Kyberhyökkäys Eseduun

Loppuraportti

ESEDU
Etelä-Savon ammattiopisto

SISÄLLYSLUETTELO

1 LYHYT YHTEENVETO

Etelä-Savon Koulutus Oy:n IT-ympäristöön kohdistui kyberhyökkäys 16.11.2023. Hyökkäys esti IT:hen pohjautuvan opetustoiminnan yhdeksi arkipäiväksi. Henkilöstöverkon palvelut olivat tavoittamattomissa tai kärsivät häiriöistä vajaan kahden viikon ajan.

Heti hyökkäyksen jälkeen katkaistiin IT-ympäristön tietoliikenneyhteydet ja ajettiin kaikki palvelimet alas. Tietohallintopäällikkö informoi heti tapahtuman jälkeen Esedun turvallisuusnyrkin jäseniä. Nyrkki kokoontui ensimmäisen kerran varhain seuraavana aamuna. Kyberhyökkäyksestä tehtiin ilmoitukset Tietosuojavaltuutetun toimistolle ja Kyberturvallisuuskeskukselle sekä rikosilmoitus Poliisille.

Opetus jouduttiin toteuttamaan poikkeusjärjestelyin vain yhden arkipäivän ajan. Hallinnon järjestelmät ja palvelut olivat osin tai kokonaan tavoittamattomissa alle kaksi viikkoa.

Tehtyjen tutkimusten perusteella vaikuttaa siltä, että hyökkääjä on päässyt Internetistä käsin Esedun yhdelle palvelimella, jolta kautta hyökkääjä on levittänyt haittaohjelmaa ohjelmallisesti kyseisen verkon sillä hetkellä käynnissä oleville palvelimille ja työasemille. Haittaohjelma kryptasi kymmenien laitteiden sisältämät tiedostot.

Tämän hetken tiedon mukaan tietosuojan piirissä olevaa tietoa ei ole joutunut hyökkääjälle. Tätä ei ole kuitenkaan pystytty sataprosenttisesti poissulkemaan.

1.1 Tilanne ennen hyökkäystä

Etelä-Savon Koulutus Oy:n IT-ympäristö oli hybrid-ratkaisu (OnPremise ja Microsoft Azure). Henkilöstöverkon ja opiskelijaverkon AD:t oli toteutettu ominaan. Monet opiskelua ja oppimista tukevista tietojärjestelmistä, kuten myös monista hallinnollista tietojärjestelmistä, olivat ulkoistettuina palveluina, toimittajien konesaleissa. Aiempien vuosien aikana oli toteutettu useita IT-infran tietoturvallisuutta parantavia kehittämistoimenpiteitä ja oli otettu käyttöön useita eri tietoturvallisuutta parantavia teknisiä ratkaisuja. Osa näistä on toteutettu alan eri asiantuntijayritysten kanssa

yhteistyössä. Tietoturvan valvonta- ja hälytysratkaisuja uusittiin vuoden 2023 kesällä, mm. käyttöönottamalla Microsoft Sentinel SIEM-ratkaisu.

1.2 Hyökkäys

Esedun tietohallintopäällikkö havaitsi hälytyksen tietoturvapoikkeamasta 16.11.2023 klo 21.13. Seuraavien minuuttien aikana hän sai avukseen asian selvittämiseen IT-asiantuntijan ja IT-suunnittelijan. Hyvin pian tehtiin tulkinta, että kyseessä on vakava tositilanne.

Tietohallintopäällikkö otti välittömästi yhteyttä toimitusjohtajaan ja muihin Esedun turvallisuusnyrkin henkilöihin; turvallisuus- ja tilapäällikköön ja viestintä- ja markkinointipäällikköön. Varotoimenpiteenä Esedun tietoliikenneyhteydet ja kaikki palvelimet ajettiin alas. Yön ja seuraavan aamun tutkinnan kautta varmistui, että IT-ympäristössä oli levinnyt kiristyshaittaohjelma.

