COVID-19 pandemian opetukset: Turvallisuuden ja toiminnan jatkuvuuden suunnittelu

WatchGuard®

Sisältö

Johdanto 3

Tilanteen analysointi - COVID-19: Toiminnan jatkuvuuteen liittyvät haasteet. 4

Kahdeksan vinkkiä turvalliseen etätyöskentelyyn 6

Miksi valmiudella on merkitystä tietoturvallisuuden kannalta? 13

Toiminnan jatkuvuuden tarkastuslista. 14

WatchGuard palvelut pienille ja keskisuurille yrityksille haasteellisina aikoina 15

JOHDANTO

Yhteiskuntaa on kohdannut laajamittainen pandemia, ja uusi koronavirus (COVID-19) vaikuttaa käytännössä meihin kaikkiin. Koulut on suljettu, matkustamista on rajoitettu voimakkaasti, tapahtumat on peruutettu ja toimistot ovat tyhjentyneet. Näiden toimien tavoitteena on hillitä viruksen leviämistä. Yhdysvaltojen tautikeskus (Center for Disease Control) on jopa ehdottanut, että työnantajien tulisi laatia käytännöt etätyöskentelyä varten edistääkseen ihmisten liikkumisen rajoittamista. Yritykset ovat tarttuneet haasteeseen ja ryhtyneet ripeästi toimiin viruksen leviämisen estämiseksi. Tällä hetkellä etätyötä tekee enemmän ihmisiä kuin todennäköisesti koskaan aikaisemmin. Tutkimustietojen mukaan kyse on todella suuresta murroksesta, sillä pelkästään Yhdysvalloissa etätyön määrä kasvoi 159 % vuosina 2005-2017. Myös Suomi erottuu Euroopan tasolla etätyön kärkimaaksi: jo 60% työvoimasta on siirtynyt etätöihin koronaviruksen takia.

Koronaviruksen vastaiseen taisteluun tarvittavat toimet ovat olleet uskomattoman laaja-alaisia, ja useat yritykset ovat joutuneet turvautumaan etätyöskentelyyn ensimmäistä kertaa. Tässä e-kirjassa esitellään toiminnan jatkuvuuden turvaamiseen liittyviä strategioita koronaviruspandemian aikana.

TILANTEEN ANALYSOINTI - COVID-19:
TOIMINNAN JATKUVUUTEEN LIITTYVÄT HAASTEET

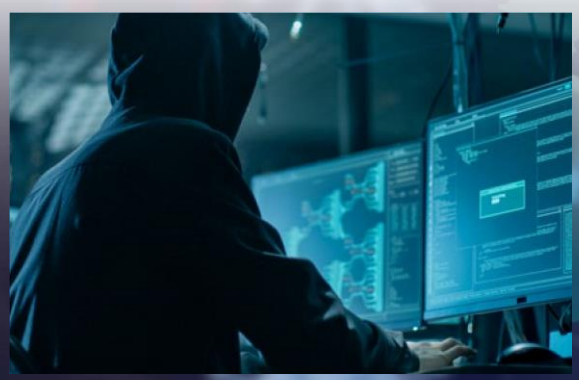
Kohtaamme päivittäin kyberturvallisuuteen liittyviä riskejä. Eräs näistä haasteista on mobiilin työvoiman huomattavasti aiempaa suurempi riski altistua verkkohyökkäyksille. Ilman yrityksen sisäverkon suomaa turvaa etätyötä tekevä voi joutua huomaamattaan kyberhyökkäyksen kohteeksi, ja jopa mahdollistaa sen leviämisen laajemmalle järjestelmään kytkeytyessään uudelleen yrityksen sisäverkkoon.

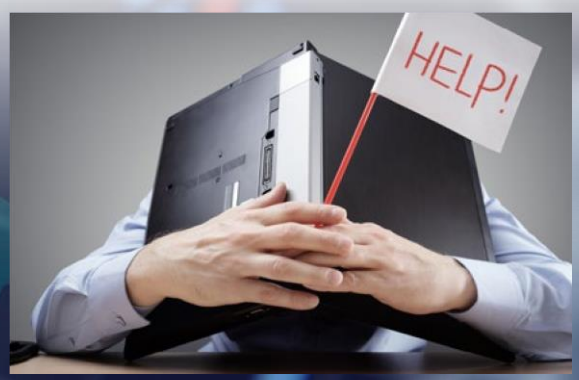
Hakkerit käyttävät hyväkseen koronavirukseen liittyvää pelkoa

