Kyber-ilmastonmuutos

Ohjeita yksilöille, yrityksille ja päättäjille

Elmo


8#1X?M%PASSWORD3Q

Sisällys

1. Kyberilmaston-muutos

Pidä pää kylmänä ja varaudu

Jo vuoden 2020 Vastaamo-tietomurto ja viimeistään 2022 vuoden alun muutokset Euroopan turvallisuustilanteessa osoittavat, että kyberilmasto on muuttunut pysyvästi. Sähköisen maailman ovia ja lukkoja kokeillaan, ja kybermaailman taskuvarkaat käyvät varomattomien taskuissa.

Kyberilmastonmuutos vaatii toimenpiteitä nyt ja meiltä kaikilta.

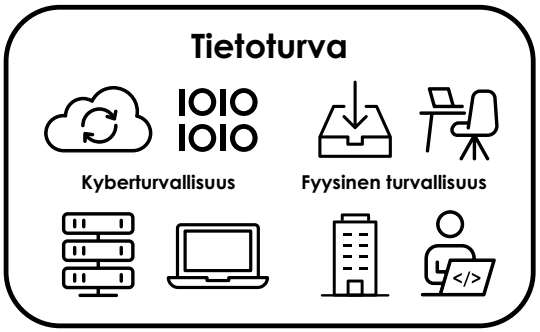
Tieto- ja viestintätekniikka on tärkeä, arvokas ja välttämätön osa yritysten ja yhteisöjen liiketoimintaa - samoin kuin ihmisten valmius hallita ja turvata omaa toimintaansa digitaalisessa maailmassa.

Näiden asioiden tärkeys, arvo ja välttämättömyys tulevat yhä kasvamaan tulevaisuudessa.

Hyvä uutinen on, että paljon on tehtävissä. Varuillaan on hyvä olla, mutta paniikkiin ei ole syytä. Oikeilla valinnoilla ja toimenpiteillä uhat saadaan hallintaan.

2. Tietoturva ei ole pelkästään kyberturvaa

Tietoturva eli tietoturvallisuus tarkoittaa tiedon saatavuuden, luottamuksellisuuden ja eheyden ylläpitämistä. Tämä tarkoittaa, että tieto on saatavilla silloin, kun sitä tarvitaan ja sille, jolla on siihen käyttöoikeus. Tieto ei saa muuttua tahattomasti. Turvattava tieto voi ilmetä useassa eri muodossa. Näitä ovat esimerkiksi digitaaliset tallenteet, fyysiset tallenteet sekä ihmisten, kuten työntekijöiden, tietämys. Tietoturva koskee tiedon suojaamista myös sen siirtämisen aikana.



Kyberturvallisuus on tietoturvallisuuden osa-alue, joka koskee digitaalisessa muodossa olevia tietoja, näiden käyttöä, käsittelyä, tallentamista ja siirtoa. Kyberturvallisuudella pyritään sähköisen ja verkotetun yhteiskunnan ja yritystoiminnan turvallisuuteen. Tieto pitää olla suojattuna turvallisen tietoverkon, virustorjunnan ja hallinnoidun palomuurin takana ja palveluihin pitää olla määritelty vahvat salasanat. Tämä ei kuitenkaan estä tietomurtoa, jos käyttäjä antaa salasanansa huijarille tai huijari päästetään yrityksen toimitilaan ja sitä kautta sisäverkkoon. Tästä syystä on tärkeää, että yritys suunnittelee, hallinnoi ja kehittää tietoturvaa kokonaisuutena eli koskien sekä fyysistä maailmaa (toimitilat, kotitoimistot, ihmiset jne.) että kybermaailmaa.

Mihin nyt pitää varautua?

Suomen ja maailman turvallisuustilanne muuttui Ukrainan sodan seurauksena. Hybridivaikuttamista on nähty ja tullaan näkemään enenevässä määrin.

Tulemme näkemään erilaista kybertoimintaa, jota kohdistetaan yksilöihin, yrityksiin ja julkishallintoon. Luvussa 5 on esitetty viisi nostoa liittyen yksityisten ja yritysten varautumiseen. On mahdollista, että tulemme näkemään ja kokemaan myös täysin uudenlaisia toimia, joita emme pysty ennakoimaan. Tähänkin pitää pyrkiä varautumaan.

