

# Azure AD Identity-IdCs

**Daniel Wood**

Program Manager

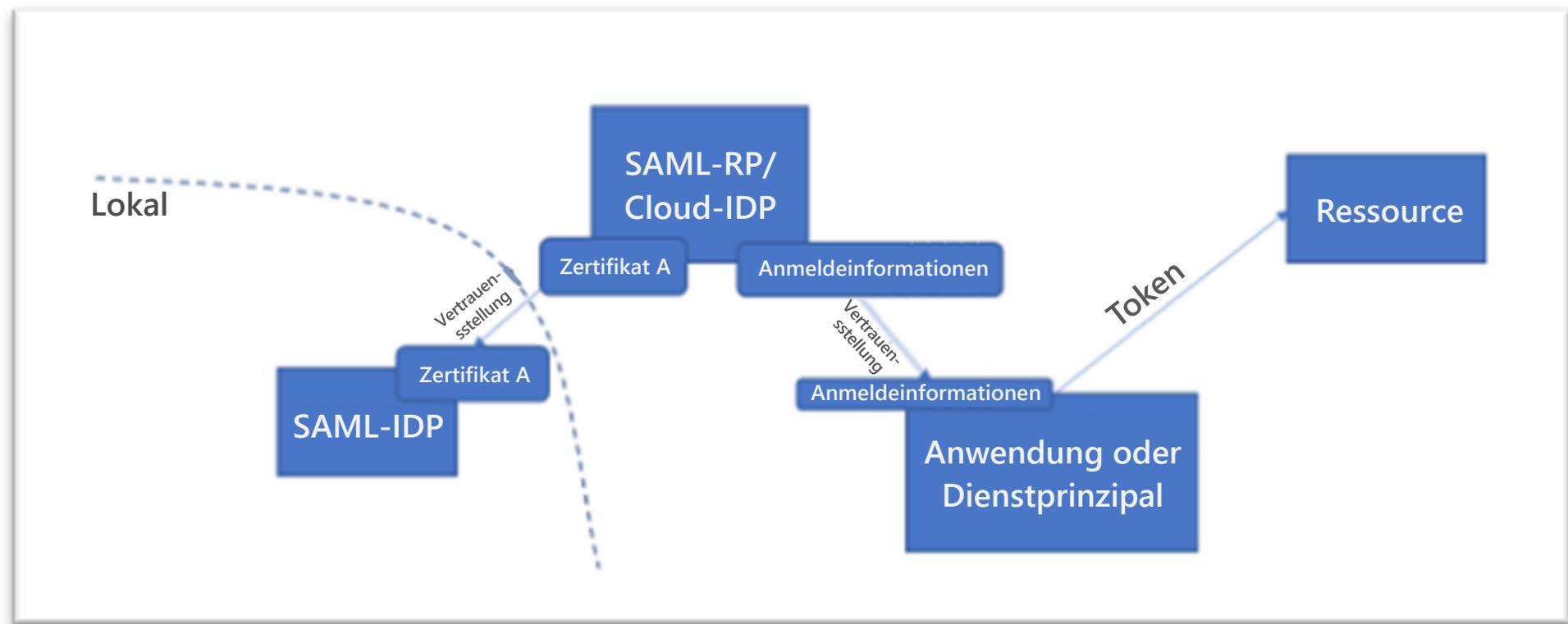
Azure AD Identity Security

18. Februar 2021

# 4 Angriffsmuster, die auf Azure Active Directory abzielen

- 1** Muster 1: Fälschen von SAML-Token mit gestohlenen Signaturinformationen
- 2** Muster 2: Unzulässige Registrierungen von SAML-Vertrauensstellungen
- 3** Muster 3: Einschleusen von Anmeldeinformationen in bestehende Anwendungen
- 4** Muster 4: Abfragen unter der "Identität" bestehender Anwendungen

# Solorigate-Videoreihe





1.