Hakkerit näyttävät hyödyntävän kaikki suuremmat otsikot ja tapahtumat hyökkäyksissään. Pelon kasvaessa työntekijöiden sähköposteihin ja sosiaaliseen mediaan suorastaan satelee virukseen liittyviä uutisia, raportteja, kommentteja, videoita ja linkkejä. Valitettavasti kyberrikolliset käyttävät lisääntynyttä pelkoa hyväkseen kalastellakseen käyttäjien tietoja, murtautuakseen järjestelmiin ja levittääkseen haittaohjelmia.

Muutamia esimerkkejä siitä, miten pandemiaa hyödynnetään:

- **Maailman terveysjärjestön (WHO) imitointi** . WHO on raportoinut epäilyttävistä järjestön nimissä lähetetyistä verkkourkintaviesteistä, joiden väitetään sisältävän kriittistä terveyteen liittyvää tietoa. Viestin saajaa pyydetään klikkaamaan linkkiä, lataamaan tiedosto ja ilmoittamaan arkaluontoisia tietoja.
- **Haittaohjelmien levitys**. Mongoliassa eräs hakkeriryhmä on levittänyt aiemmin tuntematonta Vicious Panda -haittaohjelmaa pandemian turvin.
- **Emotet-troijalainen**. Japanissa hakkerit käyttivät ensisilmäyksellä hyödyllisiä koronaviruksen leviämisen estämiseen liittyviä viestejä Emotet-troijalaisen levittämiseen osana roskapostikampanjaa. Emotet on tehokas troijalainen, joka kykenee kaappaamaan sähköpostitilejä ja lähettämään huijausviestejä.
- **Tekaistun viruksenseurantasovelluksen kylkiäisenä tulee kiristysohjelma.** Koronaviruksen leviämisen seurantaan tarjottu sovellus on tosiasiassa puhelimen lukitseva kiristysohjelma. ”COVID19 Tracker” saastuttaa laitteen ja vaatii 100 dollarin arvosta Bitcoineja 48 tunnissa.





Aloittelevat etätyöntekijät

COVID-19 johti etätyön voimakkaaseen yleistymiseen yritysten sulkiessa toimistoja ja lähettäessä työntekijät työskentelemään kotiin miltei olemattomalla varoitusajalla. Työnteon joustavuus on normi yhä useammille yrityksille, mutta etätyöskentelyä hyödynnetään keskimäärin vain noin 30 %:ssa yrityksistä. Etätyön turvallisuuden varmistaminen on ollut haaste useille yrityksille, sillä kannettavat tietokoneet oli järjestettävä nopeasti, ja joissain tapauksissa koteihin on jouduttu viemään myös turvallisesta verkosta irti kytkettyjä pöytäkoneita. Näiden verkosta irrotettujen laitteiden turvallisuus on varmistettava, ja samalla on varmistettava, että nämä samat laitteet eivät levitä haittaohjelmia ja muita uhkia, kun ne kytketään takaisin verkkoon. Nämä varmistukset voidaan tehdä VPN-yhteydellä tai palaamalla takaisin toimistoon.

Ylikuormitettu VPN

VPN-yhteyden käyttö on monikertaistunut koronaviruksen sulkiessa ihmiset koteihinsa. Tutkimusten mukaan liikenne Yhdysvalloissa kasvoi viikossa 50 %. VPN-yhteyksien järjestäminen toimistolta kotikonttoreihin siirtyneille työntekijöille on ollut haasteellista useille yrityksille. VPN-yhteyden puuttuminen voi johtaa siihen, että käyttäjät turvautuvat suojaamattomiin yhteyksiin voidakseen käyttää työssä tarvitsemiaan resursseja.

Kaistanleveysahdinko

Kotona on muitakin kuin työtä tekeviä. Koulut on suljettu, joten useiden työntekijöiden lapset ovat kotona. Etäopiskelun ohella lapset pelaavat ja surffaavat verkossa. Sekä lapset että aikuiset tarvitsevat entistä nopeammat yhteydet, erityisesti paljon resursseja kuluttavien sovellusten käyttöön. Tästä erilaiset etäkokoukset ovat oiva esimerkki. Viruksesta pahiten kärsineillä alueilla internetin käyttö on kasvanut yli 90 %. Kyetäkseen vastaamaan kysyntään useat ISP:t ovat päivittäneet asiakkaidensa yhteydet ja poistaneet datakatot varmistaakseen yhteyksien toimivuuden.