Hybridivaikuttaminen (engl. hybrid operations) on valtion poliittiseen järjestelmään kohdistuvaa ulkovaltojen vihamielistä vaikuttamista. Hybridivaikuttamisessa pyritään hyödyntämään kohdemaan erilaisia haavoittuvuuksia. Toiminta tehdään mahdollisimman peitellysti. Keinovalikoimaan voivat kuulua esimerkiksi poliittiset, diplomaattiset, taloudelliset ja sotilaalliset keinot sekä informaatio- ja kybervaikuttaminen (Wikipedia).

Tietoturvariskeihin voidaan yleisesti varautua kahdella tavalla

1

Ensimmäinen tapa ovat toimenpiteet, jotka pienentävät riskin tapahtumisen todennäköisyyttä. Tällöin taustaoletus on, että uhka on tunnistettu. Kuten kerrottu, saatamme nähdä tulevaisuudessa myös täysin uusia toimia. Ammattimaisen tietoturvan hallintamallin mukaisella riskianalyysillä ja sipulisuojauksella (katso luku 5.3) pystytään näihinkin uhkiin varautumaan, sillä monikerroksinen suojaus usein pysäyttää myös ennakoimattomat uhat.

2

Toinen tapa on reagointinopeuden kasvattaminen. Mitä nopeammin reagoimme yllättävässä tilanteessa, sitä pienemmät vaikutukset yleensä ovat.

Kaksi vinkkiä!

Tiedä ja tarkista, ennen kuin palkkaat

Ukrainan sodan myötä on nähty rikollisia toimia, joilla on pystytty ohittamaan monet perinteiset tekniset ja hallinnolliset suojaukset. Tämä on tapahtunut soluttautumalla kriittisten järjestelmätoimittajien sisälle ohjelmistokehittäjäksi, jolloin haittaohjelma on rakennettu osaksi virallista ohjelmistopäivitystä.

Kattavassa tietoturvan hallintamallissa (katso luku 4.) on tähänkin työkaluja. **Henkilöstön kattavat ja systemaattiset taustatarkastukset voivat estää rikollisten soluttautumisen yrityksen sisälle.**

Kopioi kriittiset tiedot riippumattomaan paikkaan

Yritysten on tärkeä analysoida omat liiketoimintaprosessinsa ja liiketoimintasovelluksensa ja tunnistaa niistä kriittisimmät. Hyvä testi on kysyä, miten toimimme, jos esimerkiksi asiakastieto menetetään täysin? Modernit pilvipalvelut on hyvin varmistettu ja niiden tietoturvasuojaukset ovat vahvoja. Nykytilanteessa on kuitenkin tärkeä pohtia, miten toimimme, jos varmistus pettää, esimerkiksi jos tieto tuhotaan sisältä käsin, kuten edellä on kuvattu? Tällöin ratkaisu voi olla, että kriittisestä tiedosta otetaan kopio täysin riippumattomaan paikkaan. **Liiketoimintajärjestelmästä riippumaton Excel on usein hyvä työkalu tähän, samoin aika ajoin otettava paperituloste kriittisimmistä tiedoista.**

4. ISO/IEC 27001 tietoturvan hallintajärjestelmä

Paras tapa varautua tietoturvauhkiin on rakentaa yritykselle auditoitu ja sertifioitu tietoturvan hallintajärjestelmä.

Tämä tarkoittaa, että tietoturva huomioidaan ja rakennetaan kaikkiin toimintoihin ja prosesseihin sisään. ISO/IEC 27001 on maailmanlaajuisesti tunnettu ja jatkuvasti kehittyvä standardi, joka antaa parhaan kehyksen analysoida, rakentaa ja kehittää tietoturvallista toimintaa. Vaikka yritys tai yhteisö ei päättäisi panostaa täyteen **sertifiointitasoon, antaa ISO/IEC 27001 -standardi viitekehyksen tietoturvan kehittämiseen ja ohjaamiseen.**

ISO/IEC 27001 -standardi koostuu kahdesta osa-alueesta:

Ensimmäisessä (luvut 4–10) on kuvattu, mitä osa-alueita yrityksen pitää analysoida, kuvata ja toteuttaa osaksi tietoturvanhallintajärjestelmäänsä.

