



Identitätssicherheit im Fokus: Cyber-Angriffe erkennen und verhindern

22. Oktober 2024



Christoph Pontau
Senior Solutions Engineer



Agenda

- Warum ist es so schwierig, Identitätssicherheit zu erreichen?
- Vorstellung Identity Security Insights
- Use Case - Verwaiste Konten

Warum ist es so schwierig, Identitätssicherheit zu erreichen?

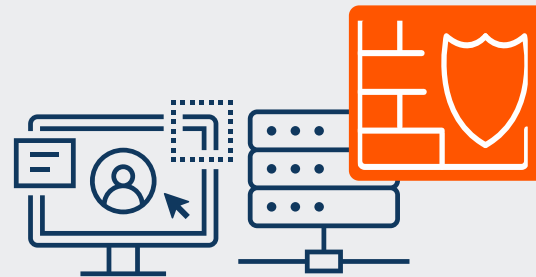


Evolution: Identity-First Security

Perimeter Security



Endpoint Security



Identity Security



“Die Dezentralisierung von Computerressourcen, -kanälen, -einheiten und -geräten führt dazu, dass herkömmliche Sicherheitsstrategien und -tools, die auf dem Perimeter basieren, nicht mehr ausreichen.

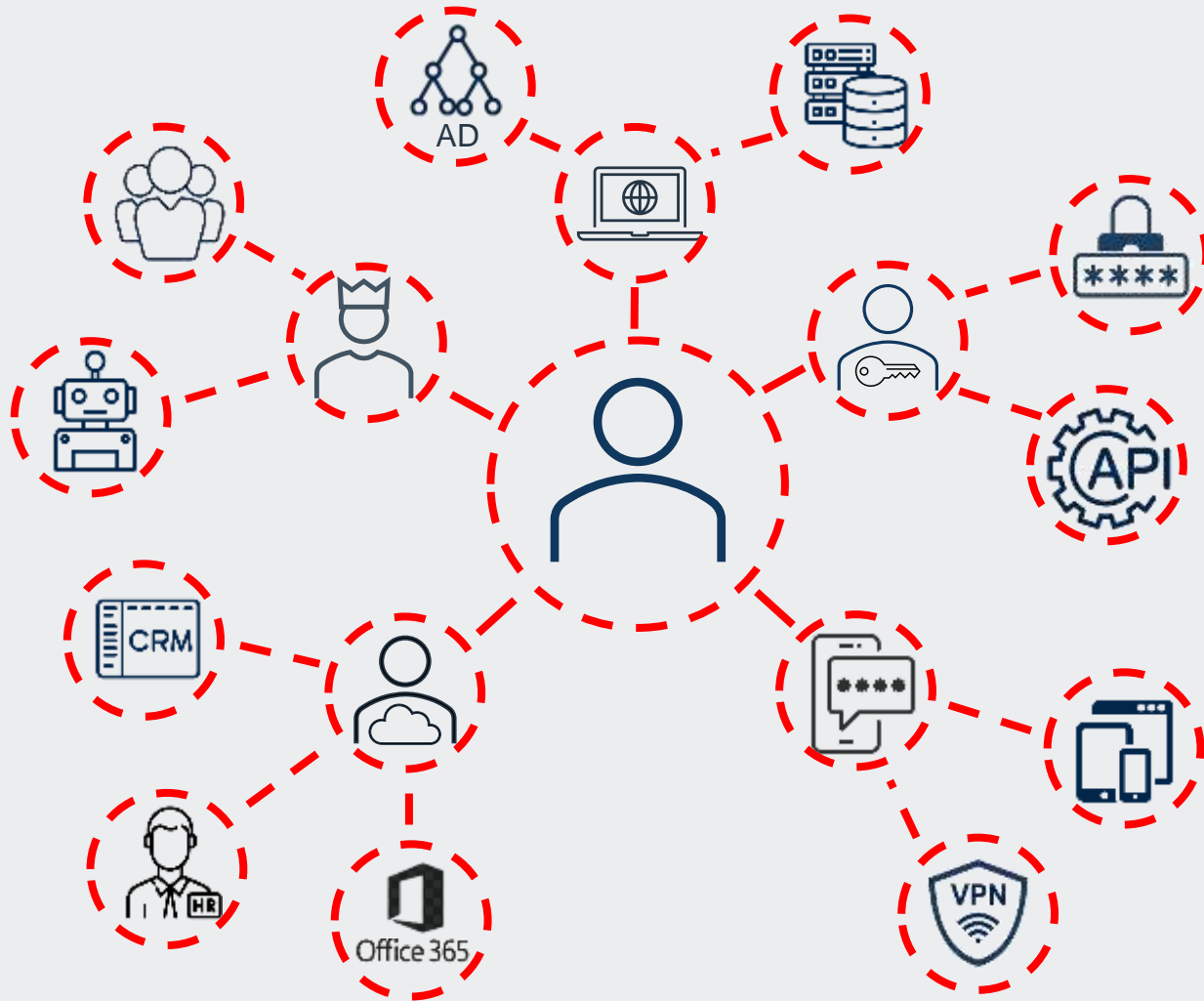
Die Verantwortlichen für Sicherheit und Risikomanagement müssen die Identität in den Mittelpunkt der Cybersicherheitsstrategie stellen und in kontinuierliche, kontextbezogene Kontrollen investieren.”

