



Fyysisten tunkeutumisharjoitusten opit osana yritysturvallisuuden kehittämistä

Seclion on yritysten ja organisaatioiden tilaturvallisuuden testaamiseen ja kehittämiseen erikoistunut suunnittelu- ja konsulttiyritys

Toteutamme toimeksiantoja sekä hyökkääjän, että puolustajan näkökulmasta:

- Hyökkääjän roolissa teemme mm. Red Teaming-harjoituksia eli fyysisiä ja hybridihyökkäyksiä
- Puolustajan näkökulmasta kehitämme asiakkaidemme kyvykkyyksiä havaita, hidastaa, reagoida ja todentaa heihin kohdistuvia rikoksia ja muita ei-toivottuja tapahtumia.

Turvallisuuden kehittämisen saralla keskitymme:

- Hallinnollinen näkökulma
 - Hallinnolliset kartoitukset, riskiarviot sekä tavoitetilojen määrittely ja kuvaaminen.
 - Turvallisuuden periaatteet: mitä, miksi, miten
- Fyysinen näkökulma
 - Projektisuunnitelmat ja asiakkaan tilaturvallisuuteen liittyvät fyysiset kartoitukset
 - Tilaturvallisuutta tukeva turvateknisten järjestelmien tavoitetilaa palveleva toiminnallinen ja tekninen turvasuunnittelu, kilpailutusmateriaalit ja hankintaprosessin johtaminen
 - Projektijohto, turvaarakoiden valvonta ja asiakkaan edunvalvonta



Mikä on fyysinen tunkeutumisharjoitus?

- Ennakkoon sovittu fyysinen tunkeutuminen toimeksiannon tilanneeseen organisaatioon, jolla testataan kohteen turvallisuuskulttuuria, turvallisuuteen liittyviä prosesseja ja fyysistä turvallisuutta
- Harjoituksen tarkoituksena on löytää kohteen heikkoudet ja haavoittuvuudet niin ihmisten toimintamallien kun ympäristön osalta ja käyttää niitä hyväksi tavoitteen saavuttamiseksi
- Harjoitus pyritään suorittamaan arjen keskellä, kun toiminta kohteessa on mahdollisimman normaalia
- Samoihin kohteisiin tehdään useampi harjoitus havaintojen ja toimintamallien otannan saamiseksi sekä tuurin osuuden poissulkemiseksi
- Fyysiseen harjoituksen yhtenä osana voi olla myös 4G- tai USB-implantin toimittaminen ja kytkeminen kohteeseen. Kytketyn 4G-implantin avulla voidaan suorittaa kyberhyökkäyssimulaatio tai testata Tilaaajan vastatoimia.





Mitä harjoituksella yleisimmin testataan?

Vierailijakäytäntöjä -> pääseekö vierailija liikkumaan vapaasti, mihin asti vierailija pääsee ja mitä tietoja vierailijasta jää jälkeen

- *"Vierailija" sai kytkettyä yrityksen sisäverkkoon kyberhyökkäykseen soveltuvan 4G-reitittimen jäätyään yksin tiloihin.*
- *"Vierailija" pääsi kulkemaan vartioidusta aulasta vapaasti hissille ja sillä ylös kerrokseen, jossa asiakkaan käyttökeseuksen oli selvitetty olevan. "Vierailija" pääsi ovikelloa soittamalla käyttökeseukseen, josta ohjattiin etänä tuotantolaitoksia.*

Alueelle / tilaan pääseminen -> puhdas tila, tuotantoalue, toimistotilat

- *Ulko-oven jälkeen ensimmäisessä sisäovessa ei ollut lukitusta tai kulunvalvontaa. Tämä johti siihen, että ulko-ovesta sisään päässeellä tunkeutujalla oli vapaa kulku puhtaalle alueelle, jossa valmis myyntiin lähtevä materiaali oli varastoituna.*
- *Tunkeutuja kulki huoltomiehen kanssa kiinteistössä ja sai selvitettyä huoltomiehen kulkuavaimen pin-koodin. Tunkeutujalla oli mahdollisuus saada kyseinen avain haltuunsa kopiointia varten.*

Kriittisiin tietoihin pääsyä -> palvelintila, avoin tietokone, salasana

- *Kohteessa oli ollut ISO 27001-auditointi kuukausi aiemmin. Tuotannonohjausjärjestelmän admin-tunnukset oli nostettu viereiselle hyllylle pois näytön reunasta, jossa oli edelleen teipin paikat osoittamassa miten niitä oli aiemmin säilytetty.*
- *Saattajana toiminut kiinteistöjen huoltomies avusti palvelin- ja tietoliikennelaitekaappien ovien avaamisissa ja kertoi, minkä järjestelmän laitteita missäkin sijaitsee (mm. rikosilmoitin-, kulunvalvonta- ja paloilmoitinjärjestelmien keskuslaitteita teletilassa).*



Havainnot ja opit – Kehäsuojaus ja turvallisuushenkilöstö

Opit

- Alueelle saapuville epäselville vieraille, kuljetuksille jne. on hyvä olla selkeä paikka alueen ulkokehällä, jossa tilanne rauhoitetaan ja selvitetään.
- Kiireisissä paikoissa tai stressaavassa tilanteessa aluetta valvovan henkilön stressinsietokyky ja/tai urautuminen työtehtäväänsä altistaa virheisiin, joka usein johtaa virheelliseen toimintaan.
- Aluetta valvovien henkilöiden ja muun turvallisuushenkilöstön turvallisuuskouluttaminen. Heidän on sisäistettävä turvallisuusprosessi, ettei alueelle päästetä ketään ilman asianmukaisia asiakirjoja, lupia tai saattajaa, joka huolehtii tilanteen valvotusti loppuun saakka.





