TURUN KRISTILLINEN OPISTO

Case: WatchGuard | 11/2015

LINNASMÄKI

Linnasmäki Oy on Turun kristillisen opiston yhteydessä toimiva kokoushotelli.

- Kokousvieraita on 20.000 – 30.000 vuosittain.
- Tietoliikennetarpeet vaihtelevat.
- Kirkolliskokous kokoontuu vuosittain, noin 200 edustajaa, 50 vierasta, lisäksi median edustajat.

Toiminnan kasvu vaati uusia, turvallisia verkkoratkaisuja

Opiskelijamäärien kasvu ja toimintojen lisääntyminen olivat johtamassa sisäverkon palvelutason laskuun. Turun kristillisellä opistolla jo pitkään käytössä ollut WatchGuard x6500e -palomuuriratkaisu ei enää palvellut riittävästi.

Opiston tietohallinto tiedosti muutostarpeen ja alkoi aktiivisesti kartoittaa mahdollisuuksia kehittää sisäverkon tietoturvaa ja hallintaa. Erityisen tärkeänä pidettiin sisäverkon monitorointia, jotta liikennemäärien kasvu saataisiin hallintaan ja pystyttäisiin varmistamaan opiston keskeiset toimintaprosessit. Myös tietoturva oli saatettava ajan tasalle, sillä useiden käyttäjäryhmien ja monenlaisten päätelaitteiden käyttö oli tiedostettu riski.

Toisena kehityskohteena oli kampuksen langaton verkko. Langattoman verkon kuormitus oli kasvanut vieläkin voimakkaammin kuin sisäverkko. Opiskelijoiden lisäksi kokoushotelli Linnasmäen asiakkaat sekä muun muassa vuotuisen kirkolliskokouksen osallistujat asettivat kovia vaatimuksia silloiselle WLAN-toteutukselle. Olemassa oleva toteutus ei enää riittänyt ja sen hallinnan mahdollisuudet olivat olemattomat, joten langattoman verkon päivitys oli myös edessä.

ONGELMAN RATKAISU

Kapasiteettia lisättiin ja palomuuriratkaisuksi päivitettiin WatchGuard XTM 850 kaikilla UTM-moduuleilla (Unified Threat Management):
- LiveSecurity Plus – laitetakuu.
- Application Control – sovellusten hallinta, esim. erilaisten tietoturvatasojen määritteleminen eri käyttäjäryhmille sovellusten mukaan.
- WebBlocker – web-kategoriaan perustuva suojaus, estää mm. sopimatonta sisältöä, seuraa internetin käyttöä, mahdollistaa räätälöidyt estolistat jne.
- SpamBlocker – roskapostien skannaus ja esto.
- Gateway Antivirus – yhdyskäytävätason antivirusohjelma.
- Intrusion Prevention Service (IPS) - hyökkäyksen havainnointi- ja esto; moduuli, joka havaitsee verkkoon tunkeutumiset, mm. vakoiluohjelmat.
- Reputation Enabled Defense (RED) – dynaaminen mainetietokanta, joka huolehtii, että käyttäjät eivät pääse virusten valtaamille web-sivustoille.

Ilkka Kiesiläinen, Turun kristillisen opiston järjestelmäasiantuntija.

Opistolla käy kymmeniä tuhansia kokousvieraita vuosittain. Käyttäjien vaihtelevat määrät asettavat tietoverkoille haasteita.

WathGuard XTM 850 on Enterprise-tason palomuuri ja se tarjoaa erinomaisen vaihtoehdon juuri vaihtelevan kuorman käsittelemiseksi.

Lisäksi valittiin työkalu uhkien tunnistamiseen ja visualisointiin - WatchGuard Dimension. Tämä konsolinäkymän tarjoama hallintatyökalu on osoittautunut erityisen toimivaksi. Dimensionia hyödynnetään erityisesti tietoturvapolitiikan käytännön jalkauttamiseen. Lisäksi työkalun avulla pystytään valvomaan, että verkon käyttö on juuri opiston tarpeiden mukaista.

Langattoman verkon kehitys toteutettiin vaihtamalla vanhat tukiasemat WatchGuard AP 100 ja 200 –malleihin. Näin langattoman verkon tietoturvaongelmat ongelmat saatiin helposti kuriin, koska myös tukiasemat ovat saman Dimension hallinnan piirissä. WatchGuard tukiasemat tarjosivat merkittävän suorituskyvyn parannuksen verrattuna edeltävään toteutukseen.