VPN-yhteyksien käyttö on moninkertaistunut,

liikenne on kasvanut 50 %

pelkästään yhdessä viikossa

Yksistään Yhdysvalloissa

VPN-yhteyden käytön odotetaan kasvavan 150% kuukaudessa.

KAHDEKSAN VINKKIÄ TURVALLISEEN ETÄTYÖSKENTELYYN

1. INVENTOI JA ARVIOI YRITYKSESI ETÄTYÖRESURSSIT

Vaikka 92 % yrityksistä on mahdollistanut etätyöskentelyn työntekijöilleen, kaikilla työntekijöillä ei ole tasavertaisia mahdollisuuksia tehdä etätyötä. Useissa yrityksissä etätyöhön siirtyminen tapahtui miltei yhdessä yössä, eikä riittävään suunnitteluun ollut yksinkertaisesti aikaa. Viimeistään nyt on aika tarkistaa ja arvioida yrityksen verkkoyhteydet ja huomioida turvallisuuteen liittyvät näkökohdat. Tietoturvapalveluiden tarjoajat (MSSP) ovat turvallisuusarviointien asiantuntijoita, jotka auttavat asiakkaitaan pääsemään nopeasti tilanteen tasalle.

Jatkuvasti paikkaa vaihtavilla verkkonomadeilla on jo todennäköisesti kaikki tarvittava pidemmälläkin aikavälillä. Sen sijaan ne työntekijät, jotka eivät ole aiemmin tehneet etätyötä, kannattaa siihen erikseen perehdyttää. Esimiesten on ymmärrettävä tiiminsä yksilölliset tarpeet ja varmistettava, että jokainen työntekijä suoriutuu tehtävistään myös etätöissä.

Tarkastuslista huomionarvoisista seikoista:

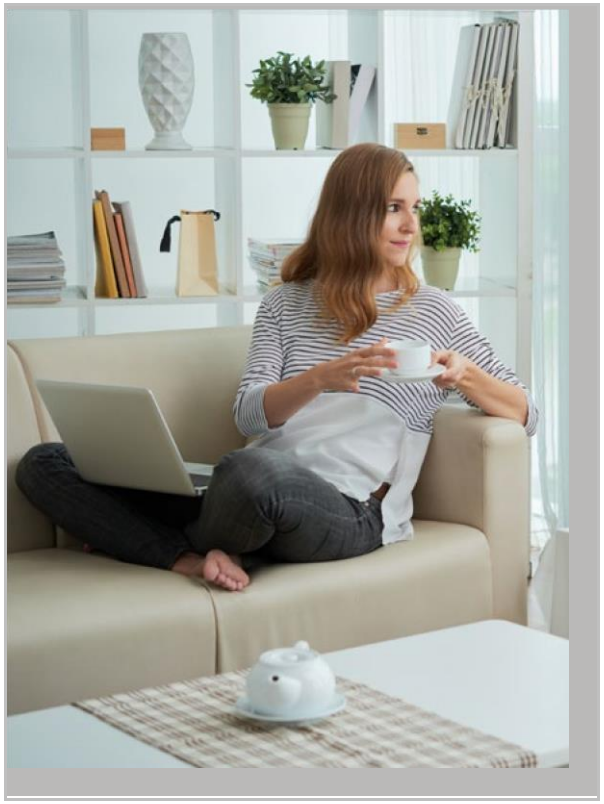
- ✔ Onko työntekijällä hyväksytty laite, ja tarvitaanko puhelimia tai kannettavia tietokoneita lisää?
- ✔ Onko VPN-lisenssejä/kapasiteettia riittävästi vai onko niitä lisättävä?
- ✔ Onko työntekijällä työskentelyyn tarvittava riittävän nopea yhteys?
- ✔ Millaisia järjestelmiä työntekijä tarvitsee työtään varten?
- ✔ Tarvitseeko työntekijä turvallisen yhteyden arkaluontoisiin järjestelmiin ja tietoihin?
- ✔ Millaisia pilvipalveluja työntekijä käyttää säännöllisesti?
- ✔ Voiko työntekijä käyttää monivaiheista varmennusta?