Havainnot ja opit – Kiinteistö / tehdas

Opit

- Luo kiinteistöön tila, joka toimii ”tuulikaappina” saapuville vieraille. Tämänlainen tila rajoittaa pääsyn eteenpäin muihin yrityksen tiloihin. Tila on valvottu ja siitä eteenpäin pääsee vain saatettuna tai omilla mekaanisilla avaimilla tai kulkuavaimilla. Samanlaiset tilat on oltava jokaisen sisäänkäynnin yhteydessä, jotta tunkeutuja ei pääse enää valvotusta sisäovesta syvemmälle kohteeseen.
- Tämä ratkaisumalli estää tunkeutujan pääsyn yrityksen tärkeisiin tiloihin isolla todennäköisyydellä, etenkin jos henkilökunta ymmärtää yrityksen yhteiset pelisäännöt.
- Iso osa tunkeutumista onnistuu, kun ulkokuoren oven jälkeen ei ole enää valvottuja ovia. Ensimmäisen sisäoven lukossa pitäminen on yhtä tärkeää kuin ulkokuoren oven lukossa pitäminen.
- Kriittisten tilojen suojaaminen kulunvalvonnalla (rajoitettu pääsy) ja muilla turvateknisillä ratkaisuilla sekä henkilökunnan kouluttaminen. Kuinka pystyt varmistamaan, kuka tilassa kävi ja oliko hän yksin?
- Miten saat selvitettyä tunkeutujan liikkeitä tiloissa jos hän kulkee muiden perässä eikä käytä kulkemiseen minkäänlaista elektromekaanista avainta?





Havainnot ja opit – Henkilökunta

Opit

- Mitä suurempi yhtiö, sen helpompi on sen tiloissa liikkua, kun työntekijät eivät tunne toisiaan ja ”ei kuulu minulle”-asenne voi olla vallitseva.
- Mitä pidemmälle tunkeutuja pääsee kohteessa, sen vähemmän hänen toimintaansa kyseenalaistetaan
- Henkilökunnalle tulee kouluttaa, ettei ulkopuolisia päästetä kiinteistöön ilman saattajaa. Ja, että tiloissa pitää olla aina saattaja.
- Toinen koulutettava huomio on se, että yrityksen/kiinteistön kriittisissä tiloissa työskentelevä henkilökunta ymmärtää tilojen tärkeyden eikä päästä tiloihin ulkopuolisia ilman pääsyn oikeellisuuden varmistamista.
- Yrityksen ”hällä väliä”-työntekijät ja sidosryhmien palvelualttiit työntekijät ovat yritykselle vaarallisimmat, koska heidän kauttaan tai avullaan pääsee helposti kulkemaan tilaan/tiloissa.
- Kiinnitä huomiota siihen, miten sinun yrityksesi sidosryhmät toimivat tiloissasi. Miten heille on jalkautettu yrityksesi turvallisuuskoulutus ja -kulttuuri?





Tunkeutumisharjoituksen hyödyt organisaatiolle

Haavoittuvuuksien tunnistaminen: Tunkeutumisharjoitukset ovat keino testata organisaation turvallisuuden nykytilaa ja tunnistaa haavoittuvuuksia.

Testaa reaaliaikaisia puolustusmekanismeja: Mahdollistaa yrityksen prosessien tehokkuuden ja toimivuuden arvioinnin todellisissa skenaarioissa.

Organisatorinen oppiminen: Harjoitukset ovat vaikuttaneet turvallisuuskulttuuriin positiivisesti henkilöstön turvallisuustietoisuuden kasvamisen myötä.

Yhteistyön tehostaminen: IT-tiimien, johdon ja muiden osastojen välinen yhteistyö on parantunut, mikä on tehnyt turvallisuuskulttuurista vahvemman.

Toiminnan kehittäminen: Harjoitusten tulokset ovat antaneet konkreettisia suosituksia yritysturvallisuuden kehittämiseen.

Havaittujen riskien korjaamisen priorisointi: Organisaatio on voinut asettaa resurssit tärkeysjärjestykseen perustuen todellisiin riskeihin, jotka harjoituksissa paljastuivat.

Saa organisaatiosi:

- luottamaan prosesseihin. Oikominen aiheuttaa virheitä!
- antamaan aina vierailijalle saattaja koko vierailun ajaksi!
- kiinnittämään huomiota tiloissa liikkuvan ei-kantahenkilöstön luvituksiin - etenkin äkillisiin pyyntöihin!
- ilmoittamaan epämääräisistä havainnoista matalalla kynnyksellä. HUOM! Suullisesta ilmoituksesta ei jää sähköistä jälkeä -> turvallisuushavaintojen kirjaaminen ja arkistointi. Varmista myös tietääkö organisaatiosi mihin tai kenelle ilmoittaa havainnoista ja painota, ilmoittamisen nopeuden tärkeydestä.
- kyseenalaistamaan tiloissa ilman saattajaa liikkuvan tuntemattoman henkilön liikkumisen tarkoitus.
- ymmärtämään minkälainen vaikutus voi olla jos pahantahtoinen henkilö pääsee henkilökunnan perässä ovesta, portista jne. alueelle, tilaan tai tiedon luokse. Enää ei voida mennä ajatuksella "Eihän meillä ole tapahtunut mitään 10 vuoteen!"



Jari Mattila

Myyntijohtaja & Red Team Lead

jari.mattila(at)section.fi

040 658 9937

section.fi