1.4.2022

AVARN Security

Varautuminen yrityksissä

Venäjän hyökkäyssodan vaikutus yritysten varautumiseen ja turvallisuuteen

Petteri Korsow
Avarn Security Oy
Development Manager
petteri.korsow@avarnsecurity.fi

Kyberhyökkäyksiin varautuminen yrityksissä

Mitä vastaan

Ei välttämättä suorana kohteena ➔ välillinen vaikutus, ”sivullinen uhri”
Käytetään hyväksi varsinaista kohdetta kohtaan (toimitusketju)
Valtiollinen toimija, opportunistinen toimija, aktivismi, vandalismi jne.

Kartoita tarpeet, kyvyt ja resurssit

Tarpeet, kyky ja resurssit varautumiseen vaihtelevat paljon
Omat tarpeet ja kyvykkyydet eivät välttämättä ole selvillä
Omien häiriöiden vaikutus asiakkaisiin ja kumppaneihin (liiketoiminta)
Kumppanien ja toimittajien häiriöiden vaikutus omaan toimintaan

Aloita varautuminen nyt

Aloita todennäköisimmistä uhista ja vaikuttavimmista toimenpiteistä
Määritä perustaso joka saavutettava ja jota sitten kehitetään pitkäjännitteisesti
Ennakointi, hallinta, minimointi, toipuminen ja palautuminen

Johtaminen

Uhat ja riskit

- Ei tiedetä kuka vastaa ja mistä
- Tilannejohtaminen puuttuu
- Varautuminen ei ole kenenkään vastuulla
- Ei tiedetä miten viestitään kun normaalit kanavat eivät ole käytössä
- Päätöksentekokyky vaarantunut
- Disinformaatio / misinformaatio vaikeuttaa päätöksentekoa
- Mainehaitta

Toimenpiteet

- Vastuu johdolla. Vaadittava toimenpiteitä ja vastauksia. Annettava resurssit
- Viestintä suunniteltava etukäteen
  - Kenelle
  - Milloin
  - Mistä aiheesta
  - Kenen toimesta
  - Ennalta mietittyä
- Päätöksentekokyvyn säilyttäminen
  - Roolit
  - Tavoitettavuus
  - Prosessit ja ”mitä jos…”
- Harjoittelu
- Tilannekuva

Vastuu vaatia ja antaa resurssit | Viestintä | Päätöksentekokyky | Tilannekuva

Keskeiset järjestelmät

Uhat ja riskit

- Ei tiedetä mitä kaikkea on käytössä ja miten
  - Turhia (”käytöstä poistuneet”)
  - Huonot asetukset (oletussalasanat, liian laajat oikeudet yms.)
- Saatavuus
  - Digi / HW
  - Alentunut
  - Täydellinen katko
- Infrastruktuurihäiriöt
  - Kansalliset / kansainväliset yhteydet
  - Häiriöt sähköverkossa

Toimenpiteet

- Kartoita järjestelmät (mikä, käyttötarkoitus)
  - Missä sijaitsevat (on-prem., pilvi, SaaS, jne.)
  - Toiminnan kannalta keskeisimmät (priorisoi)
  - Turhat pois, asetukset kuntoon
- Kuka vastaa ylläpidosta ja pääkäyttäjät
  - Varahenkilö(t), osaaminen (osaamisen jakaminen/hajauttaminen)
- Miten voidaan korvata / Voidaanko korvata
- Paikalliset järjestelmänvalvojan oikeudet pois työasemilta

Valmius & Kyvykkyys: Tunnista, reagoi, rajoita ja poista

Uhat ja riskit

- Haittaohjelmat
- Luvaton käyttö / tunkeutuminen
- Tietovuodot
- Monivaiheinen tunnistautuminen (MFA) ei käytössä
- Tietojenkalastelu / Social Engineering
- Päivityksiä ei ole asennettu
- Palvelunestohyökkäykset
- Muut tapahtumat jotka uhkaavat toimintaa (tulipalo, vesivahinko, jne.)
- Lokeja ei ole tai niitä ei säilytetä tarpeeksi kauan

Toimenpiteet

- Toimintamallit poikkeamien havainnointiin ja hallintaan
  - Tunnista, luokittele, rajaa ja poista
- Ohjeistus ja kouluttaminen
- Yleiset tietoturvaperiaatteet ja toimintamallit (ml. Social Engineering ja phishing)
- Valvonta (tapahtumat, poikkeamat jne.)
- Tekninen suojaaminen
  - Haittaohjelmilta
  - Verkkoliikenne
  - Tiedot (esim. salaaminen)
  - Lokit
- MFA pakolliseksi
- Päivitykset asennettava ajallaan kaikkiin järjestelmiin ja laitteisiin
- Kovennukset, best practice toteuttaminen

Jatkuvuus: Toipuminen ja palautuminen

Uhat ja riskit

- Puuttuvat tai toimimattomat varmuuskopiot
- Kukaan ei osaa palauttaa järjestelemiä
- Puuttuvat tilapäisjärjestelmät
- Tiedot käyttökelvottomia
  - Palautuspiste liian vanha / hidas
  - Tiedot tuhoutuneet
  - Tiedot muuttuneet/puutteelliset
- Prosessit, ohjeet, toimintamallit puuttuvat, eivät ole ajan tasalla jne.
- Ei ole harjoiteltu