On tärkeää huomata, että ISO/IEC 27001 kattaa kaikki yrityksen toiminnot, ei pelkästään tieto- ja viestintätekniikkaa vaan mukana on lisäksi HR, toimitilat, hallinto, tuotanto, myynti, projektit, johtaminen, ja toki myös tietohallinto.

Toisessa osassa on kuvattu toista sataa hallintakeinoa eli menetelmää, joilla riskejä saadaan pienennettyä.

ISO/IEC 27001 määrittää dokumentteja ja menetelmiä, joita yrityksen on pakko toteuttaa, mutta on huomattava, että jokaisen yrityksen hallintamallin käytännön toteutus on erilainen. ISO/IEC 27001 -toteutuksen voi rakentaa yrityksen liiketoiminnoista, toimintaympäristöstä ja tavoitteista käsin eli panostaa liiketoiminnalle kriittisiin osa-alueisiin ja toimenpiteisiin.

Tiesitkö!

Elmon koko toiminta on ollut ISO/IEC 27001 -sertifioitua lokakuusta 2019 lähtien. Jo ennen tätä panostimme vuosia hallintamallin rakentamiseen. Toimintaamme on kehitetty ja kehitetään jatkuvasti vastaamaan muuttuvaan tietoturvaympäristöön.

Elmon palveluita käyttävät asiakkaat hyötyvät myös siitä, että Elmon koko toiminta ja palvelutuotanto noudattaa ISO/IEC 27001 -standardin vaatimuksia. Ulkopuolisten tietoturva-ammattilaiset auditoivat toimintaa useita kertoja vuodessa. Auditointien lisäksi teemme säännöllisiä teknisiä haavoittuvuustestejä. Elmon koko henkilöstön tietoturvatietoisuuden kehittäminen ja roolipohjaiset tietoturvaosaamisvaatimukset ovat keskeinen osa tietoturvan hallintamalliamme.


Elmo

5. Ohjeita yksilöille, yrityksille ja päättäjille

5.1. Viisi nostoa yksilöille

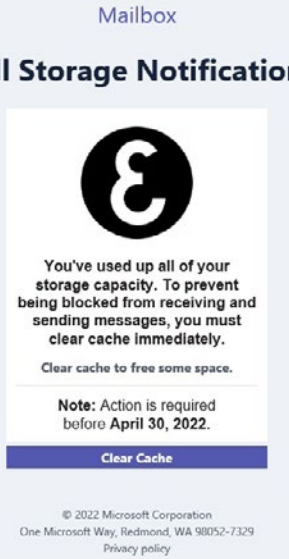
1 **Älä avaa epäilyttäviä viestejä.** Näissä on usein linkkejä, joita pyydetään avaamaan. Pyynnöissä usein kerrotaan, että jokin palvelu vaatii päivitystä ja pyyntö on saatettu muotoilla kuulostamaan kriittiseltä ja kiireiseltä. Pyytäjä on usein tunnettu taho ja sellainen, joka periaatteessa voisi vastaavia kyselyitä tehdä, esim. Microsoft tai IT-palvelun tuottaja.

Usein nopein ja helpoin tapa tunnistaa tällaiset kalastelut on tarkistaa lähettäjän sähköpostiosoite, joka yleensä ei ole palvelun pyytäjän verkko-osoitteen mukainen. Yleisohje, jota kannattaa noudattaa on, että jos yhtään epäilyttää, ei kannata avata tai klikata postia tai sen linkkejä. Tällöin voi kysyä IT-asiantuntijalta neuvoa.

Vastaavia kalasteluviestejä tehdään myös laskunmaksuun liittyen (esim. niin sanottu toimitusjohtajahuijaus). Loma-ajat ovat näille kalasteluille aktiivisinta aikaa, sijaisten hoitaessa töitä. Tällöin pyydetään toimitusjohtajan tai muun päättäjän nimissä vastaanottajaa laittamaan lasku maksuun nopeasti. **Näihin ei pidä reagoida ilman, että varmistaa pyynnön. On tärkeää, että yritys on rakentanut systemaattiset hyväksyntäketjut laskujen käsittelyyn.**

Esimerkki kalasteluviestistä

Ohessa esimerkki väitettyyn IT-ongelmaan liittyvästä kalastelusta. Viesti on ammattimaisesti luotu: Microsoftin osoitetiedot ovat oikein, kuten myös Elmon logo. Kuten näissä usein on, on tässäkin kerrottu, että asialla on kiire. Lähettäjän sähköposti on tekijä, joka tässä tapauksessa paljastaa viestin kalasteluksi.



