jamk

Organisaation kyberuhkatiedustelukysymykset

Ryhmä 3

Anthony Bäckström

Sami Koivisto

Eino Puttonen

Jussi-Pekka Rantala

Harjoitustyö
Huhtikuu 2024
Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

1 Johdanto

- Ketä asiakkaat ovat?
- Millä alalla organisaatio toimii?
- Kuka potentiaalinen hyökkääjä voisi olla?
- Mitä suojeltavia asioita organisaatiossa on?
- Mitkä uhat ovat ensisijaisia?
- Miten mahdollinen hyökkäys tehdään?

Powerpointista otetut tiedustelukysymykset

Laadi tiedustelukysymykset seuraaville organisaatioille. Perustele kysymykset: Ota kysymyksissä huomioon, että mitä vastauksia näihin kysymyksiin voisi olla? Perustele.

2 Kysymykset ja vastaukset

2.1 Päivittäistavarakauppa, jolla myymälä kauppakeskuksessa. Kanta-asiakasohjelma ja takuutuoterekisteri.

1. **Miten päivittäistavarakauppa varmistaa kanta-asiakasohjelman tietoturvan ja suojaa asiakkaiden henkilökohtaisia tietoja? Perustelu:** Asiakkaiden henkilökohtaiset tiedot, kuten nimet, osoitteet, puhelinnumerot ja ostoshistoria, ovat arvokkaita kyberrikollisille. Tietojen suojaaminen on olennaista asiakassuhteen luottamuksen säilyttämiseksi ja tietoturvaloukkausten välttämiseksi.
2. **Millaisia toimenpiteitä on toteutettu estämään tietoturvaloukkaukset ja kyberhyökkäykset kauppakeskuksen myymälän IT-infrastruktuurissa? Perustelu:** Myymälän IT-järjestelmien, kuten kassajärjestelmien, varastonhallintajärjestelmien ja Wi-Fi-verkon, turvaaminen on kriittistä. Näiden järjestelmien mahdolliset haavoittuvuudet voivat avata oven kyberhyökkäyksille, jotka voivat aiheuttaa taloudellista vahinkoa ja mainehaittaa.
3. **Kuinka päivittäistavarakauppa valvoo ja hallinnoi kolmansien osapuolien, kuten toimittajien ja alihankkijoiden, kyberturvallisuusriskiä? Perustelu:** Kolmannet osapuolet voivat olla heikko lenkki kaupan kyberturvallisuudessa. Niiden kautta voi muodostua reittejä, joita kautta hyökkääjät voivat päästä käsiksi kaupan järjestelmiin tai tietoihin.
4. **Miten kauppa varmistaa takuutuoterekisterin eheys ja saatavuus kaikissa olosuhteissa? Perustelu:** Takuutuoterekisterin tietojen tulee olla ajan tasalla ja saavutettavissa sekä normaalitilanteessa että mahdollisen kyberhyökkäyksen tai muun poikkeustilanteen aikana. Tietojen menetys tai niiden savuttamattomuus voi aiheuttaa ongelmia sekä kaupalle että asiakkaille.
5. **Millaisia varautumissuunnitelmia ja toipumisprosesseja on olemassa kyberhyökkäysten varalle? Perustelu:** On tärkeää, että kaupalla on selkeät toimintasuunnitelmat kyberhyökkäysten varalle, mukaan lukien miten tietoturvaloukkaukset tunnistetaan, miten niistä ilmoitetaan ja miten kauppa palautetaan normaaliin toimintaan mahdollisimman nopeasti.

