Kyberhyökkäys Keudassa

Hyökkäys, toipuminen ja opit

10.3.2023 Kuntaliitto

Keuda

>> keuda.fi
#kestävä #saavutettava #uniikki
#omapolku #työelämäävarten

”

28.11.2023

Cyber-Monday

MARRASKUU 2022: MUSTA CYBER-MAANANTAI KEUDASSA

Keuda lukuina

Opetushenkilöstöä
80 %
koko henkilöstöstä

Noin **850** innostunutta keudalaista työskentelee toimipisteissämme.

21 strategista kumppania

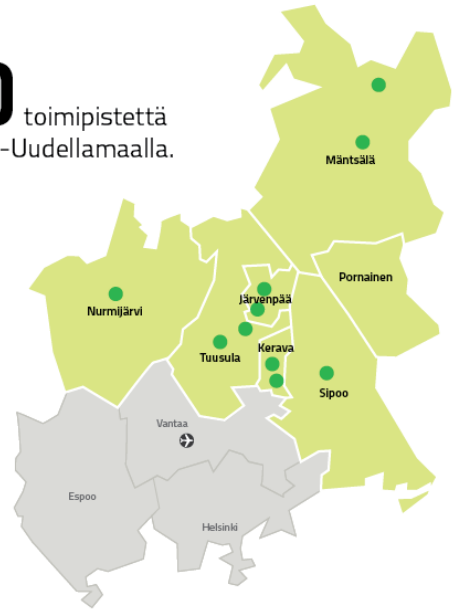
11 kumppaniverkostoa eri toimialoilta, joissa

110 yritysedustajaa

8500 yritystä.

työelämä- ja sidosryhmäyhteistyö

10 toimipistettä Keski-Uudellamaalla.



n. 12000
opiskelijaa vuonna 2022.

Ammatillinen koulutus **11024**

Aikuisten perusopetus **147**

Työvoimakoulutus **203**

Valmentava koulutus **198**

Vapaa sivistystyö **129**

80 eri tutkintoihin johtavaa ammatillista, työvoima- ja valmentavaa koulutusta sekä aikuisten perusopetusta.

77 äidinkieltä

Vieraskielisten osuus **18 %**

2873 oppisopimusta ja **4581** koulutussopimusta.

Päivitetty 03/2023

>> keuda.fi
#kestävä #saavutettava #uniikki
#omapolku #työelämäävarten

Keuda

- Keudassa oli tehty riskien arvioinnit.
- Kriisiviestintäsuunnitelma tehtynä (intrassa).
- Secapp-kriisiviestintäsovellus hankittuna, mutta käyttöönotto kesken.
- Kriisitilanteiden ”kriisijohtoryhmää” mietitty, valmisteltu, mutta ei varsinaisesti päätetty.

LÄHTÖTILANNE & VALMISTAUTUMINEN

>> keuda.fi
#kestävä #saavutettava #uniikki
#omapolku #työelämäävarten

Keuda

- **2021** Tarjous SOC-palvelusta operaattorilta, kallis
- **02 /2022** Toinen tarjous SOC-palvelusta operaattorilta, todettiin kalliiksi
- **03 /2022** Sovittu tietoturvakartoitus IT-palvelutoimittajan taholta

TEKNINEN VARAUTUMINEN ENNEN HYÖKKÄYSTÄ

- **03 /2022** Tietoturvaraportti, jonka perusteella tehtiin:
  - **MFA** henkilökunnalle ja opiskelijoille
  - **Rajattiin kirjautumisia** (O365) vain tietyistä maista
  - **Riskikirjautumisi**a rajattiin/estettiin
  - **MDE:** Microsoft päivitykset ok, muissa puutteita
  - **Käyttämättömiä DA-tunnuksia**, poistettiin mutta ei kaikkia
  - **Heikot protokollat**, kaikkia ei poistettu
  - **LAPS** ei käytössä, tilattiin, ei asennettu
- **16–17.11.2022** Savonia AMK:n esitelmä lunnashyökkäyksestä

maanantai 8.08
Oleto palaverissa?

Timo Hakkarainen maanantai 8.08
Velin kanssa puhelimessa

maanantai 8.14
Hei sammuttakaa kaikki mahdolliset järkevä järjestelmät

MK **Matti Kurki** maanantai 8.14
Onko jotain liikkeeellä?

