MICROSOFT OY
Keilalahdentie 2-4
02150 Espoo
Finland

Tel +358 71800 8000
www.microsoft.fi

26.4.2022

Lausunto eduskunnan hallintovaliokunnalle asiassa VNS 1/2022 vp Ajankohtaisselonteko turvallisuusympäristön muutoksesta

Microsoft Oy kiittää eduskunnan hallintovaliokuntaa mahdollisuudesta lausua VNS 1/2022 vp ajankohtaisselonteon osalta. Ajankohtaisselonteko on ansiokkaasti toteutettu ja tuo esille lukuisia erinomaisia jo tehtyjä toimenpiteitä sekä ehdotuksia jatkon osalta.

Tässä lausunnossa toimitetut tiedot pohjautuvat Microsoftin digitaalisen puolustuksen raporttiin v2021. Kattavampi suomenkielinen raportti on saatavissa Microsoftin sivustolta. Toivomme näiden tietojen auttavan käynnissä olevaa keskustelua.

Microsoft palvelee maailmanlaajuisesti miljardeja asiakkaita ja olemme siten ainutlaatuisessa asemassa, jossa saamme yli 24 biljoonaa päivittäistä tietoturvasignaalia. Niiden ansiosta pystymme muodostamaan erittäin tarkan kuvan kyberturvallisuuden nykytilasta ja ennustamaan hyökkääjien seuraavia liikkeitä. Lausuntomme keskittyy siis pääosin mainitun selonteon kappaleeseen 3.2 - kyperturvallisuus.

Muutos on pysyvä

Kymmenen vuotta sitten maailma oli tietotekniikan näkökulmasta huomattavasti yksinkertaisempi. Organisaation rajat olivat selkeästi määriteltyjä, joten suojaukset oli mielekästä rakentaa näitä rajojen mukaillen. Voidaan ajatella, että organisaatio tuolloin oli kuin keskiaikainen linna, jonka suojaamiseen riitti suojamuuri ja laskusilta. Muurien sisällä ylläpidettiin omaa sisäistä verkkoa, johon muurien ulkopuolella toimivilla oli pääsy VPN ratkaisujen kautta sekä palomuurien säännöstöillä. Linnan laskusillan (palomuuri) perimmäinen tarkoitus oli päästää liikennettä läpi.

Maailma on sittemmin muuttunut, eivätkä perinteiset keinot enää ole yhteensopivia tämän päivän toimintaympäristön kanssa. Myös nyt puheena oleva turvallisuustilanne tuo korostuneesti esille yhteistyön ja teknologian merkityksen.

Informaation tehokas liikkuvuus on globaalin talouden ja rajat ylittävän yhteistyön edellytys, mutta se on myös edellytys kyberturvallisuudelle.

MICROSOFT OY
Keilalahdentie 2-4 Tel +358 71800 8000
02150 Espoo www.microsoft.fi
Finland

Yhteiskunnassa tarvittavat toimenpide-ehdotukset:

Kyberturvallisuusparadigman viisi muutosta

1. **Digitaalisen empatian nousu.** Sosiologiset ja ihmislähtöiset näkökohdat ovat olennaisia teknologian ja kyberturvallisuuden kehitykselle. Kyberturvallisuudessa se tarkoittaa sellaisten työkalujen rakentamista, jotka mukautuvat entistä paremmin ihmisten ja alituisesti muuttuvien olosuhteiden monimuotoisuuteen sekä erilaisiin näkökulmiin ja kykyihin. Tietoturva ja käyttäjäystävällisyys ovat toisiaan tukevia, eivät poissulkevia, tekijöitä.

2. **Zero Trust** -siirtymästä on tulossa yhä tärkeämpi[1]. Organisaatioiden on siis lähtökohtaisesti oletettava, että heidän systeeminsä ovat jo vaarantuneet. ”Assume breach” on tietoturva-ammattilaisten lähtökohta.

3. **Datan monimuotoisuus on tärkeää**. Microsoft onnistui havaitsemaan uusia koronaviruspandemiaan liittyviä uhkia ennen kuin ne ehtivät saavuttaa asiakkaat, joskus jopa sekuntien murto-osissa. Toinen tuoreempi esimerkki on vain tunteja ennen Venäjän Ukrainaan aloittamaa hyökkäystä 24.2, jolloin Microsoft tunnisti uusia Ukrainan digitaaliseen infrastruktuurin kohdistuvia hyökkäyksiä. Tämän perusteella olemme auttaneet Ukrainan hallintoa uhkan torjunnassa mutta myös tuntien sisällä uhkan huomaamisesta tunnistusmekanismit lisättiin Defender virustorjuntaohjelmistoon[2] palvellen siis globaalisti asiakkaitamme. Nämä ovat vain kaksi esimerkkiä siitä, kuinka monimuotoinen data hyödyntäen hyperskaalattua pilvipalvelua tarjoaa selkeitä etuja uhkien torjunnassa.

