Microsoft

Azure AD -käyttäjätietojen vaarantumisindikaattorit

Daniel Wood

Ohjelmapäällikkö

Azure AD -käyttäjätietojen suojaus

18.2.2021

Solorigate-videosarja

Neljä hyökkäysmallia Azure Active Directoryssa

01 Malli 1: Väärennetyt SAML-tunnukset, jotka käyttävät varastettua SAML-tunnusallekirjoitusmateriaalia

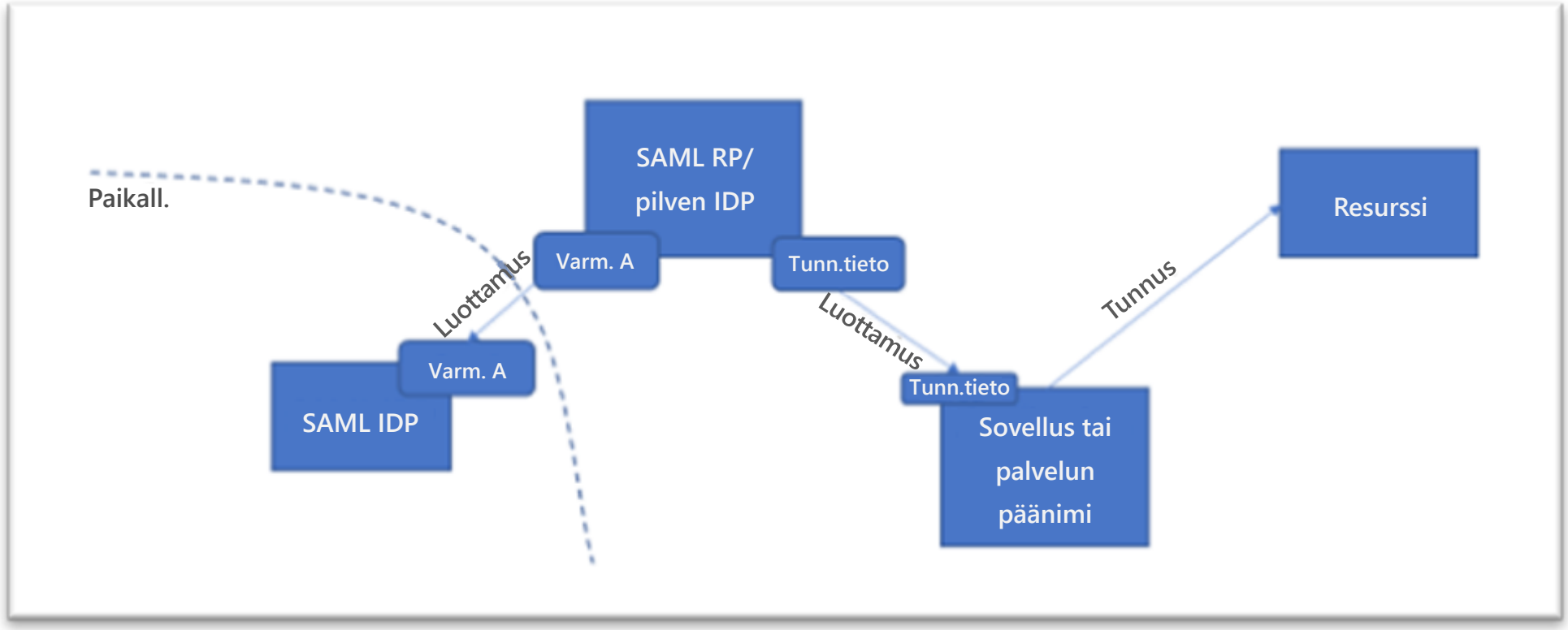
02 Malli 2: SAML-luottamussuhteiden laittomat rekisteröinnit.

03 Malli 3: Tunnistetietojen lisääminen olemassa oleviin sovelluksiin

04 Malli 4: Kyselyt, joissa tekeydytään olemassa oleviksi sovelluksiksi

Microsoft Security

Solorigate-videosarja



01. Malli

Väärennetyt SAML-tunnukset, jotka käyttävät varastettuja SAML-tunnusallekirjoitusmateriaalia

Etsittävät kohteet:

- SP:n vastaanottamat SAML-tunnukset ja määritykset, jotka poikkeavat IDP:n määritetystä toiminnasta.
- SP:n vastaanottamat SAML-tunnukset, joita vastaavia myöntämislokeja ei ole IDP:ssä.
- SP:n vastaanottamat SAML-tunnukset, joissa olevia monimenetelmäisen todentamisen vaatimuksia vastaavia monimenetelmäisen todentamisen toimintolokeja ei ole IDP:ssä.
- IP-osoitteista, agenteista, ajoista tai palveluista vastaanotettavat SAML-tunnukset, jotka poikkeavat tunnuksessa mainitusta pyytävästä käyttäjätiedosta.
- Merkit luvattomista hallintatoiminnoista.

Toimenpiteet:

1. Määritä varmenteiden luvattoman siirron mekanismi ja tee korjaukset.
2. Tarkista kaikki SAML-tunnusten allekirjoitusvarmenteet.
3. Vähennä mahdollisuuksien mukaan riippuvuuttasi paikallisesta SAML-luottamuksesta.
4. Käytä HSM:ää SAML-tunnusten allekirjoitusvarmenteiden hallintaan.

02. Malli

SAML-luottamussuhteiden laittomat rekisteröinnit

Etsittävät kohteet:

Poikkeava hallintaistunto, joka liittyy liitettyjen luottamussuhteiden muuttamiseen.

Toimenpiteet:

1. Tarkista, että kaikki liitetyt luottamussuhteet ovat kelvollisia.
2. Määritä järjestelmänvalvojatilin tekeytymisen mekanismi.
3. Tarkista järjestelmänvalvojatilin tunnistetiedot.

03. Malli

Tunnistetietojen lisääminen olemassa olevaan sovellukseen

Etsittävät kohteet:

- Poikkeava hallintaistunto, joka liittyy liitettyjen luottamussuhteiden muuttamiseen.
- Odottamattomien palvelun päänimien lisääminen etuoikeutettuihin rooleihin pilviympäristöissä.

Toimenpiteet

1	Tarkista tunnistetietojen muuttamistoiminnot kaikista sovelluksista ja palvelun päänimistä.
2	Tarkista ylimääräiset käyttöoikeudet kaikista sovelluksista ja palvelun päänimistä.
3	Poista kaikki passiiviset palvelun päänimet ympäristöstäsi.
4	Tarkista säännöllisesti kaikkien sovellusten ja palvelun päänimien tunnistetiedot.

04. Malli

Kyselyt, joissa tekeydytään olemassa oleviksi sovelluksiksi

Etsittävät kohteet:

- Poikkeavat resurssipyynnöt luotetuista sovelluksista tai palvelun päänimistä.
- Pyynnöt palvelun päänimistä, jotka ovat lisänneet tai muokanneet ryhmiä, käyttäjiä, sovelluksia, palvelun päänimiä tai luottamussuhteita

Toimenpiteet:

1. Tarkista, että kaikki liitetyt luottamussuhteet ovat kelvollisia.
2. Määritä järjestelmänvalvojatilin tekeytymisen mekanismi.
3. Tarkista järjestelmänvalvojatilin tunnistetiedot.

Solorigate-videosarja

Seuraavat vaiheet

01 Katso Solorigate-videosarja tästä sijainnista

02 Saat lisää päivityksiä Microsoft Security -sivustosta: www.microsoft.com/en-us/security/business

03 Lue blogitekstit osoitteesta www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security

Microsoft