WHITE PAPER

DIGITAALINEN TYÖYMPÄRISTÖ JA TIETOVERKOT

aruba
a Hewlett Packard Enterprise company

TYÖYMPÄRISTÖT JA VERKOT MURROKSESSA

Työn tekeminen digitalisoituu kaikilla toimialoilla erittäin nopeasti, ja menestyvän organisaation on kyettävä tarjoamaan työntekijöilleen tehokkaat ja turvalliset välineet työntekoon ajasta ja paikasta riippumatta. Yhteistyö eri sidosryhmien välillä lisääntyy, ja töitä tehdään yhä enemmän kannettavilla, tableteilla ja älypuhelimilla. Yrityksissä on oivallettu, että joustava ja tehokas työnteko edellyttää myös mahdollisuutta sallia työnteko työntekijöiden itse omistamilla laitteilla (BYOD).

Digitalisaatio ja mobilisaatio sekä pilvisovellusten kasvava käyttö ovat tuoneet jatkuvasti lisää vaatimuksia yritysten ja organisaatioiden digitaalisiin työympäristöihin. Hallittujen langattomien verkkojen merkitys on kasvanut laitteiden, sovellusten ja datan määrän kasvaessa. WLAN-verkot ovat digitaalisen työympäristön ytimessä.

Yritysten langattomiin verkkoihin on liitetty yhä laajempi kirjo erilaisia laitteita, kuten langattomia monitoimilaitteita ja tulostimia, infotauluja, projektoreita ja näyttöjä. Verkkoihin liitettyjen laitteiden määrä on kasvamassa lähivuosina äärimmäisen nopeasti, kun sensorein varustettujen IoT-laitteiden määrä kasvaa. Joillakin toimialoilla verkkoihin kytketään myös robotteja.

AUTOMAATION MERKITYS KASVAA

Digitaalinen työympäristö ei palvele verkon käyttäjiä eikä digitaalista liiketoimintaa riittävän tehokkaasti, mikäli verkoissa ilmenee suorituskykyyn tai luotettavuuteen liittyviä ongelmia.

Tietoverkkoja operoidaan ja hallitaan monissa yrityksissä edelleen manuaalisesti. Tämä tarkoittaa sitä, että verkkoon tehtävä yksinkertainenkin muutos voi olla aivan liian hidasta. Manuaalinen työ lisää myös konfigurointiin liittyvien virheiden määrää. Vikatilanteiden ratkominen hidastuu, eikä käyttäjiä ja liiketoimintoja kyetä palvelemaan verkottuvassa taloudessa riittävän tehokkaasti. Asiantuntijoiden resursseja käytetään tuki- ja päivitystehtävien suorittamiseen.

Skaalautuvuus tuottaa myös haasteita, mikäli tietoverkkoihin ja tietoliikenteen määriin ei ole näkyvyyttä. Kustannukset nousevat, eikä kyberuhkilta pystytä suojautumaan riittävän tehokkaasti.

Verkossa ilmenevät ongelmat ja pullonkaulat vaikuttavat verkottuvassa taloudessa yhä keskeisemmin myös liiketoiminnan jatkuvuuteen.

LANGATTOMIEN VERKKOJEN PAINOARVO KASVAA

Langattomilla verkoilla on korvattu jo vuosien ajan lanka-verkkoja. Langattomat verkot ovat yhä suorituskykyisempiä, ja käyttäjät liittyvät yritysten tietoverkkoon tänä päivänä jo ensisijaisesti WLAN-verkkojen kautta.

Tutkimusyhtiö Gartnerin mukaan maailmassa on vuonna 2020 noin 21 miljardia IoT-laitetta. ICT-laitteet, kuten älypuhelimet eivät sisälly lukemaan. Verkosta on rakennettava turvalliset yhteydet myös pilvestä käytettäviin sovelluksiin sekä pilvessä sijaitsevaan tietoon. Yritysten verkkoympäristöissä on usein eri laitevalmistajien laitteita. Uusimmilla hallintaratkaisuilla voidaan hallita myös eri laitevalmistajien verkkolaitteita, kuten kytkimiä ja tukiasemia.

Digitalisaatiota ja IoT:ta palvelevaa digitaalista työympäristöä ei voida toteuttaa, mikäli verkko ei ole pitkälle automatisoitu, keskitetysti hallittu, läpinäkyvä, skaalautuva ja tietoturvallinen.

MITEN YRITYKSET VOIVAT HALLITA MOBILITEETTIIN JA IOT:HEN LIITTYVIÄ RISKEJÄ?

Tietoverkkoihin liittyviä riskejä voidaan vähentää panostamalla tietoturvapolitiikkaan myös tietoverkoissa. Tietoturvapolitiikalla luodaan säännöt, ja sellainen pitää olla myös pienemmissä yrityksissä.

1. Tietoverkkoon pääsevien käyttäjien ja laitteiden tunnistaminen. Se edellyttää automaatiota. On määriteltävä, kenellä on oikeus päästä ja millä laitteella mihinkin tietojärjestelmään käsiksi.
    - Näkyvyys verkkoon ja verkkoon kytkettyihin laitteisiin. Tarvitaan kyvykkyys tunnistaa kaikki verkkoon kytketyt laitteet. On määriteltävä mihin tieto-järjestelmiin laitteet kytkeytyvät sekä varmistettava laitteiden tietoturva.
    - Automatisoitu identiteetinhallinta. Verkkoon kirjautuvien laitteiden ja henkilöiden tunnistamisen lisäksi saadaan tietoa mistä ja mihin aikaan päivästä verkossa ollaan kirjautuneena. Yritys voi rajoittaa eri henkilöiden pääsyä eri osiin verkosta.
2. Lankaverkkojen tietoturvan varmistaminen. Mobiliteetin turvaaminen edellyttää myös sitä, että lankaverkkoyhteydet on varmistettu.
3. Prosessit vikatilanteiden varalle. Pääsynhallinnan ja tietoturvan tehostaminen edellyttää myös automatisoitua kommunikaatiota tilanteissa, joissa henkilön tai laitteiden pääsy estetään tietoverkkoon.

Markkinoilla ei ole yhtään yksittäistä ratkaisuja, jonka avulla yritys pystyy ratkomaan kaikki mobiiliteettiin ja digitaaliseen työympäristöön liittyvät riskit. Yritykset tarvitsevat keskenään tehokkaasti integroituvaa teknologiaa.

G30 Finland Oy
Äyritie 12 A, 01510 Vantaa
www.g30.fi
puh. 0400 172271