4. **Organisaation resilienssi on sidoksissa sen kyberresilienssiin**.

5. **Kasvava keskittyminen integroituun tietoturvaan.** Tietoturvaorganisaatioiden tehokkuuden maksimoimiseksi työkalujen tulee olla täysin integroituja, jotta ne tehostavat toimintaa ja antavat täyden päästä päähän -näkyvyyden.

Viimeaikaiset tapahtumat ovat osoittaneet, että ajantasaiset tietoturvapäivitykset kaikissa järjestelmissä on yhä tehokkain tapa suojautua nopeasti kehittyviltä uhkilta.

Säilyttääkseen toimintavalmiutensa edistyneitä hyökkäyksiä vastaan organisaatiolla on oltava ajantasaiset, kattavat inventaariotiedot järjestelmistään ja niiden korjauspäivitystilanteesta sekä perusteelliset varmuuskopio- ja hallintasuunnitelmat.

[1] https://www.microsoft.com/fi-fi/security/business/zero-trust
[2] https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/

MICROSOFT OY
Keilalahdentie 2-4 Tel +358 71800 8000
02150 Espoo www.microsoft.fi
Finland

Sääntelykehikon ja sitä tukevat määräykset sekä ohjeistukset on oltava selkeitä.

Haastavaksi tilanteen tekee jos tietoturvallisuuskriteeristöjen vaatimusten taustalla on ajatus siitä, että tieto sijaitsee jossain eksaktissa paikassa ja että siihen pystytään kohdistamaan hallintatoimia perustuen sen fyysiseen sijaintiin. Vaatimuksia asetettaessa tulisi painopiste siirtää enemmän tiedon elinkaaren ja käyttäjien identiteettien suojaamiseen ja hallintaan, ja luopua ristiriitaisista, omalta osaltaan turhaan rajoittavista vaatimuksista.

Näin ollen lakien, asetusten, ohjeistusten ja määräysten tulisi pyrkiä ohjaamaan eri toimijoita toivottuun lopputulemaan (outcome based regulation). Fyysisestä maakohtaisesta datan lokaatiovaatimuksesta tulisi viimeistään nyt luopua ja sen sijaan huolehtia siitä, että data on siirrettävissä mutta myös sen tarvittava kopio on käytettävissä. Vaatimukset tulisi näin kohdistaa suojattavan tiedon luottamuksellisuuden, eheyden ja saatavuuden varmistamiseen kulkipa tieto missä tahansa. Vaatimustenmukaisuuden arviointiin olisi suositeltavaa käyttää kansainvälisiä standardeja.

Yhteistyön ja normien merkityksestä

Olemme edelleen erityisen huolissamme viimeaikaisista kyberhyökkäyksistä, jotka ovat kohdistuneet Ukrainan digitaalisiin siviilikohteisiin, kuten rahoitusalaan, maatalousalaan, humanitaarisen avun toimiin sekä yrityksiin. Nämä siviilikohteisiin kohdistuvat hyökkäykset herättävät vakavaa huolta Geneven yleissopimuksen nojalla. Ajankohtaisselonteko nostaa hyvin esille sekä kansallisen että kansainvälisen yhteistyön merkityksen niin teknisen yhteistyön, kansainvälisten normien ja standardien kuin poliittisen vuoropuhelun osalta. Yhteistyötä on syytä tiivistää mutta lisäksi on löydettävä keinoja koskien mm. tietoturvapoikkeamien ilmoittamisvelvollisuutta.

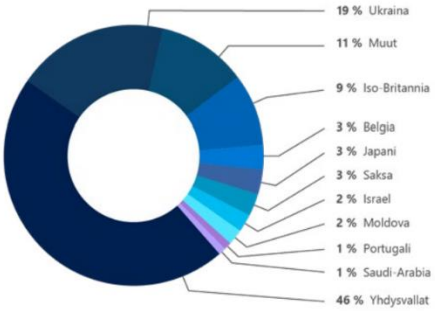
Kansallisvaltioiden haitalliset toimet

Valtioiden haitalliset toimijat (nation states eli NS) ovat suurelta osin jatkaneet toimintaansa tasaiseen tahtiin ja kehittäneet samalla uusia taktiikoita ja tekniikoita, joilla ne pystyvät välttymään havaitsemiselta ja laajentamaan hyökkäyksiään.