Muster

Fälschen von SAML-  
Token mit gestohlenen  
Signaturinformationen

# Die Anzeichen:

- Vom Dienstanbieter empfangene SAML-Token, deren Konfiguration vom konfigurierten Verhalten des Identitätsanbieters abweicht
- Vom Dienstanbieter empfangene SAML-Token, für die der Identitätsanbieter keine Ausstellungsprotokolle hat
- Vom Dienstanbieter empfangene SAML-Token mit MFA-Ansprüchen, aber ohne zugehörige MFA-Aktivitätsprotokolle beim Identitätsanbieter
- Empfangene SAML-Token mit IP-Adressen, Agents, Zeitfenstern oder Diensten, die anomal für die im Token dargestellte, anfordernde Identität sind
- Beweis für eine nicht autorisierte Administratoraktivität

# Die Maßnahmen:

1

Ermitteln Sie den Mechanismus hinter der Exfiltration von Zertifikaten, und schaffen Sie Abhilfe.

2

Ändern Sie alle Zertifikate zur Signierung von SAML-Token.

3

Verringern Sie – soweit möglich – die Abhängigkeit von Ihrer lokalen SAML-Vertrauensstellung.

4

Verwalten Sie Zertifikate zur Signierung von SAML-Token (SAML Token Signing Certificates, TSC) mithilfe eines HSMs.



2.

Muster

# Unzulässige Registrierungen von SAML-Vertrauensstellungen

## Die Anzeichen:

Anomale  
Administratorsitzung mit  
veränderter  
Verbundvertrauensstellung

# Die Maßnahmen:

1

Überprüfen Sie alle Verbundvertrauensstellungen auf ihre Gültigkeit.

2

Ermitteln Sie den Mechanismus hinter dem Identitätswechsel des Administratorkontos.

3

Ändern Sie die Anmeldeinformationen des Administratorkontos.



3.

Muster

Einschleusen von  
Anmeldeinformationen in  
bestehende Anwendungen

## Die Anzeichen:

- Anomale Administratorsitzung mit veränderter Verbundvertrauensstellung
- Unerwartete Dienstprinzipale, die privilegierten Rollen in Cloudumgebungen hinzugefügt wurden

# Die Maßnahmen:

1

Überprüfen Sie alle Anwendungen und Dienstprinzipale auf Aktivitäten, die auf geänderte Anmeldeinformationen hindeuten.

2

Überprüfen Sie alle Anwendungen und Dienstprinzipale auf übermäßige Berechtigungen.

3

Entfernen Sie alle inaktiven Dienstprinzipale aus Ihrer Umgebung.

4

Ändern Sie regelmäßig die Anmeldeinformationen Ihrer Anwendungen und Dienstprinzipale.



4.

Muster

Abfragen unter der "Identität"  
bestehender Anwendungen

## Die Anzeichen:

- Anomale Ressourcenanforderungen von vertrauenswürdigen Anwendungen oder Dienstprinzipalen
- Anforderungen von Dienstprinzipalen, durch die Gruppen, Nutzer, Anwendungen, Dienstprinzipale oder Vertrauensstellungen hinzugefügt oder geändert werden

# Die Maßnahmen:

1

Überprüfen Sie alle Verbundvertrauensstellungen auf ihre Gültigkeit.

2

Ermitteln Sie den Mechanismus hinter dem Identitätswechsel des Administratorkontos.

3

Ändern Sie die Anmeldeinformationen des Administratorkontos.

Solorigate-Videoreihe

# Die nächsten Schritte

- 1** Sehen Sie sich hier die Solorigate-Videoreihe an.
- 2** Bleiben Sie über Microsoft Security auf dem Laufenden: [www.microsoft.com/de-de/security/business](http://www.microsoft.com/de-de/security/business).
- 3** Lesen Sie die Blogbeiträge unter [www.microsoft.com/security/blog](http://www.microsoft.com/security/blog).

**<https://aka.ms/solorigate>**

