enisa

EUROOPAN UNIONIN
KYBERTURVALLISUUSVIRASTO

Kyberturvallisuusopas pk-yrityksille

12 VAIHETTA

YRITYKSEN TURVALLISUUDEN PARANTAMISEEN

Covid-19-kriisi teki selväksi, miten tärkeitä internet ja tietokoneet ovat pk-yrityksille Jotta liiketoiminta pysyi käynnissä pandemian aikana, monien pk-yritysten täytyi ottaa käyttöön toimenpiteitä turvatakseen toiminnan jatkuvuuden, kuten pilvipalveluiden käyttöönotto, internetpalvelujen parantaminen, verkkosivujen kohentaminen ja henkilöstön etätyöskentely.

Tässä esitteessä luetellaan 12 käytännön vaihetta, joita seuraamalla pk-yritykset voivat paremmin turvata järjestelmiään ja liiketoimintaansa. Tämä julkaisu liittyy ENISAn yksityiskohtaisempaan raporttiin pk-yritysten kyberturvallisuushaasteista ja -suosituksista **"Cybersecurity for SMES – Challenges and Recommendations"**.

1 HYVÄN KYBERTURVALLISUUSKULTTUURIN KEHITTÄMINEN

HALLINNOINTIVASTUU

Hyvä kyberturvallisuus on avain pk-yritysten menestymiseen. Vastuu tästä kriittisestä toiminnosta on annettava jollekin organisaation jäsenelle, joka varmistaa, että kyberturvallisuudella on riittävät resurssit, kuten henkilöstöltä liikenevä aika, kyberturvallisuusohjelmistojen, -palvelujen ja -laitteistojen hankkiminen, henkilöstön koulutus ja tehokkaiden käytäntöjen kehittäminen.

TYÖNTEKIJOIDEN SITOUTTAMINEN

Työntekijät sitoutetaan johdon tehokkaalla kyberturvallisuusviestinnällä, johdon avoimella tuella kyberturvallisuusaloitteille, asianmukaisilla työntekijöille tarkoitetuilla koulutuksilla, ja antamalla työntekijöille selkeät ja tarkat kyberturvallisuuskäytäntöihin kirjatut ohjeet.

KYBERTURVALLISUUSKÄYTÄNTÖJEN JULKISTAMINEN

Kyberturvallisuuskäytännöissä on määritettävä työntekijöille selkeät ja tarkat ohjeet yrityksen tieto- ja viestintäteknisen ympäristön, laitteiston ja palvelujen käytöstä. Käytännöistä on myös käytävä ilmi, millaisia seurauksia niiden noudattamatta jättämisestä on työntekijälle. Käytäntöjä on tarkistettava ja päivitettävä säännöllisesti.

KYBERTURVALLISUUSTARKASTUKSET

Kokeneiden ja osaavien tarkastajien tulisi tehdä tarkastukset säännöllisesti. Tarkastajien on oltava riippumattomia, joko ulkopuolisia toimeksisaajia tai pk-yritysten sisäisiä, ja heidän on oltava riippumattomia päivittäisistä IT-toiminnoista.

TIETOSUOJAN MERKITYS

Yleisen tietosuoja-asetuksen[1] mukaisesti jokaisen pk-yrityksen, joka käsittelee tai säilyttää EU-/ETA-alueilla asuvien henkilötietoja on varmistettava, että niillä on käytössään asianmukaiset turvallisuustarkastukset tietojen suojaamista varten. Tämä sisältää myös sen varmistamisen, että kaikilla pk-yrityksen puolesta toimivilla kolmansilla osapuolilla on käytössään asianmukaiset turvatoimenpiteet.

1 Yleinen tietosuoja-asetus
https://ec.europa.eu/info/law/law-topic/data-protection_fi

2

TARVITTAVAN KOULUTUKSEN TARJOAMINEN

Kaikille työntekijöille tulisi tarjota säännöllistä koulutusta, jossa keskitytään kyberturvallisuuden merkityksen ymmärtämiseen, jotta he havaitsevat ja osaavat käsitellä erilaisia kyberturvallisuusuhkia. Koulutukset on räätälöitävä pk-yrityksille sopiviksi ja niissä tulisi harjoitella tosielämän tilanteita.

Erikoistunutta kyberturvallisuuskoulutusta tulisi tarjota henkilöille, jotka vastaavat yrityksen kyberturvallisuuden hallinnasta, jotta heillä on työssä tarvittavat taidot ja osaaminen.

