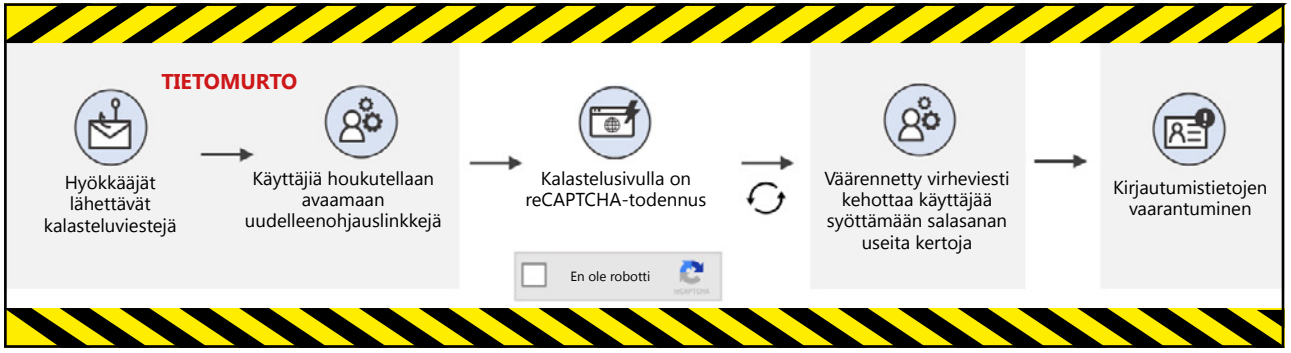
TechData A TD SYNNEX Company | Microsoft

Estä Azuren tietomurrot

Me kaikki tiedämme, että hakkerit käyttävät luovuutta ja tietomurtoja tapahtuu monin tavoin. Viime aikoina tietoomme on tullut useita tietomurtoja joissa ulkopuoliset tahot ovat aiheuttaneet kohtuuttoman suuria laskuja loppuasiakkaille.

Tiedäthän, että 91% hyökkäyksistä on peräisin kalasteluviesteistä, ja tapahtumaketju voisi olla seuraava:



Toimenpiteitä hyökkäysten estämiseksi:

- Tarkista, mitkä Azure-käyttäjät, -tenantit tai -tilaukset ovat riskeille alttiina Azure-portaalissa.
- Käy läpi ja tarkasta kaikki Azure-resurssit ja -palvelut sekä kiinnitä huomio epäilyttäviin tai uusiin tunnistamattomiin resursseihin .
- Poista kaikki epäilyttävät Azure-resurssit tai Azure-tilaukset.
- Varotoimena suosittelemme vahvasti, että kaikkien Azure-tenanttien global admin-käyttäjät vaihtavat salasanansa, jos he eivät ole niin jo tehneet.
- Tarkista ja varmista kaikki global admin-käyttäjien salasanan palautukseen käytettävät sähköpostiosoitteet ja puhelinnumerot Azure AD:ssa ja päivitä tarvittaessa.

Alle on listattu konkreettisia toimintaohjeita tietojen kalastelun ehkäisemiseksi.

Käyttöoikeudet

Loppukäyttäjien Microsoft-ympäristöille tehtävät perustarkastukset:

✓ Tarkista käyttäjien käyttöoikeudet

- Onko käyttäjälistasi ajan tasalla?
- Kuinka usein päivität käyttäjien käyttöoikeuksia?
- Onko kaikki käyttäjät koulutettu tunnistamaan kalasteluhyökkäykset?
- Kuinka monella käyttäjällä on globaalin järjestelmänvalvojan oikeudet? (Microsoft suosittelee yleensä 2-4:ää globaalia järjestelmänvalvojaa)
- Ovatko globaalit järjestelmänvalvojat koulutettuja?
- Minkä tason tietoturvatarkastuksia on käytössä? (seurantatyökalut ja pääsynesto)

- Salasanaton kirjautuminen – Windows Hello
- MFA-tunnistautuminen

✓ Laitehallinta

- Miten laitteet on suojattu?
- Onko kaikki laitteet ajan tasalla?
- Tietoturvakäytännöt?

✓ Zero Trust

- Ota käyttöön Zero Trust -malli valmistautuaksesi paremmin tulevaisuuden hyökkäyksiin käyttäen Microsoftin Zero Trust -kyselyä ja sen mukana tuomia suosituksia.