Vastauksia:

1. **Kanta-asiakasohjelman tietoturva:** Kauppa käyttää salausta ja tietoturvaloukkauksista ilmoittamisen protokollia suojatakseen asiakkaiden tietoja. Lisäksi se järjestää säännöllistä tietoturvakoulutusta henkilöstölleen ja seuraa jatkuvasti tietoturvatapahtumia.
2. **Toimenpiteet IT-infrastruktuurin suojaamiseksi:** Kauppa käyttää palomuureja, haittaohjelmien torjuntaohjelmistoja ja säännöllisiä haavoittuvuustarkastuksia. Se myös harjoittaa työntekijöitään tunnistamaan ja reagoimaan kyberuhkien merkkeihin.
3. **Kolmansien osapuolten kyberturvallisuusriskien hallinta:** Kauppa tekee säännöllisiä tarkastuksia ja arvioi toimittajiensa ja alihankkijoidensa kyberturvallisuuskäytäntöjä, vaatien niitä noudattamaan tiukkoja kyberturvallisuusstandardeja.
4. **Takuutuoterekisterin eheys:** Kauppa varmistaa tiedon eheyden ja saatavuuden käyttämällä varmuuskopiointi- ja palautusmenetelmiä sekä pilvipohjaisia ratkaisuja, jotka takaavat tietojen saatavuuden poikkeustilanteissa.
5. **Varautumissuunnitelmat ja toipumisprosessit:** Kaupalla on selkeät suunnitelmat kyberhyökkäysten varalle, sisältäen toimintatavat tunnistamiseen, ilmoittamiseen ja toipumiseen. Henkilöstö koulutetaan näiden suunnitelmien mukaisesti, ja suunnitelmia päivitetään säännöllisesti vastaamaan uusia uhkia.

2.2 Vartiointiliike, joka suorittaa piirivartiointia useissa teollisuuskohteissa

1. **Miten varmistatte, että vartiointiliikkeenne viestintäkanavat ovat suojattuja ulkopuolisten pääsyltä, erityisesti kun kyseessä on teollisuuskohteiden piirivartiointi? Perustelu:** Viestintäkanavien turvallisuus on kriittistä, sillä niiden kautta kulkee arkaluonteista tietoa, joka voi paljastaa vartiointiliikkeen toimintatapoja ja asiakkaiden tietoja.
2. **Millaisia kyberturvallisuusprotokollia/toimintatapoja noudatatte asiakastietojen käsittelyssä ja säilyttämisessä? Perustelu:** Asiakastietojen suojaaminen on olennaista luottamuksen ylläpitämiseksi ja tietoturvaloukkausten estämiseksi.
3. **Miten henkilökunta koulutetaan tunnistamaan ja reagoimaan erilaisiin uhkiin (myös kyberuhkiin), jotka voivat vaikuttaa teollisuuskohteiden turvallisuuteen? Perustelu:** Henkilökunnan turvallisuustietoisuus on tärkeää, jotta he voivat tunnistaa ja estää mahdollisia hyökkäyksiä.
4. **Mitä itse pidätte suurimpana uhkananne? Onko se enemmän fyysinen uhka vai mahdollisesti kyberuhka? Perustelut:** Mitä yritys itse pitää suurimpana uhkana omalle toiminnalle on tärkeä tieto, kun lähdetään selvittämään kokonaisuutta.
5. **Käytättekö jotain ohjelmistoja kännykässä suorittaessanne vartiointia? Onko ihmisillä omat puhelimet mukana vai pelkästään yrityksen puhelin? Perustelut:** Erilaiset ohjelmistot ja gps –seuranta voivat näyttää vartijoiden rutiinit kohteissa.
6. **Miten varmistatte, että mahdolliset alihankkijanne ja yhteistyökumppaninne noudattavat samoja kyberturvallisuusstandardeja kuin teidän organisaationne? Perustelu:** Alihankkijoiden ja yhteistyökumppaneiden kyberturvallisuus on yhtä tärkeää kuin oman organisaation, sillä he voivat muodostaa heikon lenkin turvallisuusketjussa.
7. **Onko yrityksellä jo toimintamalleja erilaisten uhkien varalta, niin fyysisten kuin kyberpuolen? Perustelut:** Nähdään miten yritys on valmistautunut jo mahdollisiin uhkiin.
8. **Varmistatteko, että teollisuusalueella mahdollisten turvakameroiden ja muu tekniikka on ajan tasalla? Perustelut:** Nähdään onko heillä mahdollisuutta vaikuttaa muihin turvallisuutta lisääviin komponentteihin ja onko yritys huomioinut näitä omassa toiminnassaan.