3

KOLMANSIEN OSAPUOLIEN TEHOKAS HALLINNOINTI

Varmista, että kaikkia toimittajia ja erityisesti niitä, joilla on pääsy arkaluonteisiin tietoihin ja/tai järjestelmiin, seurataan aktiivisesti ja että ne noudattavat sovittuja turvallisuusvaatimuksia. Toimittajien kanssa tulisi tehdä kirjallinen sopimus siitä, miten ne täyttävät kyseiset vaatimukset.

4

SUUNNITELMA HÄIRIÖTILANTEID EN VARALLE

Laadi virallinen suunnitelma häiriötilanteisiin varautumiseen ja sisällytä siihen selkeät ohjeet, roolitukset ja vastuut. Suunnitelman avulla varmistetaan, että kaikkiin kyberhäiriötilanteisiin vastataan ajoissa, asiantuntevasti ja asianmukaisesti. Häiriötilanteisiin vastaaminen nopeutuu, jos käytössä on työkalu, joka seuraa epäilyttävää toimintaa ja häiriötilanteita ja antaa niistä ilmoituksia.

5 TURVALLINEN PÄÄSY JÄRJESTELMIIN

Työntekijöille tulisi suositella sellaisen tunnuslauseen käyttöä, joka koostuu vähintään kolmesta satunnaisesta sanasta ja joka on sekä helposti muistettava että turvallinen. Jos käytetään perinteistä salasanaa:

- salasanan pitää olla pitkä, siinä pitää olla sekä isoja että pieniä kirjaimia ja mahdollisesti myös numeroita ja erikoismerkkejä.
- Ilmiselviä salasanoja, kuten ”salasana”, ja järjestyksessä olevia kirjain - tai numerojonoja, kuten ”abc” tai ”123” on vältettävä.
- Niihin ei saa sisällyttää henkilökohtaisia tietoja, jotka voi löytää verkosta.

Olipa käytössä sitten tunnuslause tai salasana:

- Älä käytä niitä muualla.
- Älä kerro niitä kollegoille.
- Ota käyttöön kaksivaiheinen tunnistus.
- Käytä salasananhallintaohjelmaa.

6

TURVALLISET LAITTEET

Henkilöstön laitteiden (pöytätietokoneiden, kannettavien, tablettien ja älypuhelinten) turvaaminen on olennainen vaihe kyberturvallisuusohjelmassa.

OHJELMISTOJEN KUNNOSSAPITO JA PÄIVITTÄMINEN

Keskitetty alusta ohjelmistokorjausten hallintaan on suositeltava. Pk-yrityksissä on suositeltavaa

- päivittää kaikki ohjelmistot säännöllisesti
- ottaa käyttöön automaattiset päivitykset aina kun mahdollista
- yksilöidä ohjelmistot ja laitteet, jotka vaativat manuaalista päivittämistä
- ottaa huomioon mobiililaitteet ja esineiden internetiin kytketyt laitteet.

VIRUSTORJUNTA

Keskitetysti hallinnoitu virustorjuntaratkaisu tulisi ottaa käyttöön kaikissa laitteissa ja se on pidettävä ajan tasalla tehokkuuden varmistamiseksi. Älä asenna piraattiohjelmistoja, sillä ne voivat sisältää haittaohjelmia.

SÄHKÖPOSTI - JA VERKKOSUOJATYÖKALUT

Ota käyttöön ratkaisuja, joilla voidaan estää roskapostit, sähköpostit, jotka sisältävät linkkejä haitallisille verkkosivustoille, tietojen kalasteluviestit sekä sähköpostit, jotka sisältävät haitallisia liitteitä, esimerkiksi viruksia.

TIETOJEN SALAUS

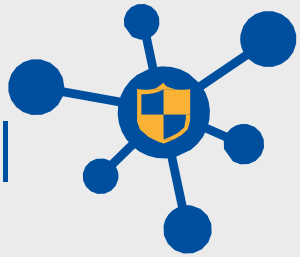
Suojele tietoja käyttämällä salausta. Pk-yritysten pitäisi huolehtia siitä, että mobiililaitteille, kuten kannettaville tietokoneille, älypuhelimiin ja tableteille tallennetut tiedot ovat salattuja. Jos tietoja siirretään hotellin tai lentokentän WiFi-verkon kaltaisten julkisten verkkojen kautta, varmista, että tiedot on salattu joko VPN-yhteydellä tai käyttämällä verkkosivustoja turvallisella yhteydellä SSL/TLS-protokollan avulla. Yritysten on myös huolehdittava, että niiden omat verkkosivustot käyttävät asianmukaista salausteknologiaa asiakastietojen siirtämiseen verkossa.

