TAITAJA MÄSTARE Pori 2022 | SkillsFinland

Pilvipalvelut – esitehtävä

Työskentelet IT-asiantuntijana Veijon Metalli Oy:llä, jonka koko infrastruktuuri kryptattiin kyberhyökkäyksessä viime kuun vaihteessa. Digitaalinen forensiikkatutkimus jatkuu kyseisessä ympäristössä koko ajan ulkopuolisen konsultointitalon toimesta ja sinun pitää alkaa pystyttää rinnalle uutta pilvipohjaista lähestymistä.

Käyttöösi on jo perustettu Office 365-ympäristö, johon sinun tulee luoda käyttäjille tilit lisätietoineen. Käyttäjätiedot on saatu ulos viimekuun HR-raportin liitteestä, joka sijaitsee kohteessa: https://elisa.to/taitaja2022-esitehtava-kayttajat.

HR-raportin liitteessä on myös toinen välilehti *Ryhmäjäsenyydet*. Luo ryhmät pyydetyn kuvauksen mukaisesti ja lisää kaikki halutut käyttäjät ko. ryhmiin. Yrityksen IT-johtaja haluaa, että kaikille **Veijon Metallin Käyttäjät** -ryhmään kuuluville annetaan nyt ja tulevaisuudessa automaattisesti Microsoft 365 E3 lisenssit. Mikäli käyttäjä poistuu ryhmästä, tulee lisenssin myös poistua automaattisesti.

Veijon metallilla on rekisteröity julkisesti selvittyvä toimialue **veijonmetalli.fi**. Koska nimipalvelusikin tuhoutuivat kyberhyökkäyksen takia, tulee sinun luoda Azureen ko. toimialueelle julkisesti selvittyvä DNS-palvelu käyttäen Azuren natiiveja kyvykkyyksiä.

Veijon Metallin nettisivut on myös saatava toimimaan. Onneksi yritys oli juuri uudistamassa www-sivujaan ja tehtävänäsi on nyt asentaa sovelluskehittäjien tekemä uusi web-sivu käyttöön Azure App Servicen päälle. Sivustolle tulee päästä valitsemallasi **<jotain>.azurewebsites.net** -osoitteella sekä valinnaisella toimialuenimellä **www.veijonmetalli.fi**. Saat ladattua sovelluskehittäjien tekemän web sivun osoitteesta: https://elisa.to/taitaja2022-esitehtava-websivu.

Kyberhyökkäyksen alustavaksi reitiksi on epäilty haavoittuvuuden hyötykäyttöä Veijon Metallin yhdellä toiminnanohjausjärjestelmään liittyvällä palvelimella, jota ei ole päivitetty vuosikausiin. Luo nyt Veijon Metallille uusi Windows Server 2022 palvelin liitteenä olevan määrityksen mukaan, jotta sovellustoimittaja pääsee asentamaan siihen toiminnanohjausjärjestelmää uudestaan. Sovelluksen sisäiset datat tullaan palauttamaan varmuuskopioista ensiviikolla.

Laita palvelin päivittymään viikoittain käyttäen Azuren natiiveja työkaluja niin, että sen päivitysten raportointi on myös saatavissa ko. työkalusta.

Palvelin on mitoitettu tarkasti kapasiteetin puolesta, joten sen prosessorin suorituskykyä tulee monitoroida ja tarvittaessa kasvattaa sen kapasiteettia. Luo Azure Monitorilla sääntö, joka hälyttää, kun prosessorin käyttöaste kasvaa yli 80% (keskiarvo 15min ajalta, mitataan 5min välein). Hälytyksen lauetessa tulee lähteä sähköpostitse ilmoitus Veijon Metallin IT-johtajalle.

Palvelimelle tulee sallia RDP-yhteydet nykyisestä julkisesta IP-osoitteestasi.

TAITAJA MÄSTARE Pori 2022 | SkillsFinland

Toiminnanohjausjärjestelmän palvelintiedot

Asetus	Arvo
Nimi	veijoerp01
Region	North Europe
Image	Windows Server 2022 Datacenter: Azure Edition
Size	Standard_D2s_v3
Username	Paakayttaja
Password	VeijonKyberhyokkays2022!
Disks	Datadisk: 64GB Standard SSD ZRS
Login with AzureAD	True