MR **Miika Raassina** maanantai 8.15
CM on kaapattu

Tiedostonimi: PPCYaNT5s.README.txt

```
~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~

>>>>> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that
once your data appears on our leak site, it could be bought by your competitors at any second, so
don't hesitate for a long time. The sooner you
 pay the ransom, the sooner your company will be safe.

Tor Browser Links:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion

Links for normal browser:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion[.]ly
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion[.]ly
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion[.]ly
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion[.]ly
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion[.]ly
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion[.]ly
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion[.]ly
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion[.]ly
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion[.]ly

>>>>> What guarantee is there that we won't cheat you?
```

HYÖKKÄYKSEN ETENEMINEN 28.11.2022

Keuda

”

Päätettiin perustaa poikkeustilaryhmä, joka kokoontuu säännöllisesti, ylläpitää tilannekuvaa ja tätä kautta johtaa tilannetta ja siitä viestintää kokonaisuutena.

ENSIMMÄISET TUNNIT 28.11.2022

10.00 Poikkeustilaryhmän ensimmäinen kokous

- Ensimmäiset päätökset
  - Toimintalinja
  - Tiedotuslinja, vastuut ja viestintäkanavat
  - Tiedotusvastuu ulkoisesta viestinnästä yhden henkilön kautta
- **Sovittiin poikkeustilaryhmän kokoonpanosta**
  - Kuntayhtymän johtaja
  - Operatiivinen johtaja
  - Rehtori/vararehtori
  - Tietohallintopäällikkö (+vara)
  - Viestintä x 2
  - Tietosuojavastaava
  - Turvallisuuspäällikkö

ENSIMMÄISET TUNNIT 28.11.2022

04:12 – 9:00 Hyökkääjän tehokasta toiminta-aikaa → ympäristö nurin
8.14-10.00 Palvelinten ja verkkojen sammuttaminen

8:30, 8:51, 9:05 Soitto KY:n johtajalle
8:36-8:40 Puhelu Savoon ->It-päivien esimerkki
8:48; 8:49 Puhelu, turvallisuuspäällikkö: huolehti rikosilmoituksesta

8.30 Ilmoitus Kyberturvallisuuskeskukselle (lomake)
8:43, 8:50, 8:53 Puhelut, Kyberturvallisuuskeskus. Yhteensä noin 20 puhelua, korvaamaton apu, tuki
8:52 Soitto viestintäpäällikkö (lomalla)
8:38 Puhelut x 4 Tietoturvayhtiö A. Lopulta vastaus, mahdollisuus tutkia 2 viikon kuluttua.
11:11 Puhelu Tietoturvayhtiö B Mahdollisuus aloittaa tutkinta heti! Sopimus klo 12.00 ja aloituspalaveri klo 14.00

- **3 x** Poikkeustilaryhmä kokoontui
- **3 viestiä** henkilöstölle Secapp-sovelluksen kautta
- **2 tiedotetta** Keuda.fi
- **8 tiedotetta** Keudan some

ENSIMMÄISEN PÄIVÄN JATKOTOIMENPITEITÄ

- **klo 10.00** kaikki sammutettu ja verkot suljettu operaattorin toimesta.
  - Kirjautumattomien koneen käyttö kiellettiin → Ohjeistus!
- **klo 14.00** Tutkinnan käynnistyminen, kaikki tehtiin etänä.
  - Verkko avataan tutkintaa varten.
  - Työasemille/palvelimelle työasemaohjelma, joka välitti tietoa tietoturvayhtiölle.
- **klo 17.15** Statustilannepalaveri.
- **klo 21.00** Selvillä hyökkäyksen mistä tultu sisään, lähde, eteneminen.

>> keuda.fi
#kestävä #saavutettava #uniikki
#omapolku #työelämäävarten

Keuda

Asiasta ilmoitettiin välittömästi
Tietosuojavaltuutetun toimistoon, Kyberturvallisuus-keskukselle ja Keskusrikospoliisille.

Tilannetta selvittämään tietoturvakumppani.
Jo saman päivän iltana oli selvillä hyökkäyksen alkulähde, sen eteneminen sekä tilanteen vakavuus ja laajuus.

