jamk

Mobiililaitteiden koventaminen

Ryhmä 13

Leevi Kauranen, AC7750
Samir Benjenna, AD1437
Eelis Suhonen, AA3910
Juho Eräjärvi, AD1276
Mikke Kuula, AC7806

Koventaminen TTC6050-3006
11.12.2024
Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

1 Johdanto

Koventaminen-opintojakson kuudennessa harjoitustyössä tutustutaan mobiililaitteiden koventamiseen. Kovennuksia ei tehdä käytännössä omille laitteille, vaan niihin tutustutaan ja arvioidaan, mitkä ovat järkeviä kovennuksia ja mitä ei ehkä kannata tehdä. Harjoitustyössä mietitään myös millaisia kovennuksia olisi hyvä tehdä organisaation työpuhelimille ja mitkä voisivat mahdollisesti olla ylilyöntejä.

2 Teoria

Tiedon keruu on olennainen, jos ei jopa kriittisin osa kyberhyökkäystä. Tämän avulla hyökkääjä saa suunniteltua, kuinka päästä sisään hyökkäysympäristöön ja saavuttaa tavoitteensa. Sitä mukaa kun digitaalinen ympäristö on kasvanut esimerkiksi IoT (Internet of Things) ja mobiililaitteiden mukana, kasvaa myös tavat, joilla tietoa voi kerätä, tai jopa päästä sisään ympäristöön.

Mobiililaitteet ovat tänä päivänä kriittinen osa sekä yksityishenkilöiden että yritysten toimintaa. Ne mahdollistavat jatkuvan yhteydenpidon, nopean tiedonsiirron ja tehokkuuden, mutta samalla niistä on tullut merkittävä kyberturvallisuusriski. Yritysten kannalta mobiililaitteiden tuomat uhat voivat johtaa vakaviin seurauksiin, kuten tietomurtoihin, maineen menetykseen ja taloudellisiin tappioihin.

3 Henkilökohtaisen puhelimen koventaminen

Henkilökohtaisen mobiililaitteen koventamisessa tulee ottaa huomioon omat käyttötarkoitukset ja niihin liittyen, puhelimen käyttäjäystävällisyys. Oman puhelimen kovennukset tehdään henkilökohtaisella tavalla ja siihen ei suoraviivaista ohjetta välttämättä ole. Minkälaisia asioita mobiililaitteilla tehdään ja mitä kaikkea tietoa niihin tallennetaan, on oma juttunsa kullekin. Älypuhelimissa voi-

daan kuitenkin pitää erittäin tärkeitä tietoja ja niillä tehdään asioita, jotka kiinnostavat kybervarkaita, kuten pankkiasiointia. Tässä muutama asia/haaste, joita voidaan pitää mielessä henkilökohtaisen puhelimen koventamisessa.

1. **Tietosuoja**
    a. Omissa puhelimissa on paljon henkilökohtaisia tietoja, kuten viestejä, kuvia, muistiinpanoja ja tilitietoja, jotka on hyvä suojata luvattomalta käytöltä, varsinkin, esimerkiksi pankkiasioihin liittyvät tiedot. Laitteen suojaaminen auttaa estämään sen, että arkaluontoiset tiedot päätyvät varkaiden käsiin, jos laite katoaa tai varastetaan.
2. **Sovellukset**
    a. Henkilökohtaisiin mobiililaitteisiin asennettavat sovellukset pyytävät erilaisia käyttöoikeuksia laitteeseen. Olisi hyvä olla selvillä siitä, minkälaisia käyttöoikeuksia laitteen sovelluksilla on. Myös haitallisista yleisistä sovelluksista olisi hyvä olla selvillä.
3. **Verkko**
    a. Omilla mobiililaitteilla käytetään usein Wifi verkkoja, jotka saattavat altistaa hyökkäyksille. Verkon käyttöä voi yrittää suojata ja vältellä epäilyttäviä Wifejä. Olisi hyvä käyttää vain varmasti turvallisia verkkoja.
4. **Fyysinen turvallisuus**
    a. Mobiililaitteet ovat mukana useimmilla ihmisillä koko ajan, ja laitteet voidaan kadottaa tai joku voi varastaa sen. Vaikka mobiililaite on tärkeä omaisuus, voi sekin unohtua johonkin. Puhelimen fyysisen turvallisuuden varmistaminen on tärkeää digitaalisen suojauksen lisäksi.
5. **Päivitykset**
    a. Laitteiden ohjelmistot ja sovellukset tarvitsevat päivityksiä säännöllisesti, jotta haavoittuvuudet saadaan pois laitteesta. Mobiililaitteiden päivitykset saadaan usein automaattisesti verkosta. Voi olla hyvä ottaa huomioon, että vanhempiin mobiililaitteisiin ei välttämättä enää tule päivityksiä, ja ne voivat olla jääneet käyttöjärjestelmään, joka sisältää haavoittuvuuksia.