MOBIILILAITTEIDEN HALLINNAN KÄYTTÖÖNOTTO

Jotta henkilökunnan etätyöskentely olisi helpompaa, monet pk-yritykset antavat työntekijöiden käyttää omia kannettaviaan, tablettejaan ja/tai älypuhelimiaan. Tästä seuraa useita turvallisuushuolia, sillä laitteille voidaan tallentaa arkaluonteisia yritystietoja. Yksi tapa hallita tätä riskiä on ottaa käyttöön mobiililaitteiden hallinnointijärjestelmä (MDM), jonka avulla yritykset voivat

- hallita, millä laitteilla on pääsy yrityksen järjestelmiin ja palveluihin
- varmistaa, että laitteelle on asennettu ajan tasalla oleva virustorjuntaohjelma
- määrittää, onko laitteella salaus
- määrittää, onko laitteelle asennettu ajan tasalla olevat ohjelmistokorjaukset
- varmistaa, että laite on suojattu PIN -koodilla ja/tai salasanalla
- etäyhteyden avulla poistaa kaikki pk-yrityksen tiedot laitteelta, jos laitteen omistaja kadottaa laitteen tai se varastetaan, tai jos laitteen omistajan työsuhde pk-yrityksessä päättyy.

7 VERKKO TURVALLI SEKSI



PALOMUURIEN KÄYTTÖ

Palomuurit valvovat verkkoon tulevaa ja siitä lähtevää liikennettä ja ovat kriittinen työkalu pk-yritysten järjestelmien turvaamisessa. Palomuureja pitäisi käyttää kaikkien kriittisten järjestelmien suojaamisessa, erityisesti yrityksen verkon suojaamiseksi internetin suuntaan.

ETÄHALLINTARATKAISUJEN ARVIOINTI

Pk-yritysten pitäisi säännöllisesti varmistaa etähallintatyökalujen turvallisuus, erityisesti:

- varmistaa, että kaikki etähallintaohjelmistoihin on tehty tarvittavat korjaukset ja että ne ovat ajan tasalla
- rajoittaa etäpääsyä epäilyttävistä maantieteellisistä sijainneista tai tietyistä IP-osoitteista
- rajata työntekijöille pääsy vain sellaisiin järjestelmiin ja tietokoneisiin, joita he tarvitsevat työssään
- edellyttää vahvojen salasanojen käyttöä etäpääsyssä ja mahdollisuuksien mukaan ottaa käyttöön kaksivaiheinen tunnistus
- varmistaa, että tarkkailu ja hälytykset ovat käytössä varoittamassa epäillyistä hyökkäyksistä tai epätavallisesta epäilyttävästä toiminnasta.

8 FYYSISEN TURVALLISUUDEN PARANTAMINEN

Asianmukaisia fyysisiä varotoimia on noudatettava siellä, missä säilytetään tärkeitä tietoja. Yrityksen tietokonetta tai älypuhelinta ei saa jättää auton takapenkille. Käyttäjän on aina lukittava tietokone lähtiessään pois sen ääreltä. Kaikkiin yritystoiminnassa käytettäviin laitteisiin kannattaa ohjelmoida automaattinen lukitus. Arkaluontoisia paperisia asiakirjoja ei saa jättää valvomatta, ja niitä on säilytettävä turvallisessa paikassa silloin, kun niitä ei tarvita.

9 TURVALLISET VARMUUSKOPIOT

Jotta olennaiset tiedot ovat tarvittaessa palautettavissa, niistä on tehtävä varmuuskopioita. Niiden avulla esimerkiksi kiristysohjelmahyökkäyksen kaltaisesta ongelmatilanteesta palautuminen on tehokasta. Seuraavat varmuuskopiointisäännöt ovat suositeltavia:

- varmuuskopiointi on säännöllistä ja automaattista aina kun mahdollista
- varmuuskopiot ovat erillään pk-yrityksen tuotantoympäristöstä
- varmuuskopiot on salattu, erityisesti jos niitä siirretään paikasta toiseen
- varmuuskopioiden toimivuutta testataan säännöllisesti kokeilemalla tietojen palauttamista ihanteellista olisi testata varmuuskopiointiprosessin toimivuus alusta loppuun.

