E-Opas

Energiayrityksen kyberturvaopas

IBM Platinum Business Partner

ATEA

Kyberturvan tärkeys kasvaa myös energiasektorilla.

Kyberturvan tärkeys kasvaa teollisen esineiden internetin (IIoT) ja pilven aikakaudella nopeasti myös huoltovarmuuskriittisellä energiasektorilla. Informaatioteknologiasta on tullut erottamaton osa energiayritysten, kuten huoltoyhtiöiden, vesilaitosten ja sähköyhtiöiden, tuotantoa.

Huono uutinen on se, että ammattimaisia rikollisia kiinnostaa myös energiayritysten verkot sekä hallinta- ja automaatiojärjestelmät.

Hyvä uutinen on se, että nyt myös pienet ja keskikokoiset yritykset voivat parantaa lokien ja tietoturvatapahtumien hallinnalla kustannustehokkaasti omaa kyberturvatasoaan.

Miten energiasektorilla toimivan yrityksen kannattaa vahvistaa kyberturvatasoaan?

Haasteet kasvavat ja vaatimukset muuttuvat.

Automaatio- ja toimistoverkkoja rakennetaan energia-alalla kiihtyvää tahtia. IIoT ja uusien palveluiden kehittäminen vaativat verkkojen avaamista mm. tiedonsiir-rolle, jolloin verkkojen eristäminen ei enää riitä tietoturvaratkaisuksi.

Nämä asiat tuottavat haasteita erityisesti pienille ja keskisuurille energiasektorin yrityksille:

- Yrityksiltä puuttuu näkyvyys verkkojen sisäiseen liikenteeseen ja verkkoon kytkettyihin laitteisiin.
- Verkkojen eristämiseen luotetaan edelleen liikaa. Se on virhe.
- Kyberrikolliset etsivät verkoista reikiä täysautomatiikalla. Hallinta- ja automaatiojärjestelmiin sekä verkkoihin tehdyt hyökkäykset lisääntyvät koko ajan. Riskikuva on muuttunut.
- Hyökkääjät ymmärtävät teollisia hallinta- ja automaatiojärjestelmiä. Internetistä löytyy ohjeita.
- Omaa kyberturvaosaamista ei ole riittävästi.

Ratkaisuna edistyksellinen lokien ja tietoturvatapahtumien hallinta.

Atean lokien ja tietoturvatapahtumien hallintapalvelu tarjoaa kustannustehokkaan suojan sekä erinomaisen näkyvyyden organisaatiosi verkkoympäristöihin. Tekoälyllä ja analytiikalla tunnistetaan haittaohjelmat ja tietoturvapoikkeamat nopeasti.

Miten teknologia toimii? Palvelu voidaan toteuttaa erityisen kustannustehokkaasti Ciscon sovellustietoiseen verkkoinfraan, joka sisältää edistyksellisiä tietoturvaominaisuuksia. **Cisco Stealthwatchilla** ja **IBM QRadarilla** saadaan näkymä tietoturvatapahtumiin lyhyellä ja pitkällä aikavälillä. Niillä voidaan yhdistää lokitapahtumia sekä automatiikkaa ikään kuin yhdeksi tapahtumaksi, jolloin valvonta helpottuu ratkaisevasti.

Molemmat ratkaisut sisältävät tekoälyä ja koneoppimista. Identiteettipohjaiset verkkopalvelut sisältyvät Ciscon älykkääseen infrastruktuuriin.

Laita kyberturvan perusasiat kuntoon näin.

Pienillä investoinneilla ja fiksuilla toimenpiteillä saat paljon aikaan.

1. Selvitä verkkoympäristösi kyberturvataso ja anna kokeneiden ammattilaisten laatia yrityksellesi oma ’**security playbook**’. Playbook sisältää ohjeita ja rajauksia, kun teille ostetaan esimerkiksi uusi tietojärjestelmä.

2. Varmista **näkyvyys koko verkkoympäristöösi**. Kerää lokitiedot talteen, ja hanki kyvykkyys lokien analysointiin. Varmista, ettei verkkoympäristöösi pysty liittämään mitään tietoturvapolitiikkasi vastaisesti.