Varsinaisen hyökkäyksen alusta tiedettiin:
- Tilannetta ei laukaissut yksittäisen keudalaisen tai opiskelijan toiminta.
- Hyökkäyksen mahdollistanut palvelinympäristössä ollut tekninen haavoittuvuus.
- Kyberrikollisten kohde on valikoitunut sattumanvaraisesti.

ENSIMMÄISET 24H SUMMATTUNA

>> keuda.fi
#kestävä #saavutettava #uniikki
#omapolku #työelämäävarten

Keuda

Välittömästi hyökkäyksen jälkeen henkilöstö sopeutui hyvin tilanteeseen ja yhteishenki oli vahva: vilpitöntä halua auttaa yli yksikkörajojen, jotta välttämättömät toiminnot saatiin toimimaan.

Keudan tietohallinto-palveluiden nopea reagointi minuuttien sisällä hyökkäyksen havaitsemisesta pelasti vieläkin suuremmilta tuhoilta**.**

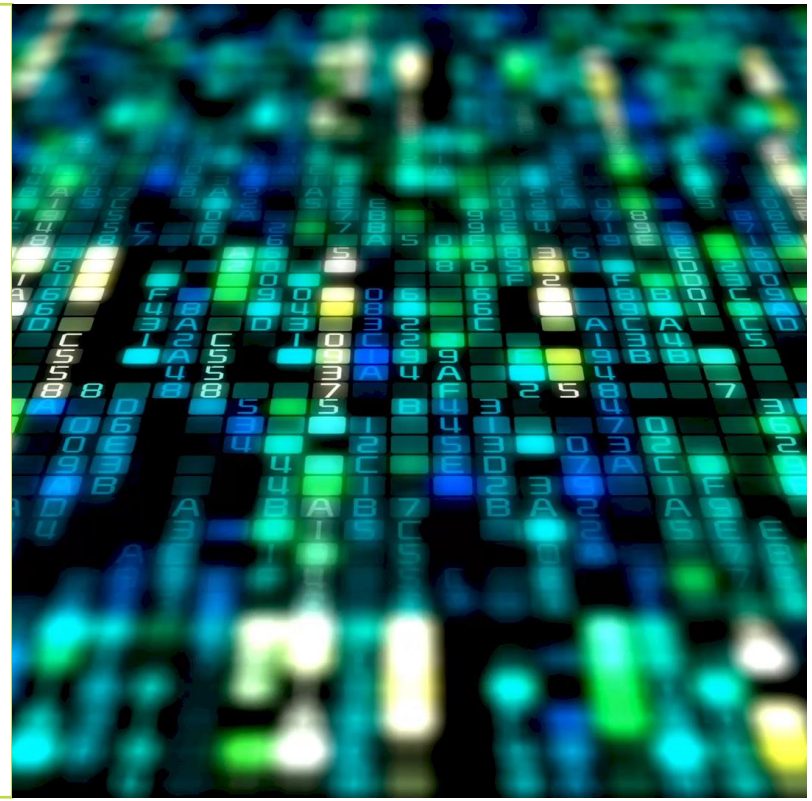
ENSIMMÄISET 24H SUMMATTUNA

>> keuda.fi
#kestävä #saavutettava #uniikki
#omapolku #työelämäävarten

Keuda

Tarkistuslistalla:

- ✓ **Koko henkilöstön tietokoneet**
- ✓ Ensimmäisen viikon aikana **500 henkilökohtaista tietokonetta**.
- ✓ **Opetusluokissa sijaitsevat tietokoneet**.
- ✓ Tietokoneista ja verkoista riippuvainen **opetus uudelleenorganisoitiin.**
- ✓ Tulostimet, kassapäätteet, palkanmaksu, kulkeminen, ilmastointi…



Ensiapu ja toiminta 28.11. jälkeen

Poikkeustilaryhmä kokoontui 14 kertaa

- Tärkein tehtävä varmistaa opetuksen ja toimintojen jatkuminen.
- Koronatartuntarypäs & tilanteen eskaloitumisen mahdollisuus→ ryhmät piti erottaa toisistaan