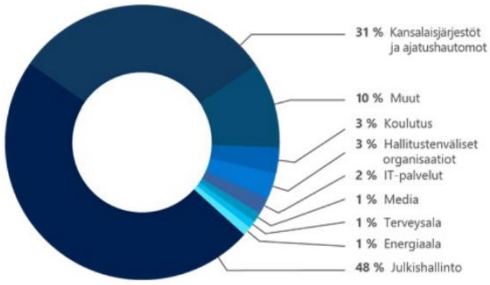
Microsoftin Threat Intelligence Center (MSTIC) ja Digital Security Unit (DSU) ovat havainneet, että useimmat valtiolliset toimijat keskittyvät edelleen viranomaisiin, hallitustenvälisiin järjestöihin (IGO), kansalaisjärjestöihin (NGO) ja ajatushautomoihin perinteisen vakoilun tai tarkkailun merkeissä. Kohteilla on usein hyökkäykseen syyllistyvän valtion kaipaamaa tiedustelutietoa, minkä vuoksi monet iskut ovatkin kohdistuneet julkishallinnon virastoihin ja ajatushautomoihin.

MICROSOFT OY
Keilalahdentie 2-4
02150 Espoo
Finland
Tel +358 71800 8000
www.microsoft.fi

Eniten kohdennetut maat (heinäkuu 2020–kesäkuu 2021)



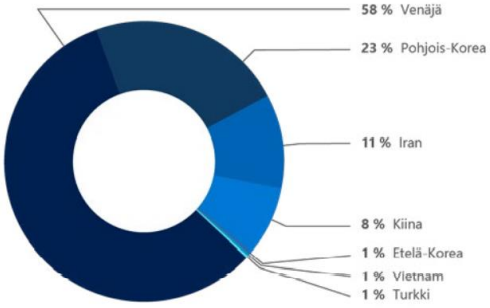
Eniten kohdennetut sektorit (heinäkuu 2020–kesäkuu 2021)



Jokainen seuraamamme haitallinen toimija kohdisti toimintaansa julkishallinnon yksiköihin. NOBELIUM, NICKEL, THALLIUM ja PHOSPHORUS olivat neljän päämaan (Venäjä, Kiina, Pohjois-Korea, Iran) toimijoista aktiivisimpia tällä sektorilla. Julkisen sektorin kohteet olivat lähinnä ulkoasiainministeriöitä ja muita kansainväliseen suhdetoimintaan osallistuvia julkishallinnon yhteisöjä eri maissa. (Kaavio ei sisällä kuluttajatilejä vaan kuvastaa ainoastaan näiden sektoreiden organisaatiokohteita.)

Raportointi ajanjaksolla kriittiset infrastruktuurit eivät NSN (nation states notification)-tietojen mukaan olleet huomion keskipisteenä. Kiinalaiset valtion toimijat osoittivat kaikkein eniten ja venäläiset vähiten kiinnostusta kriittisen infrastruktuurin sektoriin. Venäläisen NOBELUMin kybertoiminta on erinomainen esimerkki Venäjän tavasta keskittyä pääsyreittien löytämiseen ja tiedusteluun sen sijaan, että se iskisi suoraan kriittiseen infrastruktuuriin häirintätarkoituksessa. Selvyyden vuoksi todettakoon, että kriittinen infrastruktuuri, joka ei hyödynnä hyperskaalattua pilviteknologiaa, ei luonnollisesti näy tämän raportin tuloksissa.

Hyökkäysten alkuperämaa (heinäkuu 2020 – kesäkuu 2021)



Laskentatapana on käytetty kunkin toimijan hyökkäyksistä tehtyjen NSN ilmoitusten määrää.