3.1 Kovennukset, jotka suorittaisimme:

- **Android laitteiden hallinnointi työkalu:** Google tarjoaa ilmaista palvelua Android laitteiden hallinnointiin, joka vaatii vain google tilin. Tämän avulla kadonneen tai varastetun laitteen saa mahdollisesti paikannettua. Tämän avulla laitteen tiedot saa myös pyyhittyä, mikäli se katoaa.
- **Laitteen salaus:** Laitteen encryption asetuksen saa kytkettyä turvallisuusasetusten kautta. Laite pyytää käynnistyksen yhteydessä salaus avainta, jolla salaukset puretaan.
- **Automaattinen lukitus:** Asetetaan puhelin lukkiutumaan automaattisesti, kun sitä ei käytetä tiettyyn aikaan.
- **Etälukitus ja –seuranta:** Nämä ottamalla käyttöön voidaan lukita laite etänä ja paikantaa laitetta, jos se katoaa tai varastetaan.
- **Tietoturvasovellus:** Yleensä tietoturvaohjelmistoihin sisältyy tietoturva myös puhelimeen, esimerkiksi F-Securen pakettiin sisältyy usein sovellus 3 laitteelle.

3.2 Kovennukset, joita emme suoritettaisi

- **Roottaus (Android) tai Jailbreak (IOS):** Antaa käyttäjälle täyden hallinnan laitteeseen, jolloin käyttöjärjestelmän suojausominaisuudet voivat kärsiä. Altistaa laitteen haittaohjelmille ja tunkeutumiselle. Voi estää myös viralliset ohjelmistopäivitykset.
- **Kasvojentunnistuksen käyttö vanhemmissa laitteissa:** Voi olla turvallisuusriski, jos se perustuu vain valokuvan tunnistamiseen. Tätä ominaisuutta voi olla helppo huijata esimerkiksi valokuvalla. Tämä pätee tosin yleensä vain vanhempiin laitteisiin.
- **Liialliset käyttöoikeudet sovelluksille:** Sovelluksille ei tarvitse antaa enempää käyttöoikeuksia, mitä ne tarvitsevat. Liialliset käyttöoikeudet voivat johtaa ongelmatilanteisiin.
- **Sovellusten asentamisen totaalinen estäminen:** Sovellusten hallinta on tärkeää, mutta työtehtävistä riippuen käyttäjällä saattaa olla tarvetta tietyille sovelluksille, jotka saattavat tehostaa työntekoa.
- **Verkko-ominaisuuksien täydellinen rajoittaminen (esim. Bluetooth, WI-FI):** Monissa työtehtävissä tarvitaan esimerkiksi Bluetooth-kuulokkeita tai turvallista WI-FI-yhteyttä. Täysi kielto voisi johtaa tarpeettomiin hankaluuksiin ilman merkittävää lisäturvaa, jos muita suojausmekanismeja on jo käytössä.

4 Organisaation mobiililaitteiden koventaminen

Organisaation mobiililaitteiden koventamisessa on tärkeää löytää tasapaino käytettävyyden, työntekijöiden tehokkuuden ja tietoturvan välillä. Tietoturvassa, organisaation tiedot ovat ensisijaisia suojattavia, joten kovennustoimet tulee tehdä pitäen niitä silmällä. Työpuhelimissa tulisi olla työhön tarpeelliset asiat, kuten sovellukset ja palvelut saatavilla, muut asiat ovat toissijaisia ja niitä voidaan rajoittaa sitä mukaan, mitä uhkia ajatellaan organisaation mobiililaitteita kohtaan olevan. Rajoitukset tulee kuitenkin tehdä käyttäjäystävällisyys huomioon ottaen, jotta laitteen käytöstä ei tule liian monimutkaista työntekijöille.

