8 häufige Fehlkonfigurationen in Microsoft Entra ID & Co.

MICROSOFT ENTRA ID CLOUD SECURITY CHECK

Cloud-Sicherheit beginnt mit den richtigen Einstellungen – doch selbst erfahrene IT-Teams übersehen oft kritische Fehlkonfigurationen.

Diese Checkliste hilft Ihnen, die häufigsten Schwachstellen in Microsoft Entra ID und Cloud-Sicherheitsstrategien zu identifizieren – bevor Angreifer sie ausnutzen.

Finden Sie heraus, ob Ihre Cloud wirklich sicher ist – oder ob versteckte Risiken Ihre IT gefährden.

ProSec
Security redefined.

ProSec
Security redefined.

Inhaltsverzeichnis

Einleitung

Wie sicher ist Ihre Microsoft Cloud wirklich?

Fehlkonfigurationen, zu weitreichende Berechtigungen oder unzureichende Zugriffskontrollen sind die häufigsten Ursachen für Sicherheitsvorfälle in der Cloud – oft ohne, dass Unternehmen es bemerken.

Unsere Cloud Security Checkliste hilft Ihnen, die größten Sicherheitsrisiken systematisch zu überprüfen. Finden Sie heraus, ob Ihre Microsoft-Cloud-Umgebung richtig abgesichert ist – oder ob es versteckte Angriffspunkte gibt, die Sie dringend beheben sollten.

Microsoft Entra ID Security Check

1. Ist die Anmeldung für globale Administratoren auf vertrauenswürdige Geräte & Standorte beschränkt?

☐ Ja ☐ Nein

Ohne Geofencing oder Geräteeinschränkungen können Angreifer sich von überall anmelden, sobald sie Zugangsdaten kompromittiert haben.

Mehr dazu in der Knowledge Base unserer Website:

Microsoft Entra Admin Center – So stellst du es sicher ein

2. Haben Sie überprüft, ob der Entra Connect Sync-Account zu viele Berechtigungen hat?

☐ Ja ☐ Nein

Entra Connect hat oft weitreichende Rechte, z. B. Passwortrücksetzungen – ein attraktives Ziel für Angreifer.

Mehr dazu in der Knowledge Base unserer Website:

Microsoft Entra Connect – Azure AD Connect vor Hackern schützen

3. Können User selbständig und ohne Einschränkungen Apps registrieren und diesen weitreichende Berechtigungen zuweisen?

☐ Ja ☐ Nein

Ohne Einschränkungen können User selbstständig Apps registrieren und diesen weitreichende Berechtigungen zuweisen, oft unbemerkt. Das ist ein potentielles Einfallstor für Angreifer.

Mehr dazu in der Knowledge Base unserer Website:

So nutzen Hacker die Azure App Registration aus

4. Ist der Zugriff auf die Azure Management API eingeschränkt?

☐ Ja ☐ Nein

Angreifer mit Zugriff auf die Azure API können Systeme manipulieren oder neue Admin-Accounts anlegen.

Mehr dazu in der Knowledge Base unserer Website:

So nutzen Hacker die Azure App Registration aus

5. Haben Sie sichergestellt, dass Admin-Konten keine „Break Glass"-Accounts ohne MFA sind?

☐ Ja ☐ Nein

Notfall-Admin-Konten sollten existieren, aber wenn sie schlecht gesichert sind, könnten Angreifer sie ausnutzen, um MFA zu umgehen.

Mehr dazu in der Knowledge Base unserer Website:

Microsoft Entra Admin Center – So stellst du es sicher ein

Allgemeiner Cloud Security Check

1. Nutzen Sie eine zentrale Übersicht über alle Benutzer & Berechtigungen in der Cloud?

☐ Ja ☐ Nein

Ohne regelmäßige Überprüfung und Bereinigung entstehen oft „Zombie-Accounts“ mit überflüssigen Rechten.

Mehr dazu in der Knowledge Base unserer Website:
Microsoft Entra Admin Center – So stellst du es sicher ein

2. Sind Schatten-IT und nicht autorisierte Cloud-Dienste ein Problem?

☐ Ja ☐ Nein

Mitarbeitende nutzen oft unsichere Alternativen zu freigegebenen Cloud-Diensten, was Sicherheitsrisiken erhöht.

Mehr dazu in der Knowledge Base unserer Website:
So nutzen Hacker die Azure App Registration aus

3. Wird das Anmeldeverhalten der User regelmäßig überprüft?

☐ Ja ☐ Nein

Ungewöhnliche Logins aus fremden Ländern oder mehrfach fehlgeschlagene Anmeldeversuche können auf einen laufenden Angriff hindeuten.

Mehr dazu in der Knowledge Base unserer Website:
Microsoft Entra Admin Center – So stellst du es sicher ein

Jede Cloud-Umgebung ist einzigartig. Wenn Sie anhand dieser Checkliste Unsicherheiten entdeckt haben oder sicherstellen wollen, dass andere Bereiche Ihrer Cloud ebenfalls richtig abgesichert sind, nutzen Sie das ProSec Cloud Security Audit für eine umfassende Prüfung Ihrer Einstellungen und Sicherheitsmaßnahmen!

Wo liegen die Stolperfallen bei den Einstellungen von Microsoft M365 und Azure?

Vereinbaren Sie jetzt ihre Erstberatung - kostenfrei und unverbindlich

Beratungstermin sichern

ProSec
Security redefined.

WHO WE ARE

2016
gegründet

50+
Team-Mitglieder

1000+
durchgeführte Assessments

100%
Systemübernahmen

UNSERE MISSION

Menschenleben retten und schützen, indem wir die digitale Infrastruktur von Unternehmen nachhaltig sicher machen.

UNSERE VISION

Wir wollen IT Security viral gehen lassen.

HOW WE SUPPORT YOUR INFORMATION SECURITY

Penetration Testing IT Security Consulting Ethical Hacker Courses

„IT Security aus der Eifel
für Kunden weltweit."