista säilyttää asiakirjat ja liittää ne poliisille tehtävään ilmoitukseen.