Gartner. *Identity-First Security Maximizes Cybersecurity Effectiveness*, Dez. 2022

Was ist eine Identität?

Die Gesamtheit der physischen und verhaltensbezogenen Merkmale, durch die eine Person eindeutig erkennbar ist.
Hinweis: Dies umfasst auch sog. Non-Person Entities (NPEs).

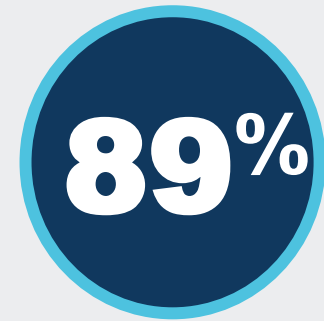
Identitäten in der IT-Umgebung



- Der Betrieb von Unternehmen hängt zunehmend von **SaaS, IaaS und anderen Cloud-Diensten** ab.
- Der Zugriff auf diese Dienste und das übrige Ökosystem hängt von **Identitäten** ab.
- Mehr als 70 % aller Sicherheitsverstöße sind auf eine **kompromittierte Identität** zurückzuführen.
- Unternehmen verlagern ihren Sicherheitsschwerpunkt auf einen besseren Schutz von **Identität und Zugriff**.

Anstieg von Jahr zu Jahr: Cloud-Nutzung, Identitäten und Schwachstellen

- **Mehr Cloud, Multi-Cloud und Bring Your Own Cloud (BYOC)**
79 % haben mehr als einen Cloud-Anbieter⁴
- **Komplexe Multi-Cloud-Berechtigungen verwalten**
40.000+ Arten von Cloud-Berechtigungen verwalten¹
- **Mehr Schwachstellen**
540 % Anstieg der Cloud-Sicherheitslücken in den letzten 6 Jahren²
- **Mehr maschinelle Identitäten**
10x mehr Workload-Identitäten als “echte” Nutzer¹
- **Mehr Identitäten**
52 % der Unternehmen verwalten mehr als 10.000 Identitäten³



**der Unternehmen
waren in den
letzten zwei Jahren
von einem
identitätsbasierten
Angriff betroffen.³**

1. 2023 State of Cloud Permissions Risks Report, Microsoft Security
2. IBM Security, 2022 IBM Security X-Force Cloud Threat Landscape Report
3. Dimensional Research – Identities and Security in 2022
4. Thales 2023 CLOUD SECURITY STUDY

Aufspüren des kompromittierten Kontos

„Da es so viele Möglichkeiten gibt, Unternehmensdaten zu kompromittieren und zu stehlen, ist die bevorzugte Taktik, sich als legitimer Benutzer auszugeben, um nicht entdeckt zu werden.“