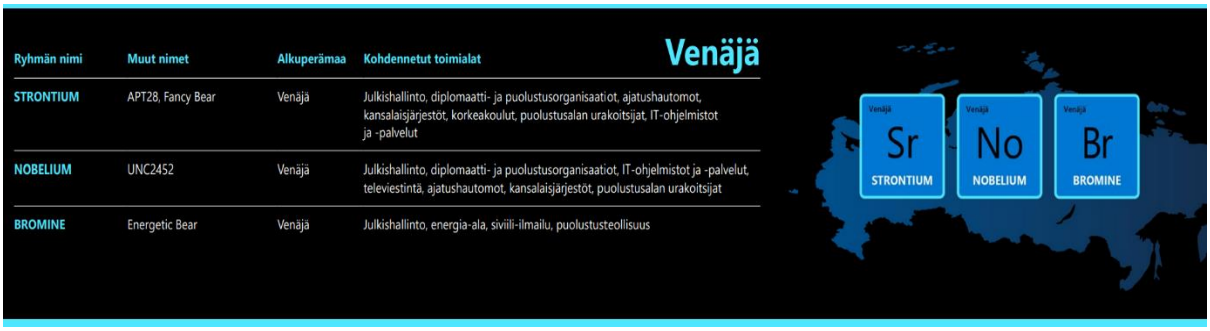
NOBELIUM ja sen aggressiiviset kampanjat IT-palveluntarjoajiin ja länsimaisiin julkishallintoihin nostivat Venäjän raportointijakson ykköseksi hyökkäysten lähtömaiden listalla. Kyseinen ryhmä oli vastuussa 92 prosentista asiakkaille lähetetyistä ilmoituksista, jotka koskivat Venäjän haitallista toimintaa. Pohjois-Korean suhteettoman suuri osuus hyökkäyksistä on seurausta THALLIUM- ja CERIUM-ryhmien strategiavalinnasta. Kumpikin käyttää suurten hyökkäysmäärien taktiikkaa. Vaikka hyökkäysten onnistumisprosentti on alhainen, niiden valtavan määrän takia ryhmät onnistuvat vaarantamaan joitakin kohteita.

MICROSOFT OY
Keilalahdentie 2-4
02150 Espoo
Finland

Tel +358 71800 8000
www.microsoft.fi

Valtioiden haitalliset toimijat käyttävät yleensä samoja työkaluja kuin muutkin haitalliset toimijat tunkeutuakseen kohteidensa verkostoihin. Esimerkiksi GADOLINIUM hyödyntää yhä useammin avoimen lähdekoodin työkaluja tai tavallisia haittaohjelmia, joilla se iskee toimitusketjuun, yrittää väliintulohyökkäystä tai käynnistää palvelunestohyökkäyksen. Haitalliset toimijat pystyvät tällöin toteuttamaan hyökkäyksiään suoraan tarkkailijoiden silmien alla.

Valtioiden jatkuvasti kehittyvä kybertoiminta on tehnyt raportointijaksosta poikkeuksellisen. Uhkat keskittyivät yhä enemmän paikallisiin palvelimiin ja paljastivat toimitusketjujen laaja-alaisia haavoittuvuuksia, erityisesti ohjelmistoissa.



Venäjään liitetyt ryhmät ovat vakiinnuttaneet asemansa akuuttina uhkana maailman digitaaliselle ekosysteemille. Ryhmien sopeutumiskyky, pysyvyys, luotettujen teknisten yhteyksien hyväksikäyttö ja anonymisoinnin ja avoimen lähdekoodin työkalujen osaaminen tekee toiminnan havaitsemisesta ja tekijän tunnistamisesta yhä vaikeampaa. Ne ovat myös vähät välittäneet oheisvahingoista, eli kaikki kiinnostaviin kohteisiin kytkeytyvät tahot voivat tilaisuuden tullen päätyä hyökkäysten kohteiksi.

Toimitusketjut sekä eheys

Sekä fyysiset että digitaaliset toimitusketjut toimivat luottamuksen varassa, ja vastustajat ovat huomanneet tämän. Viimeisimpien kymmenen vuoden aikana menestyksekkäät organisaatiot ovat pystyneet täyttämään mittakaavan, tehokkuuden ja nopeuden vaatimukset rakentamalla laajoja ja usein monimutkaisia ekosysteemejä, jotka tuottavat lisäarvoa sidosryhmille. Nykypäivän kyberrikolliset näkevät nämä järjestelmät hyväksikäytön kohteina.

OT-laitteet, kuten teollisuuden säätöjärjestelmät, sairaaloiden valvontajärjestelmät ja vedenhallintajärjestelmät, edustavat julkista infrastruktuuria, josta monet yhteisöt ovat olleet riippuvaisia jo vuosikymmenien ajan.