“Luonnollinen valintamme oli tukeutua WatchGuardin ratkaisuihin myös kehittäessämme verkkoympäristöä” – Ilkka Kiesiläinen, Turun kristillisen opisto

RATKAISUN HYÖDYT JA KOKEMUKSET

”Meillä on pitkäaikainen, noin kymmenen vuoden mittainen kokemus WatchGuardista ja koska olimme tyytyväisiä käyttäjiä, niin luonnollinen valintamme oli tukeutua samaan myös kehittäessämme ympäristöä”, kertoo Turun kristillisen opiston järjestelmäasiantuntija **Ilkka Kiesiläinen**, ja jatkaa: ”Uudemman polven palomuuri, tai oikeammin verkon tietoturvalaite, on tarjonnut meille hakemaamme suoritustehon kasvua ja mahdollistanut tietoturvamme noston uudelle tasolle. Tämä on taustalla toimiva järjestelmä, joita käyttäjät ja opiston johtokaan eivät välttämättä tiedä hyödyntävänsä, mutta ilman näitä perustoiminnat ajautuisivat nopeasti toimintakelvottomiksi.”

Kiesiläinen kertoo, että käyttäjät antavat suoraa palautetta erityisesti langattomasta verkosta. ”Langattomuus kasvaa koko ajan ja laajenee myös opetukseen ja nyt meillä on erityisen toimiva ympäristö ottamaan tulevaisuuden haasteet vastaan”, toteaa hän tyytyväisenä.

TOIMITTAJA

PINUS

myyntis@pinus.fi

Puh 075 325 0000

WWW.PINUS.FI

TULEVAISUUDEN SUUNNITELMAT JA KEHITYSPOLUT

Ilkka Kiesiläinen kertoo Turun kristillisen opiston ja siten myös Linnasmäen kehitysuunnitelmista seuraavaa: ”Tietoturvahan ei ole koskaan valmista, joten hyödynnämme Dimension-hallintaa säännöllisesti mahdollisten uusien tietoturvauhkien havainnointiin. Uhkien havainnointi on jatkossa yhä haastavampaa, koska tunnistuksia ei ehditä enää tekemään sillä nopeudella kuin uusia uhkia syntyy. Siksi olemme kiinnostuneita WatchGuardin uuden polven, käyttäytymiseen pohjautuvasta suojauksesta, APT Blockerista (Advanced Persistent Threats, kohdennettujen, kehittyneiden uhkien torjunta). Erityisesti kiinnitämme huomiota myös verkon segmentointiin ja sitä kautta turvaamme verkkoamme.”

PINUS RATKAISEE KOKONAISUUKSIA

Pinus-ryhmään kuuluvat IT-infrastruktuuriin ja siihen liittyvien ICT-palveluiden sekä laitteiden toimituksiin erikoistunut PC Pinus Oy, Baltiassa toimiva PC Pinus Computer SIA, atk- ja toimistotarvikkeiden toimittaja Turku X-Files Oy sekä asiantuntijayritys PC Pinus Solutions Oy, joka keskittyy ICT-infrastruktuurin ja siihen liittyvien palveluiden ja laitteiden toimituksiin. Asiakkaille tämä tarkoittaa palvelujen löytymistä saman katon alta, luotettavasti ja joustavasti. Pinus uskoo henkilökohtaiseen palveluun ja kulkee tekniikan kehityksen kärjessä. Palvelukonseptin tavoitteena on taata asiakkaiden liiketoiminnan jatkuvuus kaikissa tilanteissa.

Tietoturva on paljon laajempi kokonaisuus kuin pelkkä virusten torjuminen. Tietoturvapalvelut voidaan kytkeä saumattomaksi osaksi perustietotekniikkaa. Pinus kartoittaa yrityksen tietoturvatason ja tekee kehityssuunnitelman, joka huomioi esimerkiksi virransyötön, kameravalvonnan, vikasietoisuuden, autentikoinnin, käyttöoikeudet, etäyhteydet ja -käyttäjät sekä tiedon turvallisen hävittämisen. Pinus on WatchGuardin Silver-sertifioitu kumppani.