DIE 5 GRUNDLAGEN



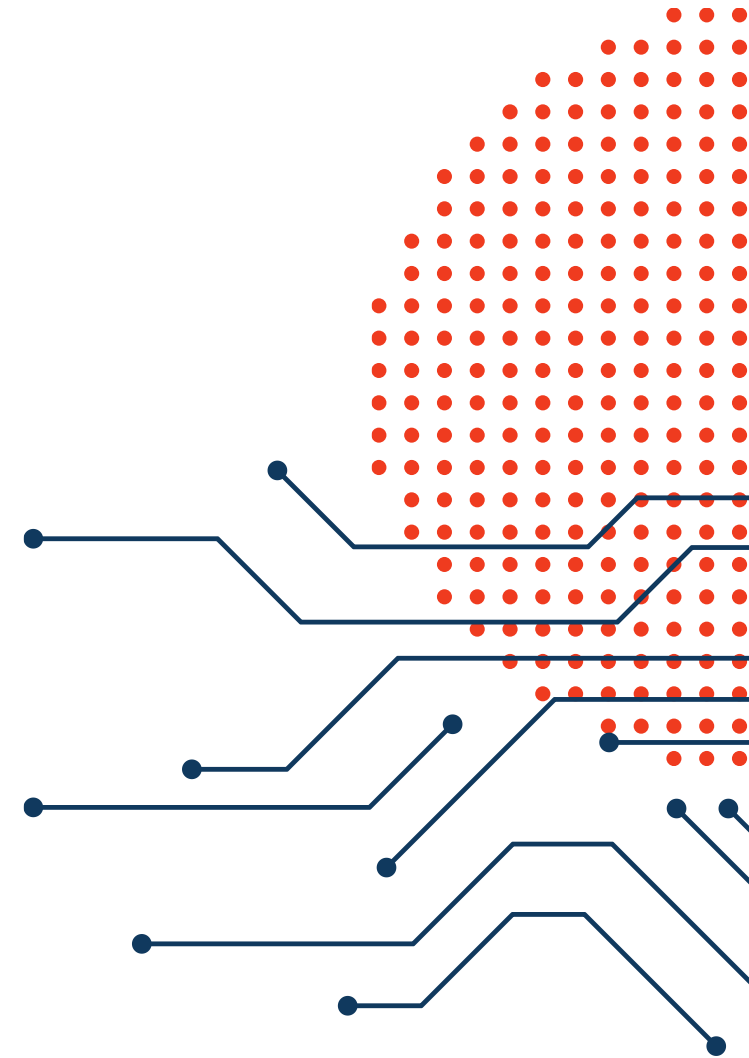
Protecting Your Paths to Privilege

- 1** **Ganzheitliche Visibilität** für Identitäten, Konten, Sitzungen und verknüpfte Privilegien über mehrere IT- und OT-Landschaften hinweg
- 2** **Aufdeckung aller riskanten Zugriffspfade** durch Mapping der Schwachstellen von Identitätssilos sowie Priorisierung des Risikos/Werts jedes privilegierten Zugriffspfads
- 3** **Begrenzung der Angriffsgefahr** durch Umstellung auf Least Privilege und situativ angemessenen Zugriff mit personalisierter Autorisierung für Nutzer/Sitzung/Anwendung/Gerät/Endpunkt
- 4** **Sofortiges Wissen, wenn sich Ihre Umgebung verändert hat** oder der Zugriff manipuliert wird, durch Erkennung identitätsgesteuerter Angriffe und Statusüberwachung der privilegierten Zugriffswege
- 5** **Schnelle Reaktion auf Identitätsverletzungen** und Stärkung der Widerstandsfähigkeit durch das Verhindern von Lateral Movement mittels Umstellung auf autonomes Erkennen/Reagieren/Lernen mit KI