Vastauksia:

1-kohtaan: Käyttämissämme viestintäkanavissa on kaksivaiheinen tunnistautuminen. Tällä voidaan varmistaa, että vain luvan saaneet henkilöt voivat käyttää niitä. Vartiointiliikkeen välineistöä ei voi saada käyttöönsä ilman tätä. Piirivartijan viestintälaitteilla on vain välttämättömät tiedot ja sovellukset työn suorittamiseksi. Mitään ylimääräisiä tietoja laitteilla ei saa säilyttää. Asiakkaiden ja yhteistyötahojen puhelinnumerot löytyvät yrityksen sähköisestä puhelinluettelosta, joka vaatii tunnistautumisen. Mukana kannettavilla laitteilla ei asiakkaiden tietoja säilytetä.

2 –kohtaan: Käytämme salattuja tietokantoja asiakastietojen säilyttämiseen ja noudatamme tiukkoja tietosuojakäytäntöjä. Tämän lisäksi mahdolliset paperit ja muut, joita joudumme kantamaan ovat siirtojen aikana lukitussa salkussa ja autossa on erillinen lukollinen kaappi. Perustelut: Vartiointiliikkeellä paljon tietoa kohteista, joita vartio niin nämä tiedot pitää olla hyvässä tallessa, ettei ne vuoda heidän kauttaan mahdolliselle hyökkääjälle.

3 –kohtaan: Koulutamme henkilöstöä jatkuvasti erilaisten uhkien varalta, niin fyysisten kuin kyberuhkien ja pyrimme harjoittelemaan näitä tilanteita mahdollisuuksien mukaan. Perustelut: Jatkuva kouluttaminen on tärkeää missä tahansa organisaatiossa, ja vartiointiliikkeessä varsinkin fyysinen uhka on mahdollinen, joten näihin pitää järjestää esim. voimankäyttökoulutuksia.

4-kohtaan: Tietojen vuotamisen kannalta suurin uhka on sosiaalinen vektori. Yrityksellämme on suuri määrä työntekijöitä ja vaikka järjestelmät ovat mahdollisimman turvallisia ja toimintaohjeet selkeitä. Riski väärinkäytöksille tai huolimattomuudelle on aina olemassa. Kyberuhkan havaitsemisessa käytettävät työkalut hälyttävät nopeasti mahdollisista riskeistä. Sosiaalisia riskejä on vaikeampi havaita ennen kuin joku taho niitä pyrkii hyödyntämään. Sosiaalisen vektorin uhkiin voidaan pyrkiä vaikuttamaan rajaamalla yksittäisen työntekijän oikeudet vain niihin tietoihin, joihin hänen tarvitsee työnsä suorittaakseen päästä.

5-kohtaan: Yrityksessä käytetään sovelluksia vartioinnin ja turvallisuuden hallintaan. Ohjelmistot pidetään päivitettyinä. Jokaisella vartijalla on yrityksen puhelin. Puhelimet ovat tarkoitettu vain työkäyttöön ja ne mahdollistavat salatun ja turvallisen viestinnän muiden vartioiden ja keskuksen kanssa.

6-kohtaan: Alihankinta ja yhteistyösopimuksiin sisällytetään selkeät ja tiukat vaatimukset kyberturvallisuusstandardeista. Alihankkijoiden ja yhteistyökumppaneiden kanssa ylläpidetään jatkuvaa ja avointa kommunikaatiota kyberturvallisuusasioissa.

