YRITYKSIIN KOHDISTUVAT HYBRIDIUHAT

Maailmalla on eletty jo pitkään yrityksiin kohdistuvan tietojen kalasteluyritysten kulta-aikaa ja vallitseva maailmantilanne voi pahentaa jo ennestään vaikeaa tilannetta. Suomen NATO -jäsenyys voi altistaa erityisesti Venäjän vastatoimille hybridivaikuttamisen muodossa. Pahimmillaan hybridivaikuttaminen voi romahduttaa yrityksen toimintakyvyn. Keskuskauppakamari on koonnut yrityksille kymmenen keinoa hybridivaikuttamisen ehkäisemiseksi.

Keskuskauppakamarin ja Huoltovarmuuskeskuksen tekemä selvitys paljasti, että suuriin yrityksiin kohdistunut hybridivaikuttaminen on lisääntynyt ja jopa kolmasosa suurista vastaajayrityksistä (32 %) on havainnut hybridivaikuttamiseksi epäilemäänsä toimintaa. Venäjä ja Kiina mainittiin tuoreessa selvityksessä useimmiten vaikuttamisen takana olevana maana.

Hybridivaikuttajalla on käytettävissään kolme toimintatapaa. Ne ovat informaatiovaikuttaminen, kybertoiminta ja fyysinen vaikuttaminen. Usein yrityksiin kohdistuu vakoilua, vaikutusvallan tavoittelua tai pyrkimys päästä kontaktiin jonkun tietyn tahon kanssa.

Selvitys paljastaa, että suomalaisyritysten merkittävimmät heikkoudet, joita ulkomaiset tahot hyödyntävät, ovat liika avoimuus ja sinisilmäisyys (67 %), kyky tunnistaa liiketoiminnaksi peitelty vaikuttamisyritys tai hanke yrityksen hyödyntämiseksi tarkoituksena vaikuttaa varsinaiseen kohteeseen (56 %). Yritysjohtajilla ja yritysten hallituksilla on tärkeä rooli sen varmistamisessa, että yrityksen työntekijät ymmärtävät kyberturvallisuuden merkityksen ja omaksuvat oikeat toimintatavat. Vallitsevina aikoina jokaisella työntekijällä siinä on tärkeä rooli.

Peräti 96 prosenttia yrityksistä kaipaa hybridiuhista lisää tietoa ja koulutusta viranomaisilta. Keskuskauppakamarin mukaan tärkeintä on yrityksen henkilökunnan kouluttaminen ja tiedon jakaminen työyhteisössä, jotta hybridivaikuttaminen osataan tunnistaa ja siihen osataan varautua asianmukaisesti. Pahimmillaan yrityksen toimintaan suoraan tai välillisesti kohdistuva hybridivaikuttaminen voi romahduttaa yrityksen toimintakyvyn estäessään esimerkiksi sähkön saatavuuden tai tietoliikenneyhteyksien toimivuuden.

Suuret yritykset ovat taas näkyviä, niillä on usein laaja asiakaskunta, valtiollisia asiakkaita, suhteita poliitikkoihin, yhteiskunnan infraan liittyviä toimeksiantoja ja muita vastavia tekijöitä, joiden kautta ne voivat valikoitua vaikuttamisen kohteiksi tai reiteiksi lopullisiin kohteisiin. Sinisilmäisyys ja liika avoimuus on nyt unohdettava. Helpoilla toimenpiteillä yritys voi estää vakavimmat seuraukset ja varmistaa toiminnan jatkuvuuden.

KESKUS-
KAUPPAKAMARI

Alvar Aallon katu 5 C, PL 1000 | 00100 HELSINKI | +358 9 4242 6200
kauppakamari.fi

Keskuskauppakamari on koonnut alle keinoja, joilla jokainen yritys voi parantaa omaa kykyään ehkäistä hybridivaikuttamista ja varautua vaikuttamisen kohteeksi joutumista.

1. Huolehdi tietoturvasta sekä teknisestä että henkilöstön osaamisesta.
2. Kouluta henkilökuntaa tunnistamaan erilaiset tiedon urkintayritykset. Kerro samalla, että yrityksesi voi olla vaikuttamisen kohteena esimerkiksi asiakassuhteiden, toimialan, omistajapohjan tai viranomaisyhteyksien vuoksi. Yrityksen tietoa voivat urkkia myös rikolliset.
3. Varmista, että yrityksen normaali rikosturvallisuus on ajan tasalla. Tarkista ohjeiden ajantasaisuus ja ennen kaikkea se, että henkilökunta osaa toimia niiden mukaan.
4. Kerro työntekijöille, että heidän tekemänsä havainnot ovat tärkeä osa yrityksen turvallisuutta. Kynnys havaintojen kertomiseen tulee olla matala.
5. Ota väärinkäytösten ilmoituskanava käyttöön ja kouluta työntekijät käyttämään sitä. Työntekijät havaitsevat paljon asioita, mutta eivät aina tiedä, pitäisikö heidän ilmoittaa havainnoistaan ja kenelle he ilmoittaisivat. Mahdollisuus ilmoittaa anonyymisti havainnoista nostaa yrityksen valmiutta ja alentaa huomattavasti kynnystä ilmoittaa epäilyistä.
6. Pyri aina selvittämän uusien yhteistyötahojen ja henkilöiden taustat.
7. Selvitä, mitkä tiedot ovat kriittisiä yrityksen kannalta ja varmuuskopioi ne. Testaa myös varmuuskopioiden turvallisuus.
8. Selvitä liiketoiminnan jatkuvuus, miten toimitte ilman tietolaitteita ja pääsyä verkkoon.
9. Varmista, että henkilökunta osaa tunnistaa informaatiovaikuttamisen. On tärkeää, että työntekijät osaavat olla jakamatta ja samalla vahvistamatta tällaista vaikuttamista. Yleensä informaatiovaikuttaminen kohdistuu kaikkiin kansalaisiin ja siksi yrityksen on hyvä varmistaa työntekijöiden kyky tunnistaa sitä.
10. Kouluta ja ohjeista henkilökuntaa. Johdon vastuulla on liiketoiminnan suojaaminen ja toiminnan jatkuvuuden varmistaminen.

Selvitys on toteutettu osana LUJAT-hanketta, joka on Keskuskauppakamarin ja Huoltovarmuuskeskuksen yhteishanke. Hankkeessa kehitetään pk-yritysten toiminnan jatkuvuutta ja kestävyyttä. Selvityksen toteutti Taloustutkimus ja se tehtiin maalis-huhtikuussa 2022.

Huoltovarmuuskeskus
Försörjningsberedskapscentralen
National Emergency Supply Agency

KESKUS-
KAUPPAKAMARI

Alvar Aallon katu 5 C, PL 1000 | 00100 HELSINKI | +358 9 4242 6200
kauppakamari.fi