Toimenpiteet

- Prosessit, harjoittelu, dokumentointi ajan tasalle
- Varmuuskopiot
  - Missä säilytetään (3-2-1 malli)
  - Onko palauttamista harjoiteltu ja toimiiko se
  - On-prem to cloud, cloud to on-prem.
- Muut korvaavat järjestelyt ja toiminnan jatkaminen poikkeusoloissa
- Recovery Point Objective (RPO), Recovery Time Objective (RTO), Business Impact Analysis (BIA)

Toimitilat

Uhat ja riskit

- Infrastruktuurihäiriöt
  - Ei sähköä, vettä, lämpöä
  - Ei kulkuyhteyksiä/heikenneet
- Tilat eivät käytettävissä
  - Käyttö estynyt
  - Tuhoutuneet
- Siirrettävyys
  - Laitteet
  - Järjestelmät
  - Varasto, tuotteet jne.

Toimenpiteet

- Väistötila
- Hajautus esim. etätyönä
- Toiminnan keskeyttäminen
- Kartoitus mitä uhkia sähkön, veden, lämmityksen puute aiheuttaa (järjestelmille, tuotteille, varastolle jne.)
- Toiminnan siirtäminen uusiin tiloihin (vaativuus?)

Henkilöstö

Uhat ja riskit

- Saatavuus
  - Alentunut
  - Eivät pääse työpaikalle
- Ei tehty (vanhentuneet) / saatu tarvittavia VAP varauksia
- Disinformaatio / Misinformaatio
- Palkanmaksun keskeytyminen

Toimenpiteet

- Toiminnan kannalta keskeisimmät henkilöt
  - VAP varaukset tarvittaville ja suostuvaisille
- Riittääkö tekijöitä kaikkien keskeisten toimintojen pyörittämiseen
- Mistä toiminnoista karsitaan ensimmäisenä ja mitkä pidetään käynnissä viimeiseen saakka
- Kuinka hyvin etätyöskentelyä voidaan soveltaa
- Tiedottaminen ja oikean tiedon jakaminen

Kumppanit

Uhat ja riskit

- Toimitusketjuhyökkäys
- Ei pysty toimittamaan sovittua palvelua
  - Osittain / kokonaan
  - SLA tasot eivät pidä
- Materiaalien saatavuus heikkenee/estyy
- Maksuliikenne (sisään / ulos)

Toimenpiteet

- Toimittajat
  - Mitä palveluja hankitaan – kriittisyys
  - SLA tasot
  - Sopimusten Force Majeure rajaukset
  - Päivitetyt yhteystiedot
- Verkostot
  - Riippuvuus ekosysteemeistä
- Voidaanko korvata
  - Kokonaan / osittain
- Onko osaamista ydintoiminnoista, vai onko kaikki ulkoistettu

Sopimukset ja sopimusvelvoitteet

Uhat ja riskit

- Sopimusvelvoitteet eivät täyty
  - Omassa toiminnassa
  - Toimittajan toiminnassa
- Ei auditoida kriittisiä toimittajia
- Ei ole vaadittu kyber- ja/tai jatkuvuussuunnitelmia tai
  - niitä ei ole auditoitu
  - niiden toimivuutta ole varmistettu harjoittelemalla
- Vahingonkorvaus ja/ tai sopimussakko eivät varmista jatkuvuutta vaan ovat jälkikäteisiä

Toimenpiteet

- Velvoitteet asiakkaita kohtaan
  - Mitä on sovittu (esim. onko sovittu, että pitää olla VAP varattuja)
  - Ilmoitusvelvollisuus jos palvelutaso heikkenee
  - Force Majeure
- Toimittajien ja kumppanien velvoitteet
  - SLA
  - Ilmoitusvelvollisuus jos palvelutaso heikkenee
  - Force Majeure
  - Auditoinnit (itseauditoinnit)
- Kyber- ja/tai jatkuvuussuunnitelma
- Toimivuuden harjoittelu yhdessä

Yhteenveto

Johtaminen	Vastuut, viestintäsuunnitelma, päätöksentekokyky, harjoittelu
Keskeiset järjestelmät	Kartoitus, prioriteetti, vastuut, korvaavat järjestelmät, ylläpito, pääkäyttäjät
Valmius & Kyvykkyys	Tekninen kyvykkyys, prosessit, ohjeistus ja kouluttaminen, MFA, päivitykset kaikkiin järjestelmiin ja laitteisiin
Jatkuvuus & Palautuminen	Varmuuskopiot, korvaavat järjestelyt, suunnittelu ja harjoittelu
Toimitilat	Väistötilat, toiminnan siirtäminen, etätyön hyödyntäminen
Henkilöstö	Saatavuus, työhön pääsy, VAP varaukset, tiedottaminen
Kumppanit	Kartoitus, priorisointi, SLA:t, verkostot, korvattavuus
Sopimusvelvoitteet	Velvoitteiden kartoitus ja varmistaminen (omat ja muiden), harjoittelu, auditoinnit

AVARN

Security