10

PILVIPALVELUT KÄYTTÖÖN

Pilvipalveluihin pohjautuvissa ratkaisuissa on monia etuja, mutta niissä on myös riskejä, jotka pk-yritysten pitää ottaa huomioon ennen pilvipalvelun hankkimista. ENISA on julkaissut pk-yrityksille tarkoitetun pilvipalveluiden turvallisuusoppaan (Cloud Security Guide for SMEs)[2], johon yritysten kannattaa perehtyä pilvipalveluiden käyttöön ryhtyessään.

Palveluntarjoajaa valitessaan yrityksen pitäisi varmistaa, että palveluntarjoaja ei riko lakeja tai säädöksiä säilyttämällä tietoja, erityisesti henkilötietoja, EU-/ETA-alueen ulkopuolella. Esimerkiksi EU:n yleinen tietosuoja-asetuksessa edellytetään, että EU-/ETA-alueen asukkaiden henkilötietoja ei saa säilyttää alueen ulkopuolella tai siirtää sinne kuin tietyin ehdoin.

2 https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

11 TURVALLISET VERKKO-SIVUSTOT

On äärimmäisen tärkeää, että pk-yritykset varmistavat, että niiden verkkosivustot ovat turvallisia ja että turvallisuutta ylläpidetään. Kaikki henkilötiedot ja taloudelliset tiedot, kuten luottokorttitiedot, on suojattava asianmukaisesti. Tähän sisältyvät verkkosivustojen säännöllinen turvallisuustestaus, jotta mahdolliset turvallisuusheikkoudet voidaan havaita, ja säännölliset tarkistukset, joilla varmistetaan sivuston asianmukainen ylläpito ja päivittäminen.

12 TIEDON ETSIMINEN JA JAKAMINEN

Tiedon jakaminen on tehokas työkalu kyberrikollisuuden torjumiseen. Kyberrikollisuuteen liittyvän tiedon jakaminen on tärkeää, jotta pk-yrityksillä on parempi käsitys siitä, millaisia riskejä ne kohtaavat. Yritykset, jotka kuulevat muilta yrityksiltä niiden kyberturvallisuushaasteista ja haasteiden voittamisesta, alkavat todennäköisemmin suojata omia järjestelmiään, kuin jos ne kuulisivat samat asiat ammattialansa raporteista tai kyberturvallisuustutkimuksista.

EUROOPAN UNIONIN
KYBERTURVALLISUUSVIRASTO

TIETOA ENISASTA

Euroopan unionin kyberturvallisuusvirasto, ENISA, on unionin virasto, jonka tarkoituksena on saavuttaa yhteinen korkea kyberturvataso koko EU:ssa. Virasto perustettiin vuonna 2004, ja sitä on myöhemmin vahvistettu EU:n kyberturvallisuusasetuksella. Euroopan unionin kyberturvallisuusvirasto osallistuu EU:n kyberpolitiikan laatimiseen, edistää tieto- ja viestintäteknisten tuotteiden, palvelujen ja prosessien luotettavuutta kyberturvallisuuden sertifiointijärjestelmillä, tekee yhteistyötä jäsenvaltioiden ja EU:n elinten kanssa sekä auttaa EU:ta valmistautumaan tulevaisuuden kyberhaasteisiin. Virasto jakaa tietämystä, kehittää valmiuksia ja lisää tietoisuutta sekä tekee yhteistyötä keskeisten sidosryhmiensä kanssa lujittaakseen luottamusta verkottuneeseen talouteen, parantaakseen unionin infrastruktuurin sietokykyä ja ennen kaikkea suojatakseen eurooppalaisen yhteiskunnan ja kansalaisten digitaalista turvallisuutta. Lisätietoja virastosta on osoitteessa www.enisa.europa.eu.

ENISA
Euroopan unionin kyberturvallisuusvirasto

Ateenan toimisto
Ethnikis Antistaseos 72 &
Agamemnonos 14,
Chalandri 15231, Attiki, Kreikka

Heraklionin toimisto
95 Nikolaou Plastira
700 13 Vassilika Vouton,
Heraklion, Kreikka

enisa.europa.eu