2. ETÄTYÖN ODOTUSTEN MÄÄRITYS JA VIESTIMINEN

Useat työntekijät tekevät etätyötä todennäköisesti ensimmäistä kertaa, joten juuri nyt on oikea aika laatia etätyökäytännöt. Noin 24 % yrityksistä ei ole päivittänyt etätyökäytäntöään yli vuoteen, joten viimeistään nyt käytännöt on päivitettävä.

Muutamia huomionarvoisia seikkoja:

- **Työajat** - millaisia työpäiviä odotat tiimisi tekevän? Milloin olet itse alaistesi käytettävissä?
- **Vastaaminen** - odotetaanko etätyöntekijöiden vastaavan heti? Jos, niin miten tämä tapahtuu? Välitetäänkö todella kiireelliset pyynnöt yksinomaan puhelimitse?
- **Alustat** - muistuta työntekijöitä työkaluista ja alustoista, joita heidän odotetaan käyttävän, mukaan luettuna pilvipalvelut, videokokoussovellukset, projektinjohtotyökalut jne. Pyydä työntekijöitä välttämään kaikkia muita hyväksymättömiä alustoja.
- **Laitteet** - jos tiimilläsi on työnantajan järjestämät laitteet, muistuta heitä niiden käyttöön liittyvistä käytännöistä. Jos työntekijät käyttävät omia laitteitaan työskentelyyn, laadi ohjeistukset sopivista laitteista ja niiden käytöstä.
- **Tietoturvaloukkausten raportointi** - keneen työntekijän tulee ottaa yhteyttä, jos hänellä on syytä epäillä yrityksen tietojen vaarantumista? Kenelle tietoturvaloukkauksista on ilmoitettava, ja millaisiin toimiin on ryhdyttävä haittojen minimoimiseksi?



3. KYBERTURVALLISUUTTA PAINOTTAVA YRITYSKULTTUURI

Useimmat esimiehet ymmärtävät, että työpaikan ilmapiirillä on merkittävä vaikutus onnistumiseen ja myös epäonnistumiseen. Sama dynamiikka pätee myös kyberturvallisuuteen. Työntekijät ovat potentiaalisia kohdennettujen verkkohyökkäyksien kohteita, ja toisinaan tämä tarkoittaa myös tiimin jäseneksi naamioitumista. Näissä tapauksissa yrityskulttuuri on usein se erottava tekijä, joka auttaa estämään hyökkäyksen ja jopa koko verkon saastumisen.

Hakkerit hyödyntävät erilaisia tekniikoita manipuloidakseen ja saadakseen työntekijät ryhtymään haluamiinsa toimiin. Kiireellisyyttä ja asiantuntemusta käytetään usein työkaluina. Johtajan tulee rohkaista avoimeen viestintään, jotta organisaation työntekijät rohkenevat ilmoittaa mahdollisesta uhasta, koska he tietävät, että heidät otetaan vakavasti.

Vinkkejä kyberturvallisuutta painottavan yrityskulttuurin edistämiseen:

- **Jaa tarinoita.** Työntekijä sai kalasteluviestin tai koneelle asennettiin kiristysohjelma? Tarinan kertominen eteenpäin yrityksessä voi auttaa tekemään uhasta todellisemman työntekijöille ja auttaa siten välttämään vastaavat tilanteet. Samantyyppisiin yrityksiin kohdistuneista hyökkäyksistä kertovien uutisten jakaminen.
- **Toiminnasta palkitseminen.** Mahdollisesta hyökkäyksestä ilmoittava työntekijä voi säästää yrityksesi paljolta päänvaivalta, joten siitä kannattaa palkita, eikö vain? Työntekijöiden kannustaminen epäilyttävästä toiminnasta raportoimiseen voi auttaa lisäämään tietoisuutta ja osallistumista.
- **Ole ystävällinen.** Yritykset koostuvat loppujen lopuksi ihmisistä, joiden tekninen osaaminen vaihtelee. Ei ole yksinkertaisesti realistista, että kaikki työntekijät pystyvät välttämään kaikki uhat ja noudattaisivat joka ikistä käytäntöä. Me teemme virheitä. Siksi on tärkeää auttaa ja tukea muita.