1.3 Vahingot ja vahinkojen laajuus

Kiristyshaittaohjelman suorittama tiedostojen kryptaus kohdistui kymmeniin laitteisiin; useimpiin henkilöstöverkon palvelimista ja useaan tapaushetkellä käynnissä olleeseen työasemaan. Tutkinnassa syntyi ymmärrys, että haittaohjelmaa oli levitetty henkilöstö-AD-ympäristössämme ohjelmallisesti. Henkilötietojen joutumisesta vääriin käsiin ei saatu näyttöä. Opetuksen AD ja pilvipalvelut olivat hyökkääjän ulottumattomissa.

1.4 Tilanne hyökkäyksen jälkeen

Hyökkäyksen jälkeen Esedun turvallisuusnyrkki kokoontui välittömästi seuraavana aamuna. Nyrkki päivysti ensimmäiset tilannepäivät. Nyrkkiin kuuluvat:

- Esedun toimitusjohtaja Arja Flinkman
- Esedun tietohallintopäällikkö Mika Pynnönen
- Esedun turvallisuus- ja tilapäällikkö Petteri Häkkinen
- Esedun viestintä- ja markkinointipäällikkö Marika Auvinen

Esedun tietosuojavastaava, opettaja Johanna Taavitsainen oli keskeisessä roolissa tietosuojan näkökulmasta.

Esedun tietohallinnon apuna oli alan asiantuntijayritys selvittämässä tapahtunutta ja sen seurauksia heti iskun jälkeisenä aamuna, 17.11. klo 8.20 alkaen. Samainen yritys oli myös tietohallintomme apuna päivystämässä ja suorittamassa teknistä tutkintaa osittain hyökkäyksen jälkeisen viikonlopun ajan. Päivystysvalvonta ja havainnointi suoritettiin yhteistyössä viikonlopun ajan kellonympäri, jokaisena päivänä.

Opetus ja muu oppilaitoksen toiminta toteutettiin poikkeustilaratkaisuin pe 17.11. hyökkäyksen jälkeisen päivän ajan. Viikonloppuna la-su 18.-19.11. pystyttiin varmistamaan, että hyökkäyksen ulkopuolelle olivat jääneet opetuksen AD ja käyttämämme pilvipalvelut. Nämä otettiin jälleen käyttöön sunnuntain 19.11. aikana. Opetus, ml. verkko-opetus, käynnistyi normaalisti maanantaina 20.11. Opetus häiriintyi tästä hyökkäyksestä vain yhden arkipäivän ajan. Henkilöstöverkko palautettiin pääosin iskun jälkeisen viikon aikana vaiheittain normaalikäyttöön niin, että viimeinenkin On-Premise-tietojärjestelmäpalvelu oli henkilöstömme käytössä ti 28.11. Henkilöstöverkko palveluineen oli toimimaton tai kärsi häiriöistä noin kahdeksan arkipäivän ajan.

Viranomaisilmoitukset

Hyökkäyksen jälkeisenä päivänä pe 17.11. tehtiin ilmoitus tietoturvaloukkauksesta Tietosuojavaltuutetun toimistolle, rikosilmoitus Poliisille ja tapahtuneesta tehtiin ilmoitus myös Kyberturvallisuuskeskukselle. Seuraavien päivien ja viikkojen aikana Etelä-Savon Koulutus Oy:n vastuuhenkilöt ja asiantuntijat olivat useita kertoja yhteydessä em. viranomaisiin, mm. teknisen aineiston, lisähavaintojen sekä pyydettyjen lisäselvitysten toimittamisen näkökulmista.

Viestintä kyberhyökkäyksessä

Esedun turvallisuusnyrkki vastasi toiminnan johtamisesta ja tiedottamisesta sisäisesti henkilöstölle, opiskelijoille sekä ulkoisesti ulkopuolisille tahoille (ml. media).