Henkilöstölle viestittiin 16 viestillä Secapp-sovelluksen kautta. Hyvä kanava, mutta käyttöä harjoiteltava

Viestintä ja tiedottaminen suuressa roolissa

- Keskimäärin **8 tiedotetta / päivä** Keudan some-kanaviin.
- **6 henkilöstöinfoa** Teamsilla
- Keudan intraan oma sivusto kyberhyökkäyksestä tiedottamiseen
- Erillinen tiedote yhteistyö-kumppaneille

29.11.2022 – 11.12.2022

>> keuda.fi
#kestävä #saavutettava #uniikki
#omapolku #työelämäävarten

Keuda

Henkilökunnan koneet 900 kpl

- Noin 1/3 saastuneita
- Saastuneet pois käytöstä ja uudelleen-asennus. Valmis10.12.

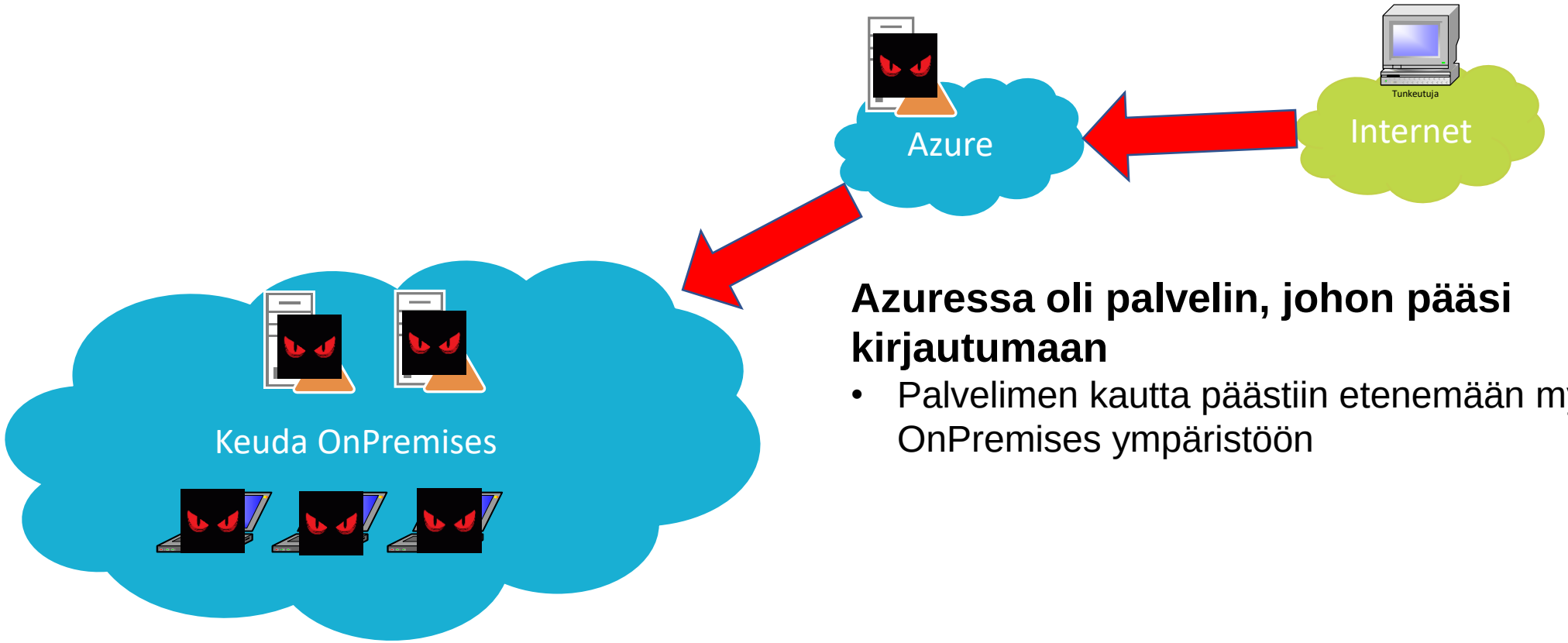
Luokkien koneet 1600 kpl

- 70% saastuneita
- Samalla Win10 → Win11
- Datan ja opetuksen ohjelmien palauttaminen vielä kesken