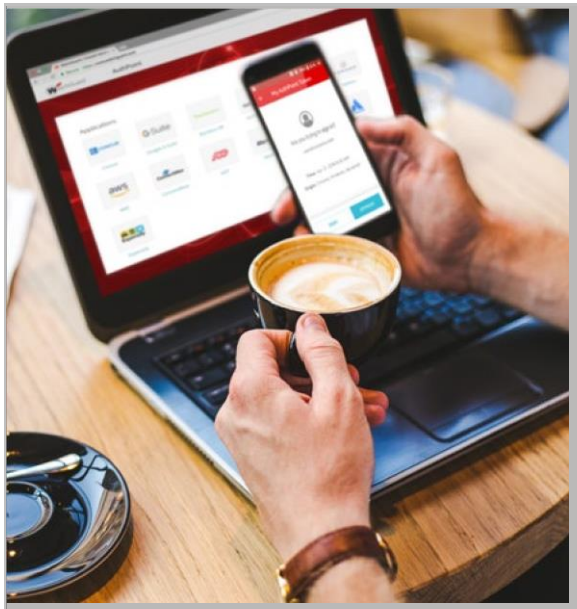
4. MONIVAIHEISEN TUNNISTAUTUMISEN (MFA) KÄYTTÖÖNOTTO

Yrityksen sisäisten työkalujen turvalliseen käyttöön liittyy omat haasteensa valtaosan työntekijöistä siirryttyä etätyöhön. Samaan aikaan hakkerit pyrkivät aktiivisesti saamaan käyttäjätilien tiedot haltuunsa. Tästä syystä suosittelemme monivaiheisen tunnistautumisen käyttöä käyttäjän todentamiseksi.

Monivaiheinen tunnistautuminen takaa myös turvallisen pilvipalvelujen sekä sisäverkossa käytettävien palvelujen käytön. Näin varmistetaan tarpeellinen täydentävä suojaus yritysten ollessa haavoittuvaisimmillaan.

Vaatimukset monivaiheiselle tunnistautumiselle:

- **Pilvipalvelu.** Käyttäjä voi ladata sovelluksen suoraan puhelimeen pilvipalvelusta ja ryhtyä käyttämään sitä välittömästi toisin kuin laitteistoon kytkettäviä tunnisteita käytettäessä.
- **Suojauksen laajuus.** Ratkaisun tulisi suojata kaikki työntekijöiden tarvitsemat kriittiset sovellukset.
- **Helppokäyttöisyys.** Sovelluksen tulisi olla helppokäyttöinen kaiken tasoisille käyttäjille.
- **Useat varmennusmenetelmät.** Useamman verkossa ja verkon ulkopuolella tehtävän varmennuksen yhteensopivuuden ansiosta käyttäjät voivat käyttää tarvitsemiaan tietoja ja työkaluja juuri silloin, kun niitä tarvitaan.
- **Useat tunnisteet.** Sosiaalinen media, pankit, verkkokaupat ja useat muut palveluntarjoajat käyttävät nykyään monivaiheista varmennusta. Kannattaa etsiä ratkaisu, joka mahdollistaa tunnisteiden yhdistämisen yksinkertaiseen monivaiheiseen varmennussovellukseen ongelmattoman pääsyn varmistamiseksi koko henkilöstölle.