Vorstellung Identity Security Insights

Unübertroffene Sichtbarkeit von
Identitäten, Konten und privilegiertem Zugriff



BeyondTrust ist einzigartig positioniert, um Ihre Paths to Privilege zu schützen



**Ganzheitliche
Visibilität**

Aufdeckung
Ihrer Paths to
Privilege



**Einfaches
Management**

Durchsetzung von
Least Privilege und
Erzielung von
Effizienzgewinnen



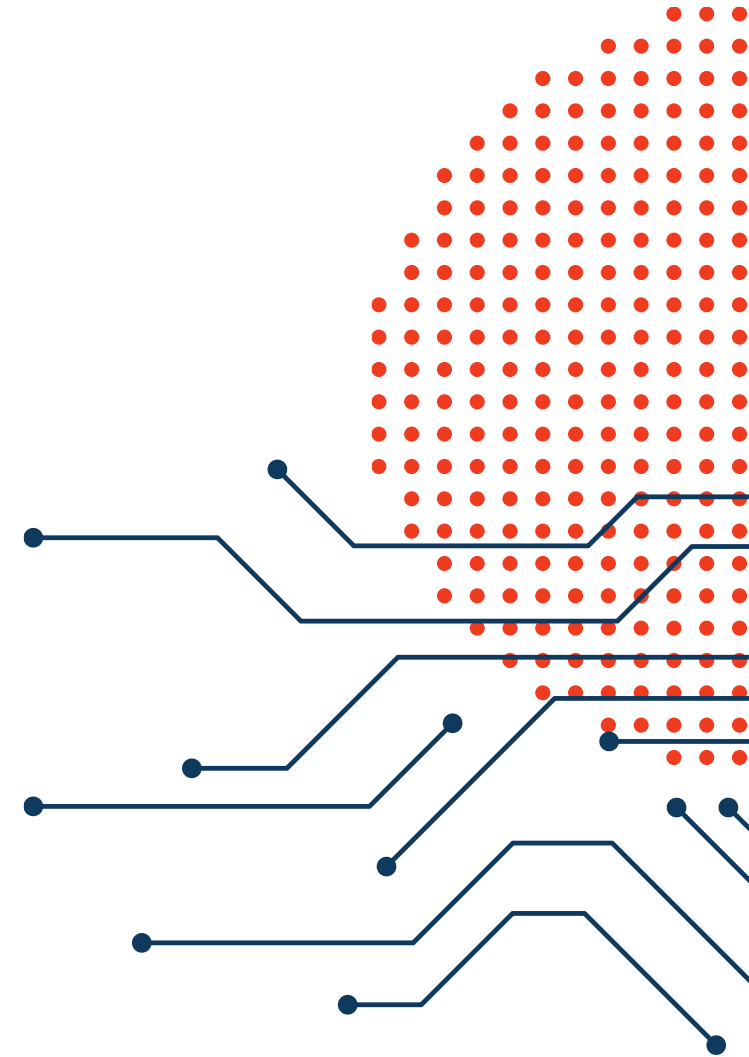
**Intelligenter
Schutz**

Kontinuierliche
Verbesserung durch
KI- und ML-
Erkenntnisse



Use Cases

Verwaaste Konten



Identity Security Insights in Aktion



Unübertroffene Sichtbarkeit
von Identitäten, Konten und privilegiertem Zugriff

Use Case: Verwaiste Konten



Verwaiste Konten

Was ist damit gemeint?

Inaktive und nicht gepflegte Konten stellen ein **erhebliches Sicherheitsrisiko** für Nutzer und Unternehmen dar. Cyberkriminelle nutzen gestohlene Infos von vergessenen oder nicht gepflegten Konten, um **aktive Konten auszunutzen**.

Ist dies ein reales Problem?

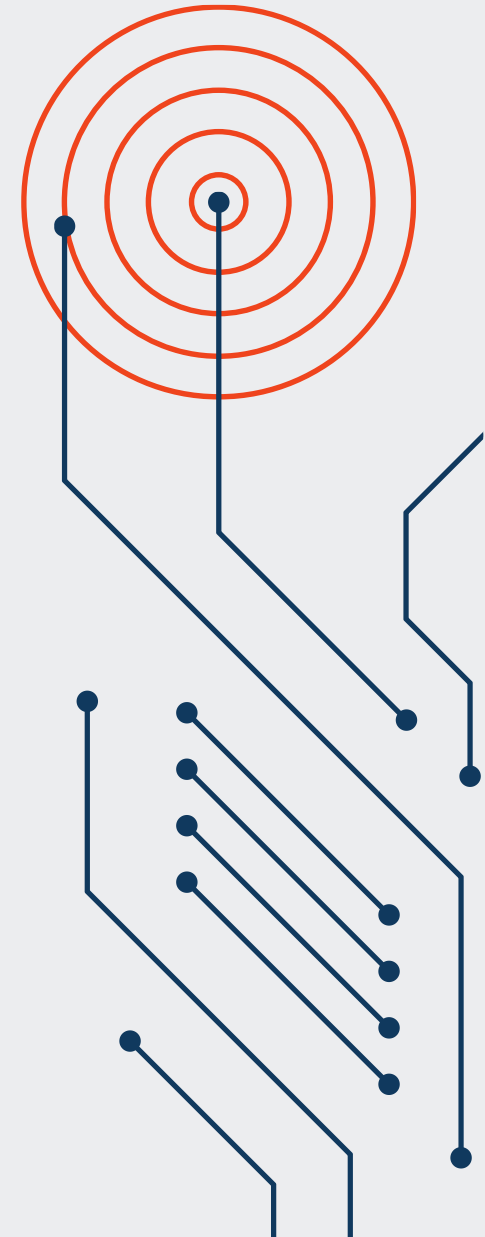
Ja, Sicherheitsforscher haben beobachtet, dass es **APT29 (Cozy Bear)** auf **inaktive Microsoft-Konten** abgesehen hat, um sich als erstes für die Multi-Faktor-Authentifizierung (MFA) anzumelden.

Quellen:

<https://www.csoonline.com/article/575347/inactive-accounts-pose-significant-account-takeover-security-risks.html>

<https://securityboulevard.com/2022/09/threat-actors-exploiting-dormant-accounts-to-bypass-mfa-what-you-need-to-know/>

<https://attack.mitre.org/groups/G0016/>



Verwaaste Konten

Menu CPlab

Apps Help Profile

Home > Recommendations > Recommendation Details

Recommendation Details

Dormant Admin Account With Stale Password Hide Description ^

●●●○ High Importance | 4 Entities

Recommendation: A privileged account has not logged in over three months and has not rotated its password in over a year.