2 **Ota käyttöön monivaiheinen tunnistus** myös henkilökohtaisissa palveluissa. Suurimmassa osassa kuluttajien palveluita tämä on mahdollista. Tämä lisää palvelun turvallisuutta merkittävästi.

3 **Tiedosta ja tunnista informaatiovaikuttaminen:** Valtionhallinnon viestintäsuosituksessa ja tehostetun viestinnän ohjeessa informaatio-vaikuttaminen määritellään toiminnaksi, jolla pyritään järjestelmällisesti vaikuttamaan yleiseen mielipiteeseen, ihmisten käyttäytymiseen ja päätöksentekijöihin sekä sitä kautta yhteiskunnan toimintakykyyn. Vaikuttamisen keinoja ovat esimerkiksi väärien tai harhaanjohtavien tietojen levittäminen ja painostaminen sekä sinänsä oikean tiedon tarkoitushakuinen käyttö (esimerkiksi faktat irrotetaan todellisesta asiayhteydestään). Kyse on strategisesta toiminnasta, jonka tavoitteena on saada kohde tekemään itselleen haitallisia päätöksiä ja toimimaan omaa etuaan vastaan. Usein vielä tiedostamattaan (lähde: Kyberturvakeskus).

On tärkeä arvioida kriittisesti lukemaansa kiinnittämällä huomiota luettuun sisältöön kokonaisuutena: kuka on julkaisija, pystytkö varmistamaan luetun tiedon jostain muista lähteistä ja niin edelleen.

4 **Huolehdi älypuhelimen turvallinen käyttö** esim. vahva salasana kirjautumisessa, näytön lukitseminen ja niin edelleen.

5 **Noudata työnantajan ja IT-palveluntarjoajan ohjeita.** Älä kerro työasioista vieraille. Älä kerro työnantajan ohjeita tai toimintatapoja ulkopuolisille.

5.2. Viisi nostoa yrityksille ja päättäjille

1 **Ymmärrä ja kuvaa yrityksesi tietoturvan nykytila, uhat ja kehityskohteet** kattaen sekä fyysinen maailma että kybermaailma. Tämä on kohtuullinen panostus, ja tässä kannattaa käyttää ISO/IEC 27001 -standardiin perehtynyttä ammattilaista.

2 **Tunnista liiketoiminnan jatkuvuusriskit.** Kuten mainittu luvussa 3., Suomen muuttuneessa tietoturvatilanteessa on todennäköistä, että tulemme kohtaamaan uusia ja yllättäviäkin uhkia. Näihin varautuminen lähtee liikkeelle siitä, että tunnistetaan liiketoiminnalle kriittisimmät prosessit ja näihin liittyvät liiketoimintasovellukset. Tämän jälkeen analysoidaan, miten toimitaan, jos pahin mahdollinen tapahtuu.

3 **Pilviratkaisut ovat yleisesti turvallisia ja hyvä tapa varautua tietoturvaiskuihin.** Tämä pohjaa muun muassa siihen, että alan suuret pilvipalvelutoimijat panostavat voimakkaasti tietoturvaan. Esimerkiksi Microsoft käyttää yli miljardi dollaria vuosittain tietoturvaan ja talossa on lähes 10 000 tietoturva-asiantuntijaa. On ja tulee olemaan sovellusalueita ja liiketoimintatarpeita, jotka kannattaa toteuttaa asiakkaan omalle palvelimelle tai virtualisoituna palvelin-ratkaisuna. Virtualisoitu, tietoturvasertifioitu konesaliratkaisu on tällöin tietoturvallisin ratkaisu ja ammattimaisilla hallinta- ja valvontapalveluilla näiden tietoturva saadaan hyvälle tasolle.

4 **Varmista henkilöstön tietoisuus.** Kouluta henkilökuntaa säännöllisesti tietoturva-asioihin. Useimmiten, kun tietoturvaongelmia tapahtuu, on taustalla inhimillinen tekijä. Kouluttaminen ja tietoisuuden lisääminen on paras tapa tämän riskin hallintaan.