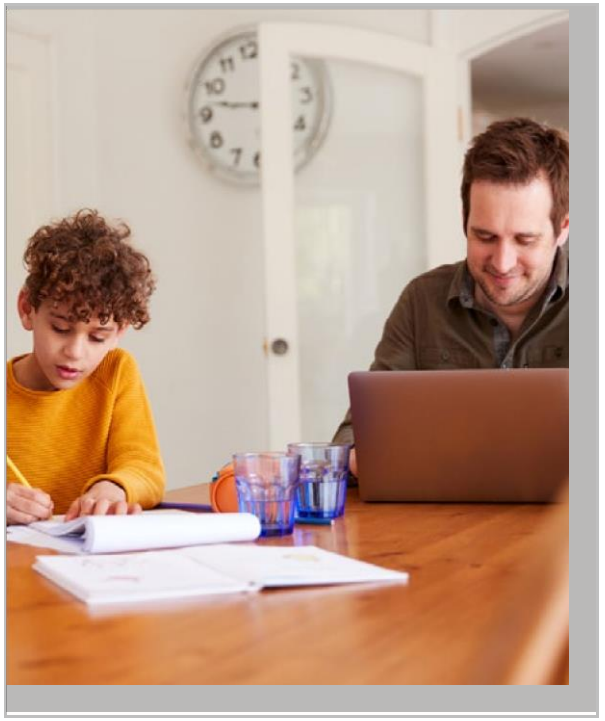


5. VPN-YHTEYDEN KÄYTTÖ

Ehdottoman toimiva yhteys pääkonttorin ja kriittisten sovellusten välillä on erityisen tärkeää silloin, kun työntekijöiden tuottavuuden ei haluta heikentyvän etätöissä. VPN-yhteyden avulla varmistetaan yksityisten ja julkisten verkkojen turvallisuus, jotta henkilöt ja yhteisöt voivat lähettää sekä vastaanottaa tietoa turvallisesti verkossa.

Yleensä yritykset tarjoavat VPN-yhteyden vain rajatulle työntekijäryhmälle tai paljon matkustaville työntekijöille. Olemme laatineet muutamia vinkkejä VPN-yhteyden käytön hallintaan häiriöiden välttämiseksi:

- **Priorisoi VPN-yhteyden käyttö**. Toiset työntekijät tarvitsevat toisia enemmän pääsyoikeuksia, ja osa työntekijöistä ei välttämättä tarvitse VPN-yhteyttä lainkaan. Käyttötarpeen määrittäminen ja VPN-yhteyden käytön priorisointi auttaa välttämään verkon ylikuormittumista.
- **Pilvipalvelun palomuuri auttaa vastaamaan kysyntään.** VPN-palvelujen kysynnän kasvu ei edellytä kuitenkaan lisätilan raivaamista palvelimelta. Pilvipalveluna toimivat palomuurit voivat auttaa tasoittamaan pääkonttoriin liittyvää VPN-liikennettä ja varmistamaan tarvittavan skaalauksen, jotta tarpeelliset yhteydet toimivat.
- **Monivaiheinen tunnistautuminen vaaditaan.** Ilman monivaiheista tunnistautumista VPN-yhteyden käyttö voi pahimmassa tapauksessa antaa hakkereille täyden pääsyn yrityksesi verkkoon.
- **Käytä palomuuria.** Käyttäjän kotikonttorissa käyttämä palomuuri voi tarjota täyden suojauksen (UTM) rasittamatta turhaan yrityksen VPN-yhteyttä.

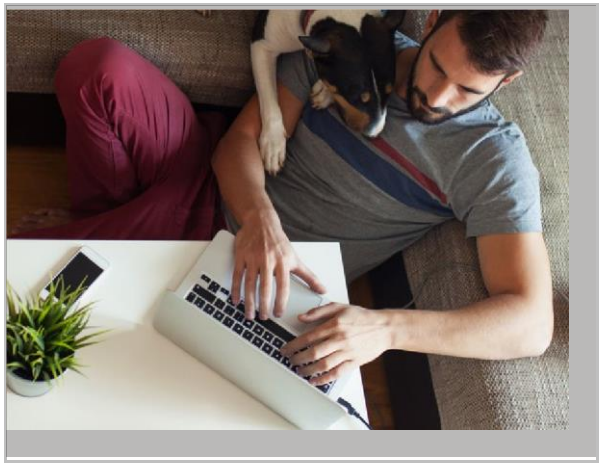


6. WATCHGUARD DNSWATCH SUOJAA KÄYTTÄJIÄ VAARALLISILTA KLIKKAUKSILTA

Käyttäjien turvallisuuden varmistaminen verkossa on entistäkin haasteellisempaa nyt, kun verkkoa käytetään kotoa käsin. Kotona työskentelevät käyttävät työkonetta todennäköisesti myös verkossa surffailuun ja yksityisen sähköpostin lukemiseen. Pilvipohjainen WatchGuard DNSWatch estää ja rajoittaa pääsyn kalastelusivuille. Vaarallisten linkkien avaaminen ja tietojen kalasteluun ja haittaohjelmiin liittyville sivustoille pääsy voidaan estää ilman VPN-yhteyttä.