Muistuta kaikkia pilvipalveluiden käyttäjiä Microsoftin jaetun vastuun mallista.

Tech Data
A TD SYNNEX Company

Microsoft

Mitkä työkalut auttavat suojautumaan uhkatilanteilta?

- **SecureScore**
  Arvioi nykyinen tietoturvatilanteesi ja tunnista mahdolliset parannukset kaikissa Microsoft 365 -ympäristöissäsi käyttäen Secure Scoren keskitettyä näkymää.
- **Microsoft Defender Office 365**
  Microsoft Defender for Office 365 suojaa organisaatiosi sähköpostiviestien, linkkien (URL) ja tiimityökalujen (esim. Teams ja SharePoint) muodostamilta vahingollisilta uhilta.
- **MFA-tunnistautuminen**
  Monivaiheinen tunnistautuminen (MFA) lisää uuden suojauskerroksen kirjautumisprosessiin. Tililleen tai sovellukseen kirjautuessaan käyttäjät suorittavat identiteetin lisävarmennuksen esimerkiksi skannaamalla sormenjälkensä tai syöttämällä puhelimeen lähetetyn koodin.
- **Microsoft Defender for Cloud**
  Defender for Cloud on työkalu tietoturvatilanteen hallintaan ja uhilta suojautumiseen. Se vahvistaa pilviresurssien tietoturvaa sekä suojelee valmiiden palvelupakettien avulla Azuressa, hybrid-ympäristöissä ja muilla pilvialustoilla toimivia työkuormia.
- **Sentinel**
  Microsoft Sentinel on skaalautuva, pilvinatiivi tietoturvaratkaisu, joka yhdistää Security Information and Event Management (SIEM) sekä Security Orchestration, Automation and Response (SOAR) toiminnallisuuden. Microsoft Sentinel mahdollistaa älykästä tietoturva-analytiikkaa ja uhka-analyyseja kattaen koko yrityksen tarpeet, tarjoten kokonaisratkaisun hyökkäysten havaitsemiseen, uhkien näkyvyyteen, ennakoivaan seulontaan sekä uhkiin vastaamiseen.

Seuranta ja estäminen

- **Azure Cost Management**
  Azure Cost Management -työkalun avulla voit asettaa kulubudjetteja sekä määrittää niihin haluamiasi hälytysrajoja. Saat hälytyksen, kun kulutus ylittää tietyn ennaltamääritetyn raja-arvon. Jos haluat luoda Azure-budjetteja, lue tämä artikkeli.

Microsoftin parhaat käytännöt

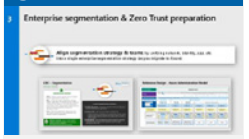
1

Secure Scoren käyttöönotto riskien vähentämiseksi

2

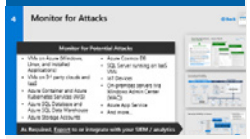
Salasanaton tai MFA-kirjautuminen järjestelmänvalvojille

3



Zero Trust yrityksen tietoturvastrategiassa

4



Tietoturvauhkien suojauksen käyttöönotto Azure-resursseille

5

Seuraa suosituksia DevOps-ympäristöjen suojaamiseksi

Miten Tech Data voi auttaa

✓ Koulutus
- Tech Data Security Awareness -ohjelma

✓ Käyttövalmiit Click-to-Run-ratkaisut
- Secure Score
- Cloud Backup
- Sentinel
- Ransomware

✓ Tietoturvaan keskittyneet palvelut
- Opeta minua
- Auta minua
- Tee se puolestani

✓ BPA-tiimi
- Botin ajaminen MSFT Partner Centerissä
- Asiakasympäristöjen tietoturva-asetusten tarkastus (MFA käyttö)

Kaksi asiaa jolla tarjoat paremman suojan asiakkaillesi (TEE AINAKIN TÄMÄ!):

1. MFA-tunnistautuminen pakolliseksi kaikille admin-käyttäjille
2. Aseta kulubudjetti Azure Cost Management-palvelussa

Lisätietoa löydät seuraavista :

Next Gen pdf >

Ransomware >

Suojaa Azure-asiakkaasi >

Azuren kustannushallinta >

Kiinnostavatko pitkän aikavälin ratkaisut? Ota yhteyttä paikalliseen Tech Data -toimipisteeseesi:
cloudsoftware.fi@techdata.com