29.11.2022 – 11.12.2022

Palvelinympäristö

- AD palautettiin varmuuskopioista
- 90% palvelimista asennettiin uudestaan.
- Varmistuksista palautettiin yksi Domain Controller parin päivän takaisesta puhtaasta tilanteesta, jonka päälle alettiin rakentamaan palveluita uudelleen
- Microsoft 365 Defender auttoi puhtaan tilanteen määrittämisessä → apu selvitystyössä →mistä oli murtauduttu ja mitä tehty
- Pilvipalvelut säilyivät vahingoilta
- Ympäristö sisälsi tietosuojan alaista materiaalia, tietoturvayhtiön loppuraportin mukaan sen joutuminen ulos epätodennäköistä.



Azuressa oli palvelin, johon pääsi kirjautumaan

- Palvelimen kautta päästiin etenemään myös OnPremises ympäristöön

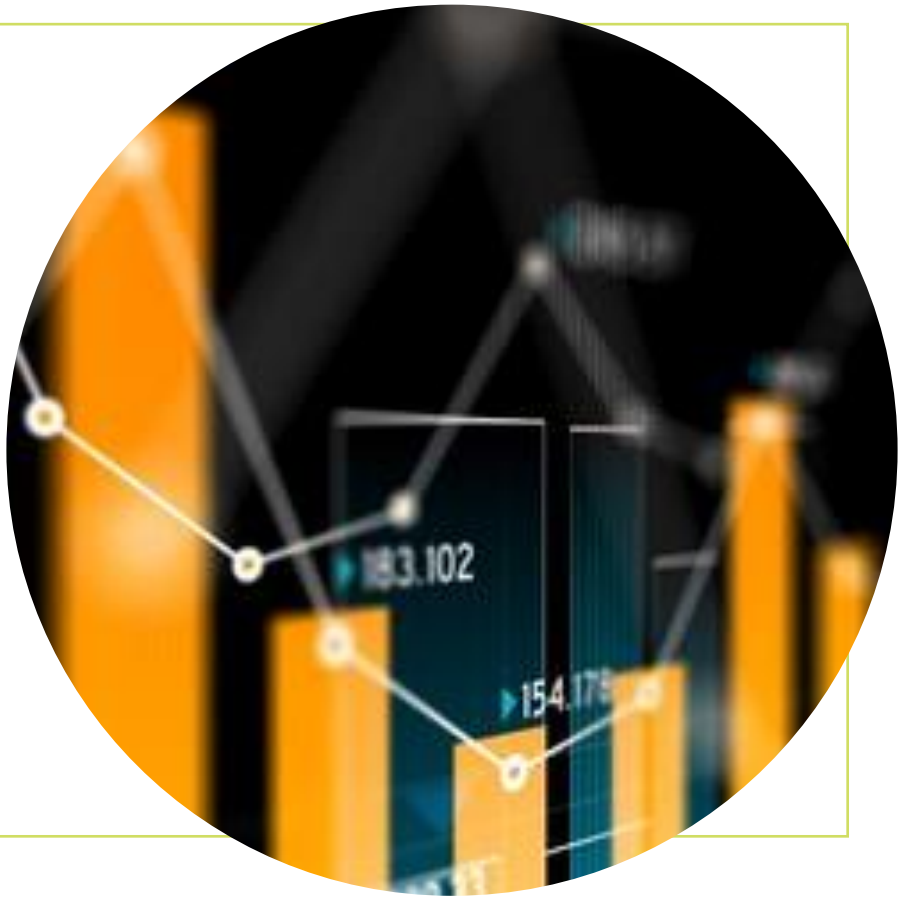
MITÄ TEKNISESTI TAPAHTUI?

Olemme päässeet palautumaan tilanteeseen nähden erittäin hyvin.

- Palautumistoimenpiteet jatkuvat tämän hetken tiedon mukaan **vielä pitkälle kevääseen 2023.**
- Emme tule palautumaan samaan ympäristöön, vaan **uudistamme samalla rohkeasti Keudan ICT-ympäristöä**.