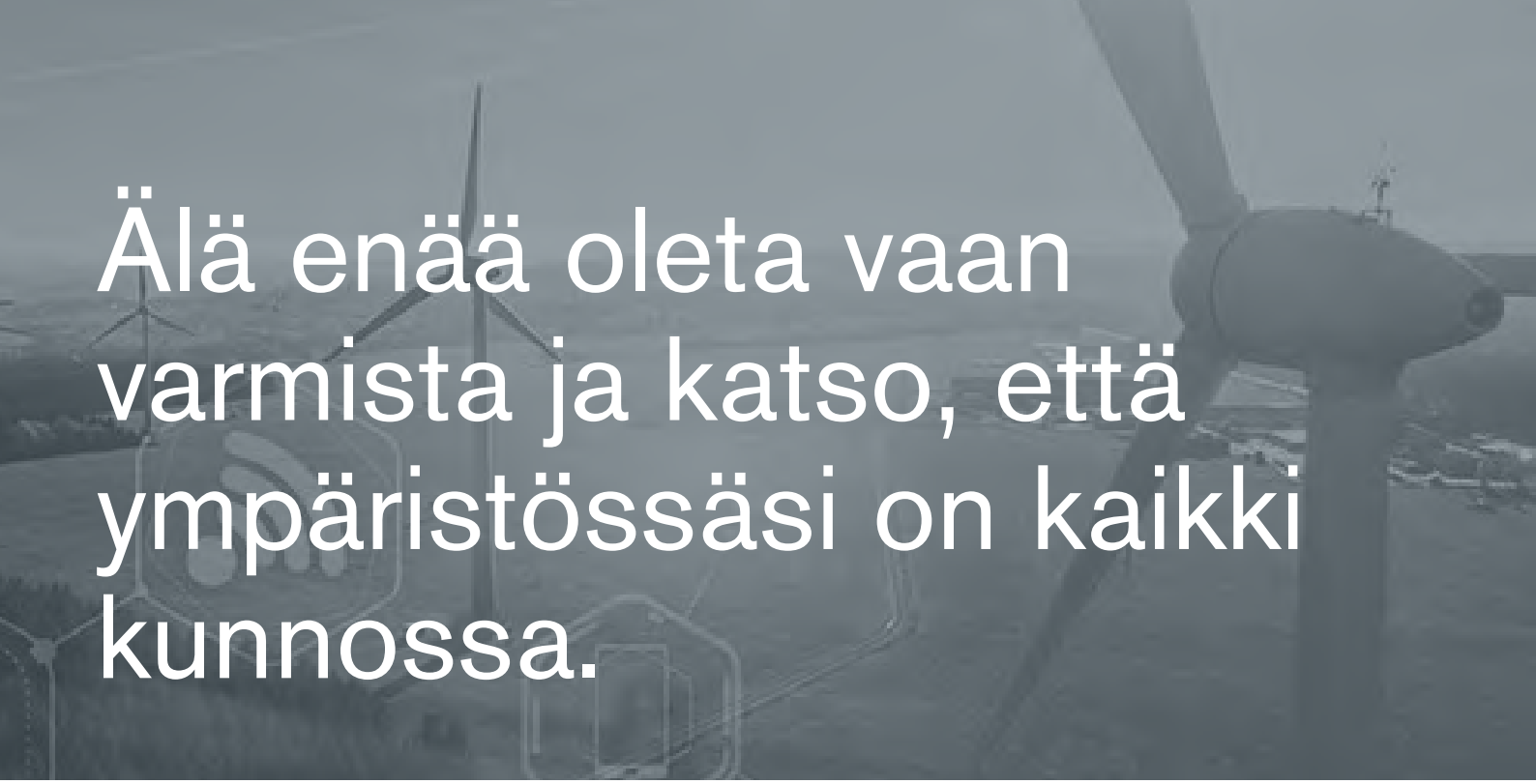
3. **Koveta rajapinnat** ja karsi kaikki turhat rajapinnat pois. Jätä rikollisille mahdollisimman vähän tartuntapintaa.

4. Panosta **tietoturvalliseen verkkoteknologiaan**.

5. **Tunnista jokainen laite, käyttäjä ja tietojärjestelmä** identiteettipohjaisella tietoturvalla.

6. **Varmista aina myös tietoturva, kun uudistat teollisuusverkkojasi.** Kysy ammattilaisten näkemyksiä.

Punaisen lipun noustessa on osattava toimia nopeasti. Saatko apua hyökkäyksen sattuessa?



Älä enää oleta vaan varmista ja katso, että ympäristössäsi on kaikki kunnossa.

Atealta saat tietoturvaopastusta sekä yrityksesi liiketoimintaa tukevan pelikirjan palveluineen.

- Rakennamme yrityksellesi tiekartan ja tarjoamme konkreettisen etenemissuunnitelman tietoturvan kehittämiseen.
- Huomioimme suunnittelussa nykyisen it-infrastruktuurisi, ja teemme ehdotuksen mikä olisi yrityksesi liiketoiminnan kannalta kustannustehokkain tapa edetä.
- Vahvistamme tietoturvaasi kerroksittain, ja tarjoamme kattavan valikoiman palveluja, kuten tukipalvelut ja tarvittaessa jopa 24/7 valvonnan (SOC).
- Atea Experience Centerissä näytämme miten lokien ja tietoturvatapahtumien hallinta oikeasti toimii.

IBM Platinum Business Partner

ATEA

atea.fi
customercare@atea.fi
010 613 611