Viestintä aloitettiin Esedun kriisiviestinnän toimintaperiaatteiden mukaisesti sisäisin toimenpitein. Ensimmäinen hälytys asiasta annettiin henkilöstölle torstaina 16.11. Turvallisuusnyrkki kokoontui pe 17.11. aamusta koolle, jonka jälkeen julkaistiin en-

simmäinen tiedote opiskelijoille sekä ulkoisille sidosryhmille. Turvallisuusnyrkki kokoontui ensimmäisinä tapahtumapäivinä fyysisesti samaan tilaan, toimintakeskukseen.

Ulkoinen viestintä keskitettiin aluksi ensimmäisinä päivinä Esedun verkkosivuille (esedu.fi). Median osalta yhteydenotot keskitettiin viestintä- ja markkinointipäällikölle. Viestintä- ja markkinointipäällikkö kontaktoi ensimmäisen tapahtumapäivän aikana myös Mikkelin sekä Pieksämäen kaupunkien viestintähenkilöt, jotka kertoivat tilanteesta omissa kanavissaan, ja pyysivät seuraamaan tilanneseurantaa Esedun verkkosivuilta.

Lisäksi tilanteesta tehtiin julkaisut Esedun virallisiin sosiaalisen median kanaviin, joista pyydettiin seuraamaan tilanneseurantaa Esedun verkkosivuilta päivittyvästä uutisseurannasta: Eseduun kohdistunut kyberhyökkäys - Etelä-Savon ammattiopisto. Verkkosivujen tilannetiedotus toteutettiin sekä suomen että englannin kielellä. Jokaisessa tilannetiedotteessa kerrottiin aina seuraava ajankohta, jolloin on seuraavan kerran luvassa tietoa tilanteeseen liittyen.

Tilannetiedotteiden lisäksi toteutettiin myös tiedotustilaisuuksia sisäisesti. Ensimmäisinä tapahtumapäivinä henkilöstölle pidettiin tiedotustilaisuuksia 2 kpl ja opiskelijoille 1 kpl turvallisuusnyrkin toimesta. Henkilöstölle ja opiskelijoille tarjottiin myös ensimmäisen viikon aikana mahdollisuus kysyä asiasta tekstiviestitse. Tekstiviestipäivystys palveli jokaisena viikon päivänä. Myöhemmin henkilöstön intraan sekä Esedun verkkosivuille rakennettiin Usein kysytyt kysymykset -palstat: Kyberhyökkäys: Usein kysytyt kysymykset - Etelä-Savon ammattiopisto (esedu.fi)

Viestintätoimenpiteet

	Henkilöstö	**Opiskelijat**	**Ulkoiset sidosryhmät**
to 16.11.	1 Tilannehälytys		
pe 17.11.	Tilannetiedote 5 kpl *Tekstiviestipäivystys klo 7-20*	Tilannetiedote 4 kpl Sosiaalisen median julkaisut 6 kpl UKK-palsta luotu verkkosivuille *Tekstiviestipäivystys klo 7-20*	Tilannetiedote 4 kpl Sosiaalisen median julkaisut 6 kpl UKK-palsta luotu verkkosivuille *Tekstiviestipäivystys klo 7-20*
la 18.11.	Tilannetiedote 1 kpl *Tekstiviestipäivystys klo 6-20*	Tilannetiedote 1 kpl Sosiaalisen median julkaisut 2 kpl *Tekstiviestipäivystys klo 6-20*	Tilannetiedote 1 kpl Sosiaalisen median julkaisut 2 kpl *Tekstiviestipäivystys klo 6-20*
su 19.11.	Tilannetiedote 1 kpl *Tekstiviestipäivystys klo 6-20*	Tilannetiedote 1 kpl Sosiaalisen median julkaisut 2 kpl *Tekstiviestipäivystys klo 6-20*	Tilannetiedote 1 kpl Sosiaalisen median julkaisut 2 kpl *Tekstiviestipäivystys klo 6-20*
ma 20.11.	Tilannetiedote 1 kpl Tiedotustilaisuus 1 kpl + koontitiedote tilaisuudesta 1 kpl *Tekstiviestipäivystys klo 6-18*	Tilannetiedote 1 kpl Sosiaalisen median julkaisut 2 kpl *Tekstiviestipäivystys klo 6-18*	Tilannetiedote 1 kpl Sosiaalisen median julkaisut 2 kpl *Tekstiviestipäivystys klo 6-18*
ti 21.11.	Tilannetiedote 1 kpl *Tekstiviestipäivystys klo 6-18*	Tilannetiedote 1 kpl Tiedotustilaisuus 1 kpl Sosiaalisen median julkaisut 2 kpl *Tekstiviestipäivystys klo 6-18*	Tilannetiedote 1 kpl Sosiaalisen median julkaisut 2 kpl *Tekstiviestipäivystys klo 6-18*
ke 22.11.	Tilannetiedote 1 kpl	Tilannetiedote 1 kpl	Tilannetiedote 1 kpl
to 23.11.	Tilannetiedote 1 kpl		
pe 24.11.	Tilannetiedote 1 kpl Tiedotustilaisuus 1 kpl		
su 26.11.	Tilannetiedote 1 kpl		
ma 27.11.	Tilannetiedote 1 kpl		
ti 28.11.	Tilannetiedote 1 kpl	Tilannetiedote 1 kpl	Tilannetiedote 1 kpl