5 **Vaadi ammattimaista tietoturvan hallintamallia ICT-toimijaltasi.** Kattavin ja kansainvälisesti tunnistettu malli on ISO/IEC 27001. Kuten mainittu, tietoturva on paljon muutakin kuin kyberturvaa, mutta tietoturvan peruskallio on ammattimaisesti johdettu tietoturvan hallintojärjestelmä, ja tätä kannattaa vaatia.

Elmo on ISO/IEC27001 -sertifioitu ICT-talo, jolta löytyy tietoturvaan perehtyneitä arkkitehtejä ja konsultteja asiakkaidemme avuksi.

5.3. Kirsikka kakun päälle: sipulisuojaus

Paras tietoturvallisuuden taso saadaan rakennettua, kun käytetään monitasoista suojausta. Tällaista monitasoista suojausta kutsutaan usein sipulisuojaukseksi. Nimi tulee sipulin mallista: vaikka kuorii yhden kerroksen (suojauksen), alta paljastuu useita muita kerroksia (suojauksia).

Sipulin kerroksia voidaan rakentaa esimerkiksi seuraavasti:

1. Tietokoneen kovalevy on salattu.
2. Käytetään vahvaa salasanaa koneelle ja yrityksen verkkoon kirjautumisessa.
3. Käytetään monivaiheista kirjautumista (MFA, multi-factor authentication) eli pelkällä salasanalla ei pääse koneelle.
4. Pidetään tietokoneen käyttöjärjestelmä, ohjelmistot ja ajurit ajan tasalla (tämä on hyvä delegoida IT-palveluntuottajalle ja näin automatisoida).
5. Uudistetaan itse tietokone ja oheislaitteet riittävän usein: tekniikka ja myös tietoturva kehittyvät jatkuvasti. Kolme vuotta on hyvä aika uusia tietokone.
6. Käytetään vahvaa salasanaa ja monivaiheista kirjautumista yrityksen sovelluksiin kirjautumisessa.
7. Noudatetaan puhtaan näytön periaatetta eli aina, kun poistutaan koneelta, näyttö lukitaan (Windows-koneilla ⊞ + L-näppäinyhdistelmä eli painetaan samanaikaisesti ⊞- ja L-näppäimiä).
8. Käytetään näytönsuojaa (privacy filter), jolloin ulkopuoliset eivät näe näytön sisältöä.
9. Ei jätetä tietokonetta autoon, erityisesti ei näkyville.
10. Koulutetaan tietokoneen käyttäjä tietoturva-asioista.

Vaikka koulutus on viimeisenä listalla, se on silti kriittisen tärkeä: kaikki muut sipulin kerrokset voidaan ohittaa, jos käyttäjä tiedostaen, tiedostamatta, vahingossa tai harhaan johdettuna toimii muiden vastaisesti.

6. Mistä lisää tietoa

Elmo on panostanut ja panostaa jatkuvasti tietoturvaan, jotta voimme turvata asiakkaidemme tietotekniikkapalvelut ja liiketoiminnan. Elmon ulkoistusasiakkaille on nimetty asiakaskokemusarkkitehti, joka on hyvä ensi kontakti myös tietoturva-asioissa.

Elmon koko henkilökunta käy vuosittaisen tietoturvakoulutuksen ja kaikkiin tehtäviin on määritelty ko. tehtävän edellyttämät tietoturvavaatimukset. Elmon hallinnollisen ja teknisen tietoturvan konsultit ja arkkitehdit auttavat analysoimaan ja kehittämään asiakkaan tietoturvan hallintamallia. Elmo tekee myös tietoturvatietoisuuden nostamiseen tähtääviä koulutuksia asiakkaille.

Kyberturvakeskukselta (www.kyberturvallisuuskeskus.fi) on saatavissa monenlaista tietoa kyberturvasta:

Kyberturvakeskuksen haavoittuvuustiedotteita sisältävän postituslistan kautta saa reaaliaikaisia tietoja tietoturvahaavoittuvuuksista.

Kyberturvakeskus julkistaa säännöllisiä yhteenvetoja ja raportteja, mm. Kybersää.

Kyberturvakeskus julkistaa ohjeita ja oppaita eri kyberturvan osa-alueisiin ja eri kohderyhmille.

Lisätietoja antaa myös Elmon asiakaspalvelu: 03 455 2000

Elmon tieto-turvapalveluista voit lukea lisää sivulta:
elmo.fi/palvelut/tietoturva

Elmo