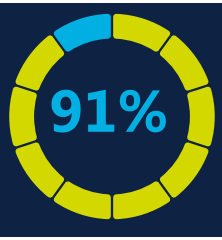
TechData A TD SYNNEX Company | Microsoft

Konkrete Maßnahmen gegen Hacking bei den Azure Services



der Angriffe starten über Pishing E-Mails

Hacker sind bei ihren Angriffen bekanntlich sehr kreativ. In den letzten Monaten wurden mehrere Cloud-Umgebungen von Hackern angegriffen, was in einer ungewöhnlich hohen Nutzungsrechnung resultierte.

Bitte beachten Sie, dass 91% der Angriffe von Phishing-E-Mails aus erfolgen, die wie unten angegeben ablaufen:

Was können Sie tun um Angriffe zu vermeiden?

- Bitte überprüfen Sie welche Nutzer, Tenants und Abonnements im Azure-Portal einem Risiko ausgesetzt sein könnten.
- Überprüfen Sie alle Azure-Ressourcen oder -Services, die in der/den letzten Woche(n) unerwarteterweise verfügbar gemacht wurden.
- Sperren Sie alle verdächtigen Azure-Ressourcen oder Azure-Abonnements.
- Als Sicherheitsmaßnahme empfehlen wir dringend, dass alle globalen Administratoren im Tenant Ihres Kunden Ihre Kennwörter unverzüglich ändern, sofern sie dies nicht bereits getan haben.
- Überprüfen Sie alle E-Mails und Telefonnummern, die zur Wiederherstellung des Kennworts von globalen Administratoren in Azure AD verwendet werden und aktualisieren Sie diese gegebenenfalls.

Nachstehend finden Sie einige konkrete Maßnahmen zur Verhinderung von Phishing.

Zugang

Grundlegende Überprüfungen für Microsoft-Umgebungen von Nutzern:

✓ Zugangsrechte der Nutzer wie folgt überprüfen

- Ist Ihre Liste der Nutzer auf dem neuesten Stand?
- Wie oft aktualisieren Sie die Zugangsrechte der Nutzer?
- Sind alle Nutzer darin geschult Phishing-Angriffe zu erkennen?
- Wie viele Nutzer haben globale Administratorrechte? (Die offizielle Empfehlung von Microsoft lautet maximal 2 bis 4 globale Administratoren einzusetzen)
- Wurden Ihre globalen Administratoren geschult?
- Welche Sicherheitskontrollen haben Sie eingerichtet? (Tools/Überwachung und Sperrung)

- Kennwortloser Zugang – Windows Hello
- MFA

✓ Geräteverwaltung

- Wie sind alle Geräte gesichert?
- Sind alle Geräte auf dem neuesten Stand?
- Pflegen Sie Sicherheitsrichtlinien?

✓ Zero Trust

- Führen Sie ein Zero Trust-Modell ein, um sich dadurch besser gegen künftige Angriffe zu schützen. Nutzen Sie das Microsoft Zero Trust Quiz und erhalten Sie Schnellstart-Empfehlungen.

Nutzen Sie das Modell der geteilten Verantwortung von Microsoft !

Tech Data
A TD SYNNEX Company

Microsoft

Welche Tools stehen für die Abwehr von Cyberattacken bereit?

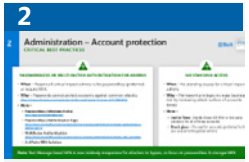
- **SecureScore**
  Bewerten Sie Ihre aktuelle Sicherheitslage. Schaffen Sie mit Hilfe von Secure Score mehr Transparenz und machen diese sichtbar, dadurch Erreichen Sie potenzielle Verbesserungen für alle Ihre Microsoft 365-Auslastungen.
- **Microsoft Defender for Office 365**
  Microsoft Defender for Office 365 schützt Ihr Unternehmen vor schadhaften Bedrohungen, die von E-Mail-Nachrichten, Links (URLs) und Tools für die Zusammenarbeit wie Teams und SharePoint ausgehen.
- **MFA**
  Die Multifaktor-Authentifizierung (MFA) fügt dem Anmeldevorgang eine zusätzliche Schutzebene hinzu. Wenn Nutzer auf Konten oder Apps zugreifen, führen sie eine zusätzliche Identitätsüberprüfung durch indem sie z. B. einen Fingerabdruck scannen oder einen per Mobiltelefon erhaltenen Code eingeben.
- **Microsoft Defender for Cloud**
  Defender for Cloud ist ein Tool für die Verwaltung der Sicherheitslage und den Schutz vor Bedrohungen. Es stärkt die Sicherheitsstruktur Ihrer Cloud-Ressourcen. Zudem schützt Defender for Cloud mit seinen integrierten Microsoft Defender-Plänen Auslastungen, die auf Azure-, Hybrid- und anderen Cloud-Plattformen ausgeführt werden.
- **Sentinel**
  Microsoft Sentinel ist eine skalierbare, Cloud-native Lösung für die Verwaltung von Sicherheitsinformationen und Ereignissen (durch SIEM) und hilft bei Orchestrierung, Automatisierung und Reaktion auf Sicherheitsvorfälle (durch SOAR). Microsoft Sentinel liefert intelligente Sicherheitsanalysen und Bedrohungsdaten für das gesamte Unternehmen und bietet eine einzige Lösung für die Erkennung von Angriffen. Die Bedrohungslage ist dadurch transparent, es hilft bei der proaktiven Suche und der Reaktion auf Bedrohungen.

Cloud-Backup

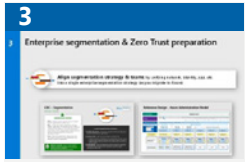
- **Azure Cost Management**
  Azure Cost Management unterstützt durch eine Warnfunktion. Warnungen werden generiert, wenn die Nutzung einen definierten Schwellenwert erreicht. Zur Erstellung von Azure-Budgets lesen Sie bitte folgenden Artikel.

Microsoft Praktiken

Implementierung von Secure Score zur Risikobereinigung



Kennwortlos oder MFA für Administratoren



Unternehmensse-gmentierung und Zero Trust-Vorbereitung

Aktivierung des Bedrohungsschutzes für Azure-Ressourcen

Anleitung zur Sicherung Ihrer DevOps Umgebung befolgen

Unser Angebot

✓ Schulungen

- Tech Data Programm: Förderung der Sicherheitssensibilisierung

✓ Vorkonfigurierte Click-to-Run-Lösungen

- Secure Score
- Cloud-Backup
- Sentinel
- Ransomware

✓ Professionelle Sicherheitsservices

- Mich schulen
- Mir helfen
- Es für mich erledigen

✓ BPA-Team

- Einen Bot gegen unsere MSFT PACs einsetzen
- Auf Kunden-Setups zugreifen, um ein MFA-Flag zu überprüfen

Zwei Maßnahmen, die Ihnen auf kurze Sicht mehr Sicherheit bieten:

1. Mehrfaktoridentifizierung für die Administrationsfunktionen verwenden
2. Schwellenwerte im Azure Cost Management festlegen

Materialien, die weitere Informationen enthalten:

PDF Nächste Generation >

Ransomware >

Schützen Sie Ihre Azure-Kunden >

Azure Cost Management >

Benötigen Sie Unterstützung bei der Implementierung?

089 4700 3020 oder csp-microsoft@techdata.com