PALAUTUMINEN JA UUDISTUMINEN

- Riittävän taitavaan hyökkäykseen ei käytössämme olevilla resursseilla pystytä suojautumaan
- **Ainoa keino suojautua: havaita poikkeukset ympäristössä riittävän ajoissa.**
- Vahingot minimoidaan + hyökkäyksen nopea pysäyttäminen.
- Ennen hyökkäystä luotto Keudan ICT-ympäristöön ja varautumiseen.
  - Suurin pelko liittyi yksittäisen käyttäjän toimiin.
  - Kaksivaiheinen tunnistautuminen opiskelijoille.
  - Ulkopuolisella yrityksellä teetetty tietoturvakartoitus.



JÄLKIPYYKKI

Johtaminen

>> keuda.fi
#kestävä #saavutettava #uniikki
#omapolku #työelämäävarten

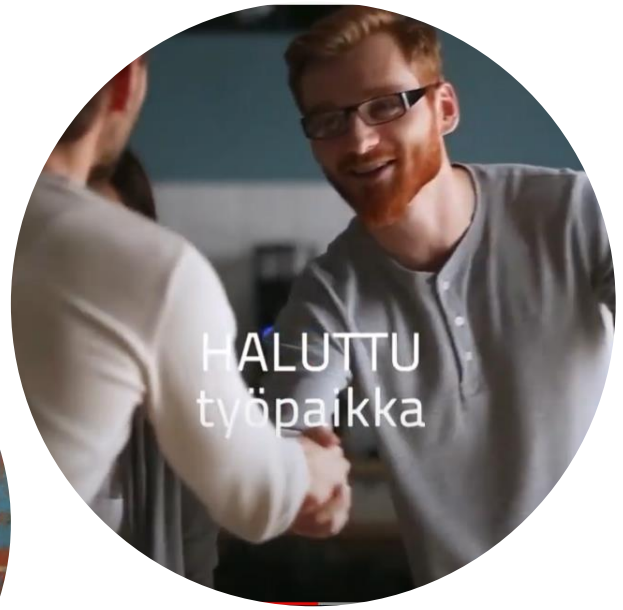
Keuda

Opit: Johdon rooli kyberkriisissä

- **Vastuun ottaminen kriisin ratkaisussa**
  - Nopeat ratkaisut vajailla tiedoilla
  - Rauhoittaminen
- **Tiimin rakentaminen kriisinhallintaan**
  - Kokoa moniammatillinen tiimi, jolla tavoite
  - Tunnista asiat, jotka vaativat koordinaatiota
  - Tunnista rajoitukset ajankäytössä ja ammattitaidossa
  - Muista inhimilliset tekijät
- **Toimien valitseminen kriisin päättämiseksi**
  - Auta priorisoinnissa
  - Hallinnoi päätöksentekoa, ei lopputulosta
- **Tilannekuvan viestiminen ja vaikeiden asioiden kiteyttäminen avoimesti ja säännöllisesti**
  - Läpinäkyvyys vs tietojen vähäinen salassapito
  - Oma epätietoisuus
  - Yksinkertaistaminen vs. tietotulva
- **Jälkihoitaminen**

Opit: Strateginen johtaminen ja rakenteet vaikuttavat kriisistä selviämiseen

- Resilienssikyky
  - Hyväksyttävä organisaation keskeneräisyys
- Organisaatiokulttuuri
  - Organisaation arvopohja testataan kriisissä
  - Keuda VAU - Välitämme, Arvostamme, Uudistumme
- Turvallisuuspolitiikka ja –organisaatio
  - Poikkeustilanteeseen valmistauduttava
- Viestintä
  - Työyhteisöviestinnän rakenteet kuntoon



Keuda

Yhteistyössä

Veli-Heikki Anttolainen

Tietohallintopäällikkö

E-mail: veli-heikki.anttolainen@keuda.fi

Puh: 050 2074

Twitter: @

LinkedIn: Veli-Heikki Anttolainen

Timo Hakkarainen

Operatiivinen johtaja

E-mail: timo.hakkarainen@keuda.fi

Puh: 050 5679022

Twitter: @

LinkedIn:

Riikka-Maria Yli-Suomu

Kuntayhtymän johtaja

E-mail: riikka-maria.yli-suomu@keuda.fi

Puh: 050 3486544

Twitter: @RiikkaMYliSuomu

LinkedIn: Riikka-Maria Yli-Suomu