Concern: Privileged users are often targeted by attackers. Unrotated passwords increase the likeliness of compromise.

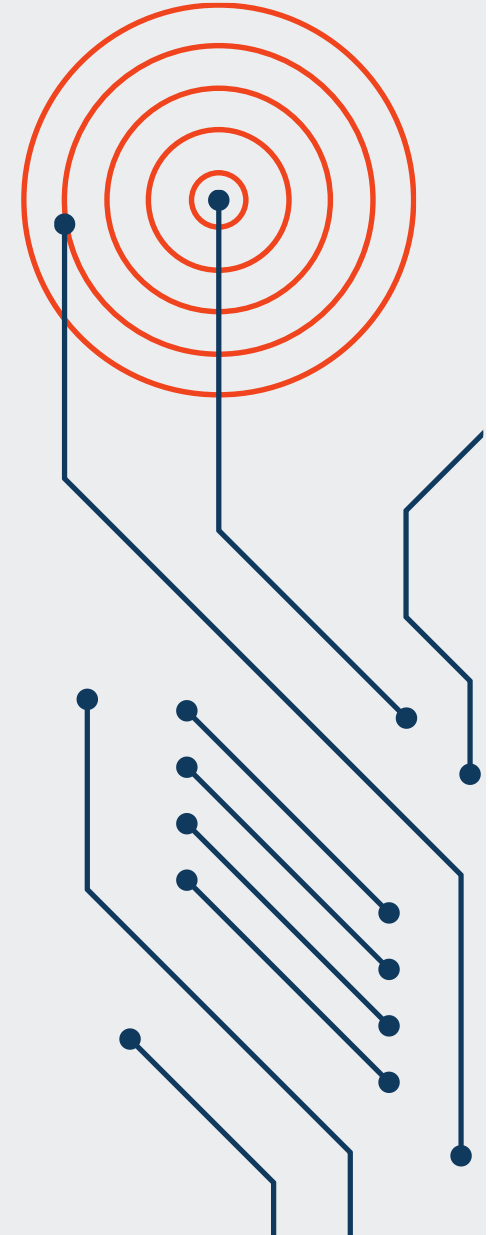
How to address: Use a credential management solution, like Password Safe, to manage and rotate the passwords of privileged accounts.

Entity Name	Entity Type	Source	Status	First Recommended	Actions
<input type="checkbox"/> BT_PASSWORDSAFE@CPLABAD.LAB	Account	5-1-5-21-2252953384-1966636586-3303455154	New	06 Mar 2024 01:23 PM	Quick View
<input type="checkbox"/> ADMINISTRATOR@CPLABAD.LAB	Account	5-1-5-21-2252953384-1966636586-3303455154	New	06 Mar 2024 01:23 PM	Quick View
<input type="checkbox"/> DIRECTORYBROWSER@CPLABAD.LAB	Account	5-1-5-21-2252953384-1966636586-3303455154	New	06 Mar 2024 01:23 PM	Quick View
<input type="checkbox"/> INTERNAL_ADM@CPLABAD.LAB	Account	5-1-5-21-2252953384-1966636586-3303455154	New	06 Mar 2024 01:23 PM	Quick View

Microsoft Midnight Blizzard Breach

Aktuelles Beispiel

- Password-Spray-Angriff
- Standard Kennwörter werden genutzt für Login-Versuch
- Verwaiste Konten sind anfällig
- Konten ohne MFA sind anfällig



Password Spray Attack



Menu



CPLab



Apps



Help



Profile

[Home](#) > [Detections](#) > Detection Details

Detection Details



Entra Password Spray Attack

Hide Description

●●●○ High Severity | 0 Entities

Detection:

Microsoft Entra ID Protection detected a possible password spray attack. A password spray attack is an attempt to test passwords against several accounts over a short period of time, followed by a successful login.

Concern:

Password spray attacks can lead to several adverse outcomes, including credential compromise and account lockout.

How to address:

Investigate the accounts targeted in the password spray attack to determine if the attack was successful.

BeyondTrust Plattform



Kostenfreies Identity Security Assessment

Ohne Verpflichtungen

- ✓ 30 min einfache Einrichtung
- ✓ Visibilität innerhalb 24 Std.
- ✓ **Bonus:** 30 Tage Zugriff, Threat Monitoring & Detection

Jetzt anmelden: beyondtrust.com/assessment

Vielen Dank

Bitte kontaktieren Sie uns,
falls Sie weitere Fragen haben:
kontakt@beyondtrust.com

Besuchen Sie uns:

Halle 9
Stand 326

beyondtrust.com