7 –kohtaan: Meillä on valmiina toimintasuunnitelma niin fyysisten uhkien ja kyberhyökkäyksen varalta, joka sisältää välittömät toimenpiteet uhkan rajoittamiseksi, viestintäsuunnitelman asiakkaille ja viranomaisille sekä palautumissuunnitelman normaaliin toimintaan palaamiseksi. Perustelut: Toimintamalleja, jotka mahdollistavat normaalin toimintaan mahdollisimman nopeasti on tärkeässä roolissa, ja tämä näyttää, että yritys on miettinyt jo valmiiksi mahdollisia toimia tilanteen sattuessa, jotka henkilöstö tietää.

8-kohtaan: Yritys varmistaa, että kaikki turvakamerat toimivat ja ovat teknologia on ajan tasalla. Tämä toteutetaan säännöllisillä tarkistuksilla ja huolloilla.

2.3 Verkkosivustoja valmistava yritys, jolla myös omat palvelinsalit sivustojen ylläpitoon ja tarjoamiseen.

1. **Minkälaisia uhkia voi kohdistua palvelinsaleihin ja verkkosivustoihin? Perustelu:** Palvelinsaleihin ja verkkosivustoihin kohdistuvat hyökkäykset voivat aiheuttaa liiketoiminnan keskeytyksen, maine haittaa, tietojen menetystä ja taloudellista vahinkoa.
2. **Minkä tyyppisiä hyökkäyksiä voisi tapahtua palvelinsaleihin ja verkkosivustoihin? Perustelu:** Hyökkäystyyppien kartoittamisella voidaan varautua ja estää palvelinsaleihin ja verkkosivustoihin kohdistuneita hyökkäyksiä.
3. **Mitä tietoja on saatavilla nykyisistä kyberuhkista ja miten näitä voisi hyödyntää palvelinsalien ja verkkosivustojen suojaamiseen? Perustelu:** Ajan tasalla ja luotettavista lähteistä olevat tiedot auttavat palvelinsalien ja verkkosivustojen suojaamisessa.
4. **Minkälaisia varmuuskopiointi ja palautumisstrategioita on otettu käyttöön yrityksessä mahdollisten hyökkäysten varalta? Perustelu:** Hyökkäyksen sattuessa ja jos tietoja menetetään tai palvelut kaatuvat, on hyvä olla varmuuskopioinnit ja jokin suunnitelma tämmöistä tapahtumaa varten.

Vastauksia:

1 ja 2-kohtaan: Palvelinsalien ja verkkosivustojen uhkiin varaudutaan, toimivalla verkonsuojauksella ja palomuurilla, verkkosivujen liikenne on salattua. Jatkuvalla haavoittuvuuksien hallinnalla ohjelmistoja ja verkkosivuja tarkkailemalla ja päivittämällä. Tietojen säännöllisellä varmuuskopioinnilla ja turvallisessa paikassa säilyttämisellä. Ajantasaisella pääsynhallinnalla, oikeutetuille tahoille. Henkilöstön kouluttamisella ja tietoturvan hallinnalla esim. ISMS mukaisesti.

3- kohtaan: Tietoturvatiimi pitää palomuurin ja virus- sekä uhkatorjuntaohjelmistot ajantasaisina. Lisäksi he suorittavat manuaalista tiedonhakua uusimmista uhista ja heidän vastuullaan on henkilöstön jatkuva kouluttaminen hyvistä tietoturvakäytänteistä, jolla sosiaalisen vektorin uhkaa voidaan vähentää.

4- kohtaan: Kriittisten tietojen ja järjestelmien varmuuskopiointi on automatisoitu ja tapahtuu säännöllisesti. Niistä pidetään sopimuksen mukaan off-site kopiot pilvipalveluissa tai fyysisissä varastoissa. Palautusprosessit on säännöllisesti testattu ja varmistettu, että riittävän moni työntekijä osaa ne toteuttaa. Varmuuskopioiden kanssa hyödynnetään sopimuksen mukaan versionhallinnan eri aikapisteistä, jolloin voidaan varmistua, että tarvittaessa palautuspiste saadaan varmasti ”puhtaaseen” versioon esimerkiksi käyttöjärjestelmästä