Muista nämä DNS-suojauksesta:

- **Tuottavuus ja käytännön juurruttaminen.** Yhä useamman työskennellessä kotoa käsin myös käyttäjien pääsyä tietynlaiseen sisältöön voi olla tarpeen rajoittaa työn tuottavuuteen liittyvistä syistä. Tällaisia sivustoja ovat sosiaalisen median ohella myös aikuisviihdesivustot. Tähän tarkoitukseen sopivat esimerkiksi käyttäjien ja ryhmien estäminen sekä keston määrittely.
- **Turvallisuuskoulutuksen tehostaminen.** Useimmat yritykset ovat järjestäneet kyberturvallisuuskoulutusta työntekijöilleen, mutta etätyöskentelyssä koulutuksen merkitys kasvaa entisestään. Osa DNS-suojauksista ei pelkästään estä kelvottomia yhteyksiä, vaan muistuttaa myöhemmin samantyyppisistä vaaroista.



7. PIDÄ HAITTAOHJELMAT POISSA TYÖNTEKIJÖIDEN KONEILTA

Haittaohjelmien ja kiristysohjelmien määrä on kasvanut koronapandemian aikana. Tartuntariski ei ole vielä koskaan ollut yhtä korkea, sillä käyttäjillä ei ole enää työpaikan palomuuria suojanaan. Työntekijöiden koneille asennettavat virusohjelmat nappaavat useimmat uhat, mutta ne eivät pysty kuitenkaan suojaamaan nykyään niin yleisiltä nollapäivähaittaohjelmilta. EDR-ratkaisut pystyvät yleensä näiden pitkälle kehitettyjen uhkien havaitsemisen lisäksi myös poistamaan uhan ja palauttamaan laitteen entiselleen. Ja tämä kaikki tapahtuu kokonaan etänä.

EDR-ratkaisujen ominaisuudet:

- **Havaitseminen.** Edistyneiden haittaohjelmien havaitseminen edellyttää pitkälle kehitettyjä menetelmiä. Kannattaa etsiä sellaisia ratkaisuja, joissa yhdistellään useita havaitsemismenetelmiä, kuten toiminnallista ja heuristista analysointia ja hiekkalaatikkoanalytiikkaa.
- **Automaatio ja tekoäly.** Nopea uhkiin vastaaminen voi säästää paljolta vaivalta. Automaattisen havaitsemisen ja reagoinnin ansiosta tämä onnistuu miltei hetkessä.
- **Laitteiden eristäminen.** Uhkan havaitsemisen jälkeen kyseinen laite tulisi kytkeä irti verkosta viruksen leviämisen estämiseksi.

8. Varmista langattoman verkon turvallisuus

Kotona työskenneltäessä myös langaton verkko voi olla turvallisuusriski. Esimerkiksi kerrostalossa asuville kaikki kodin langattomat laitteet, kuten ovikellot, pelikonsolit ja IoT-laitteet, voivat pahimmassa tapauksessa olla turvallisuusriski, jota pahantahtoiset naapurit voivat hyödyntää. Rikolliset naapurit voivat nähdä mahdollisuutensa tulleen, kun talossa on paljon kotoa käsin työskenteleviä, ja langattoman verkkoyhteyden käyttö muodostaa jopa puolet kaikesta IP-liikenteestä.

Tärkeää tietoa langattoman verkon käytöstä etätyössä:

- Luotettavien liitäntäpisteiden, kuten WatchGuard AP225W:n käyttö lisää tietohallintopalvelujen näkyvyyttä asiakkaalle ja tehostaa verkon toimintaa, jotta etätöitä tekeville työntekijöille voidaan tarjota entistä parempaa IT-tukea.
- **Konfiguroi liitäntäpisteet valmiiksi** helpon käytön varmistamiseksi.

Tiheään asutuilla alueilla, kuten asuinkerrostaloissa, langattoman verkon käyttö muodostaa jopa **50% kaikesta IP-liikenteestä**

MIKSI VALMIUDELLA ON MERKITYSTÄ TIETOTURVALLISUUDEN KANNALTA

Koska kaikkea ei voi ennakoida, on varauduttava yllätyksellisyyteen. Miten yrityksen toiminnan jatkuvuus voidaan siten turvata? Valmiussuunnitelma ei takaa täydellistä onnistumista, mutta se tarjoaa työkalut haasteista selviytymiseen sekä toiminnan jatkuvuuden varmistamiseen.