MICROSOFT OY
Keilalahdentie 2-4 Tel +358 71800 8000
02150 Espoo www.microsoft.fi
Finland

Kaikki järjestelmät eivät pysty käyttämään Zero Trustin mahdollistamia työkaluja. Esimerkiksi monissa operatiivisen teknologian (OT) järjestelmissä teknologian elinkaari on pitkä, ja niissä voi olla käytössä käyttöjärjestelmiä ja ohjelmistoja, joita ei voida päivittää.

Verkkosegmentointia tulisi soveltaa pääsyn rajoittamiseksi näihin järjestelmiin. Tämä voi auttaa varmistamaan, että operatiivinen teknologia ei ole alttiina hybridityön riskeille ja että IoT-laitteilla ja antureilla on pääsy ja yhteydet vain niiden tukemiin älykkäisiin ekosysteemeihin. Tällä vältetään se, ettei vanha teknologia jarruta nykyaikaisten arkkitehtuurien hyödyntämistä.

Journalismista on huolehdittava

Valtiolliset ja valtioista riippumattomat toimijat voivat käyttää tekoälymenetelmiä muotoillakseen ja edistääkseen tehokkaita psykologisia toimia, joissa hyödynnetään ihmisen kognition analytiikkaa ja tietoja. Koneoppimista ja päättelyä voidaan käyttää yksilöiden ja ryhmien profilointiin, minkä jälkeen heihin voidaan suunnata personoituja disinformaatio-ohjelmia heidän uskomustensa, mielipiteidensä ja toimiensa muokkaamiseksi.

Kyberhyökkäykset käyttävät tietokoneinfrastruktuuria hyväkseen luodakseen häiriöitä, kun taas disinformaatio käyttää hyväkseen ”ihmisen infrastruktuuria”, ja hyökkäys vaarantaa loogisen, analyyttisen ja kriittisen ajattelun.

Eri valtiot ja valtioista riippumattomat toimijat käynnistävät nyt ennennäkemättömiä disinformaatiokampanjoita ja niihin liittyviä kyberoperaatioita. Osa kampanjoista kohdistuu julkiseen mielipiteeseen ja toiset yritysten toimintaan ja luottamukseen. On tärkeää pysyä kehitysten tasalla ja toimia yhdessä haasteiden ratkaisemiseksi tietoisuuden, teknologioiden ja käytäntöjen avulla.

Syvävääreennökset (deep fakes) ovat tekoälyllä manipuloituja valokuvia, videoita ja äänitiedostoja, joihin tehdyt muutokset ovat vaikeasti havaittavissa. Syvävääreennösten aseistamisella voi olla merkittäviä vaikutuksia talouteen ja kansalliseen turvallisuuteen. Syvävääreennökset heikentävät journalismin uskottavuutta heikentämällä kansalaisten luottamusta mediaan.

Meidän on reagoitava disinformaation lisääntyvään hienostuneisuuteen ja laajuuteen – sekä ryhdyttävä toimiin useilla eri osa-alueilla. Suomessa on erinomaisesti panostettu moderniin medianlukutaitoon, ja tätä työtä on jatkettava. Medialukutaitoon liittyvä työ ulottuu myös koulutuksen ulkopuolelle ja siihen sisältyy pyrkimyksiä luoda uudenlaisia työkaluja, joiden avulla ihmiset voivat arvioida uutisten ja tietojen lähdettä ja totuudenmukaisuutta kriittisesti. Meidän on myös tuettava korkealaatuista journalismia ja luotettavia uutisorganisaatioita.

MICROSOFT OY
Keilalahdentie 2-4
02150 Espoo
Finland

Tel +358 71800 8000
www.microsoft.fi

Lopuksi

Yhteistyömallit on rakennettava toimiviksi. Suomessa ansiokkaasti harjoitetaan tietoturvaan pohjautuvaa yhteistyötä ja tätä työtä on jatkettava. Yksikään toimija tai valtio ei näitä valitettavasti kykene yksin ratkaisemaan sillä uhkakuvat ovat kasvussa, ei laskussa. ”Oleta, että sinun järjestelmääsi on jo hyökätty” eli ns Zero Trust tulisi olla vallitseva toimintamalli, yhdistettynä skaalautuvan teknologian hyödyntämiseen, jolloin mahdollistamme Suomen kyvykkyyden varautua, suojautua sekä vastata kasvaviin uhkakuviin. Osaavat tekijät ovat Suomen turvallisuuden mutta myös menestyksen kulmakiviä jatkossakin.

Espoossa 26.4.2022

Susanna Mäkelä

Yhteiskuntasuhdejohtaja

Microsoft Oy