4.1 Organisaation mobiililaitteiden haasteet kyberturvallisuudessa

Mobiililaitteiden käyttö tuo lukuisia haasteita organisaation tietoturvaan. Älypuhelimet kulkevat työntekijöiden mukana organisaation ulkopuolella, mikä mahdollistaa nopean yhteydenoton, mutta altistaa myös erilaisille kyberuhille. Tässä muutama kohta, joissa käydään läpi haasteita, joita mobiililaitteen ominaisuuksista ja sen käytöstä organisaatiolle syntyy. Näiden pohjalta voidaan miettiä, mitä kovennuksia mobiililaitteisiin tulisi ainakin tehdä, ja myös, mitä laitteen käyttäjän tulee pitää mielessä, kun tekee asioita organisaation laitteella.

1. **Fyysinen turvallisuus:**

- Mobiililaitteita käytetään organisaation ulkopuolella kahviloissa, hotelleissa ja julkisessa liikenteessä.
- Tämä voi tehdä laitteista alttiita katoamiselle, varastamiselle tai luvattomalle käytölle.
- Myös organisaation sisällä ne voivat joutua väärien ihmisten käsiin, mikä lisää riskiä tietovuodoille.

2. Epäluotettavat laitteet:

- Työntekijät käyttävät omia laitteitaan (BYOD, Bring Your Own Device) työtehtäviin, jotka voivat olla suojaamatta.
- Laitteista voi puuttua sisäänrakennetut tietoturvakontrollit.
- Suojaamattomat BYOD-laitteet ovat epäluotettavia, eikä niitä tulisi käyttää organisaation tietojen käsittelyyn.

3. Epäluotettavat verkot:

- Mobiililaitteilla käytetään usein julkisia Wi-Fi-verkkoja tai muita verkkoja organisaation ulkopuolella.
- Julkiset Wi-Fi-verkot voivat olla hyökkääjän omia verkkoja, jotka tekeytyvät esimerkiksi ravintolan verkoksi.
- Tämä altistaa puhelimen man-in-the-middle-hyökkäyksille ja tietovuodoille.
- Julkiset Wi-Fi-verkot voivat vaarantaa sekä laitteet että niillä siirrettävän tiedon.

4. Epäluotettavat sovellukset:

- Kolmannen osapuolen sovellukset, joita työntekijät lataavat mobiililaitteille, voivat sisältää haittaohjelmia.
- Sovellukset voivat pyytää tarpeettoman paljon puhelimen käyttöoikeuksia ja päästä organisaation tietoihin.
- Sovelluskauppojen ulkopuolelta saadut sovellukset ovat erityisen riskialttiita kyberuhille.

5. Epäluotettava sisältö:

- Mobiililaitteet altistuvat haitalliselle sisällölle, esimerkiksi QR-koodien tai linkkien avulla.
- Ne saattavat ohjata käyttäjän vaarallisille sivustoille, mikä johtaa tietojen kalasteluun tai haittaohjelman asennukseen.

6. Sijaintipalveluiden käyttö:

- Sijaintipalvelut voivat näyttää laitteen sijainnin, mikä voi johtaa kohdennettuun hyökkäykseen.
- Sijaintitietojen perusteella hyökkääjä saa lisätietoa organisaation ja työntekijöiden toiminnasta.

7. Vuorovaikutus muiden järjestelmien kanssa:

- Mobiililaitteilla voidaan synkronoida tietoja muihin laitteisiin ja pilvipalveluihin.
- Tämä voi johtaa arkaluontoisen tiedon vuotamiseen luottamattomiin ympäristöihin, kuten omiin tietokoneisiin.
- Haittaohjelmat voivat levitä, kun laitteiden välillä siirretään tietoa.

(Guidelines for Managing the Security of Mobile Devices in the Enterprise. Sivut 3–6. 2013.)

4.2 Organisaation mobiililaitteisiin tehtävät kovennukset

Alla esitetään toimenpiteitä, jotka kannattaa toteuttaa, sekä viisi toimenpidettä, jotka voivat olla ylilyöntejä ja heikentää käytettävyyttä.

1. **Laitteiden salaus:** Kaikkien mobiililaitteiden tulee olla salattuja, jotta tiedot ovat suojattuja, vaikka laite katoaisi tai varastettaisiin. Tämä estää luvattoman pääsyn tietoihin ilman salasanan tai avaimen tietämistä.
2. **Sovellusten hallinta:** Rajoitetaan sovelluksia, joita voi asentaa.