Tänään se on koronapandemia, mutta huomenna se voi olla jotain aivan yhtä haasteellista. Suuret urheilutapahtumat, kuten vaikkapa maailmanmestaruuskisat, vaikuttavat merkittävästi järjestävän kaupungin arkeen, ja samaan tapaan yksi inhimillinen erehdys riittää siirtämään yrityksen kriittiseen valmiustilaan. Kaikki sellaiset tapahtumat, jotka pakottavat yrityksen mukautumaan yllättäviin muutoksiin ovat esimerkki siitä, miten tärkeää on tuntea organisaatio ja sen tarpeet perusteellisesti.

Miksi? Koska näin näytät työntekijöille, asiakkaille ja sidosryhmille, että yrityksesi menestyy myös yllättävissä olosuhteissa. Tästä on varmasti hyötyä brändillesi, mutta sitäkin tärkeämpää on luottamuksen kasvaminen yritystäsi kohtaan yhteisön sisällä. Lisäksi sinulla on upea tarina kerrottavanasi vielä vuosienkin päästä.

Miksi? Koska se kertoo työntekijöille, asiakkaille ja sidosryhmille, että yrityksesi menestyy myös yllättävissä olosuhteissa.

YRITYKSEN IT-TOIMINTOJEN JATKUVUUDEN TARKASTUSLISTA

Yrityksesi etätyöresurssien arviointi

Onko yritykseni valmistautunut?	Kyllä	Ei	Ohjeet
Onko etätyökäytäntö päivitetty viimeisen 12 kuukauden aikana?			
Onko käytäntö ja kaikki odotukset viestitty kaikille etätyötä tekeville?			
Tarvitaanko lisää puhelimia tai kannettavia tietokoneita, jotta kaikilla työntekijöillä olisi varmasti hyväksytyt laitteet?			
Onko VPN-lisenssejä/kapasiteettia riittävästi?			
Onko työntekijällä työskentelyyn tarvittava riittävän nopea yhteys?			
Onko etätyötä tekevillä riittävä pääsy työtehtävien edellyttämiin tärkeisiin alustoihin ja järjestelmiin? *Toisin sanoen pilvisovellukset?*			
Pystyykö yritys tarjoamaan turvalliset keinot kyberhyökkäysten välttämiseen myös etätyössä? *Toisin sanoen suojattu langaton verkko, VPN ja monivaiheinen varmennus*			
Onko budjettia tarvittaessa kasvatettava?			
Täytyykö työntekijöitä kouluttaa turvalliseen etätyöskentelyyn?			

WATCHGUARD PALVELUT PIENTEN JA KESKISUURTEN YRITYSTEN AUTTAMISEKSI ENNENNÄKEMÄTTÖMÄN MAAILMANLAAJUISEN KRIISIN AIKANA

WatchGuard tarjoaa yrityksille Passport ratkaisun varmistamaan turvallisen etätyöskentelyn. WatchGuard Passportissa on useita käyttäjäkeskeisiä turvallisuuspalveluja, jotka on niputettu kätevästi yhteen tietojen kalasteluyritysten estämiseksi, verkkokäytäntöjen juurruttamiseksi ja henkilöllisyyden varmentamiseksi maailmanlaajuisesti.

Ota yhteyttä WatchGuard jälleenmyyjääsi saadaksesi lisätietoa WatchGuard Passport-tarjouksesta. Voimassa rajoitetun ajan.

Lue lisää

Lisää tietoa saa ottamalla yhteyttä valtuutettuun WatchGuardin jälleenmyyjään tai sivustolta **https://www.watchguard.com.**

WatchGuard

WatchGuard® Technologies, Inc. on johtava maailmanlaajuinen verkkoturvallisuuden, turvallisten langattomien verkkojen, varmennuksen ja älykkäiden verkkopalvelujen tarjoaja. Yrityksen palkittuja tuotteita ja palveluja myy miltei 10 000 alan jälleenmyyjää ja palveluntarjoajaa maailmanlaajuisesti yli 80 000 asiakkaalle. WatchGuardin missiona on tuoda yritystason turvallisuus helposti kaikkien yritysten ulottuville koosta ja toimialasta riippumatta. WatchGuard on ihanteellinen ratkaisu erityisesti keskisuurille ja hajautetuille yrityksille. WatchGuardin pääkonttori on Seattlessa, ja yrityksellä on toimipisteet kaikkialla Pohjois-Amerikassa, Euroopassa, Aasian ja Tyynenmeren alueella ja Latinalaisessa Amerikassa. Lisätietoja WatchGuard.com.