2 TOIMENPITEET HYÖKKÄYKSEN JÄLKEEN

2.1 Välittömät toimenpiteet

Palvelimelle jätettyyn kiristysviestiin ja lunnasvaatimukseen ei Esedu reagoinut millään tavalla. Palvelimelta löytyi viitteitä paikkaamattomasta ohjelmistohaavoittuvuudesta, mutta lopullista varmuutta hyökkäyksen syylle/mahdollistumiselle ei pystytty aukottomasti muodostamaan.

Etelä-Savon Koulutus Oy:n apuna toimineen asiantuntijayrityksen kanssa yhteistyössä suoritettiin useita pienempiä tietoturvaa parantavia toimenpiteitä OnPremise-ympäristöömme. Samalla tehtiin suunnitelma lähitulevaisuuden kehittämistoimenpiteille. Aiemmin käytetty virustorjuntaratkaisu korvattiin uudella, nykyaikaisemmalla ja kyvykkäämmällä ratkaisulla. Jo hyvässä vauhdissa ollut siirtymä Windows 10-työasemista Windows 11-työasemiin saatettiin loppuun. Joulukuun alussa 2023 otettiin käyttöön Azure Arc, jotta saataisiin entistä parempi näkyvyys ja hallintamahdollisuudet pilvestä oman konesalin ratkaisujen suuntaan. Tammikuussa 2024 otettiin käyttöön myös opiskelijoille monivaiheinen tunnistautuminen.

2.2 Pitkän aikavälin toimenpiteet

Tietoturvallisuuteen liittyvää toimintaa ja tietoisuutta tullaan entisestään kirkastamaan, mm. tietoturvan vuosikellon, tiedottamisen ja kouluttamisen avulla. Painopisteet OnPremise-, pilvi- ja toimittajien konesalien ratkaisujen välillä tullaan arvioimaan uudelleen ja tarvittaessa muuttamaan suunnitelmien mukaisesti. SOC-toiminnan suunnittelu pitkän aikavälin näkökulmasta on myös ajankohtaista.

3 KUSTANNUKSET JA MUUT VAIKUTUKSET

Hyökkäyksestä aiheutui suoria kustannuksia noin 35.000 euroa, joka sisältää asiantuntijapalvelut ja ylityöt.

4 LISÄTIETOJA

Arja Flinkman, toimitusjohtaja puh. 044 711 5691

Mika Pynnönen, tietohallintopäällikkö puh. 044 711 5487

Sähköpostit muotoa etunimi.sukunimi@esedu.fi