3. **Monivaiheinen tunnistautuminen (MFA):** Laitteissa ja käytettävissä järjestelmissä tulisi ottaa käyttöön monivaiheinen tunnistautuminen

4. **Säännölliset tietoturvapäivitykset:** Laitteiden käyttöjärjestelmät ja sovellukset on pidettävä ajan tasalla, jotta tunnetut haavoittuvuudet korjataan nopeasti. Tämä voidaan automatisoida MDM-ratkaisujen avulla.

5. **Mobiililaitehallinta (MDM):** MDM-järjestelmien avulla voidaan hallita mobiililaitteiden turvallisuusasetuksia keskitetysti. Tällaisia toimintoja ovat esimerkiksi etälukitus, tietojen tyhjennys kadonneesta laitteesta ja sovellusten hallinta. - Use an application/service to provide remote wipe functionality (Google Android Hardening Checklist)

6. **Suojaus:** MTD (Mobile threat defence) ohjelmiston käyttö laitteissa.

7. **Havaintojen välitys:** Haittaohjelma havaintojen hälytyksen on mahdollista saada SIEM järjestelmään MTD järjestelmän avulla.

8. **Minimi salasanan pituudet:** Laitteen salasanalukitukselle täytyy asettaa minimi vaatimukset.

9. **Datan pyyhkiminen:** Puhelimen sisältö voidaan pyyhkiä liiallisten virheellisten kirjautumisyritysten jälkeen, jolla voidaan estää tiedon joutumista vääriin käsiin.

10. **Turvallisuus varoitukset:** Otetaan käyttöön varoitukset epäilyttävien sivujen osalta.

Mahdollisia ylilyöntejä:

1. **Liiallinen salaus:** Esimerkiksi liian monimutkaisten salasana- ja MFA-vaatimusten asettaminen voi johtaa siihen, että työntekijät kiertävät sääntöjä, kuten kirjoittavat salasanat ylös suojaamattomasti.
2. **Käytön rajoitus tietyille ajoille:** Työpuhelimen käytön rajaaminen tietyille ajoille voi haitata merkittävästi esimerkiksi liikkuvassa työssä toimivien työntekijöiden mahdollisuuksia suorittaa tehtäviä.
3. **Liiallinen rajaus:** Liiallinen rajaus sovellusten suhteen saattaa vaikeutta jotain työtehtäviä. Tätä pitäisi soveltaa työtehtävän mukaan, esimerkiksi viestinnän asiantuntijalla saattaa olla tarve erilaisiin sosiaalisen median sovelluksiin.
4. **Paikannuspalveluiden poiskytkeminen:** Monet sovellukset tarvitsevat paikannuspalveluita toimiakseen. Niiden pois kytkeminen saattaa vaikuttaa sovellusten toimintaan ja käytettävyyteen.
5. **Jatkuvat salasanan vaihdon pakotukset:** Jatkuvat salasanan vaihdon pakotukset mobiililaitteille voivat vaikeuttaa työn suorittamista ja aiheuttaa käyttäjiä käyttämään helposti muistettavia tai toistuvia salasanoja.

5 Pohdinta

Harjoitustyössä pääsimme pohtimaan mobiililaitteiden koventamisen monia puolia. Yksityishenkilöiden sekä organisaatioiden laitteet ja niille käsiteltävä data on tärkeä turvata, mutta samalla on tärkeätä ottaa huomioon laitteen käytön sujuvuus. Harjoitustyössä pääsi käyttämään kriittistä ajattelua ja miettimään mitkä kovennukset ovat aidosti tarpeellisia ja perusteltuja, ja mitkä taas tuovat esteitä käytettävyydelle ilman merkittävää lisäarvoa.

Mobiililaitteita käytetään jatkuvasti enemmän myös työvälineinä, joten niiden tietoturvallisuus on hyvä ottaa huomioon. Mobiililaitteille on helppo ladata arkaluontoisia henkilökohtaisia tai työhön liittyviä tiedostoja, joten on tärkeää pitää huoli, että tiedot eivät vuoda vääriin käsiin.

Lähteet

Guidelines for Managing the Security of Mobile Devices in the Enterprise. NIST julkaisu. 2013. Viitattu 5.12.2024. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf.