amexus® Informationstechnik

ADN®

Microsoft

26.02.2026/Köln

Cloud. Daten. KI. –

Die digitale Zukunft mit Microsoft im deutschen Mittelstand

www.amexus.com

Sichere Cloud für den Mittelstand

Governance, Identitäten und Compliance richtig aufstellen

Tobias Elbert

Geschäftsführer | amexus

telbert@amexus.com

Agenda

- Aktuelle Bedrohungslage und Herausforderungen
- Warum Cloud-Sicherheit Chefsache ist
- 3 Strategische Hebel
- Governance- und Policy-Framework
- Use Case – Vom Wildwuchs zur sicheren Cloud-Governance
- Management-Empfehlungen
- Abschluss

Aktuelle Bedrohungslage und Herausforderungen

tagesschau.de

Bundesbank beklagt 5.000 Cyberangriffe pro Minute

Cyberkriminalität Bundesbank beklagt 5.000 Cyberangriffe pro Minute ... Hochgerechnet auf ein Jahr sind es mehr als zwei Milliarden Attacken auf...

vor 2 Wochen

Frankfurter Rundschau

„50 Euro oder die Daten eurer Kinder sind im Darknet“: Hacker erpressen Eltern

Nach Cyberangriff fordern Hacker 50 Euro von Eltern. Der Fall aus Belgien zeigt: Deutsche Schulen sind massiv angreifbar.

vor 1 Tag

Aachener Zeitung

Steuerbescheide verzögern sich – das müssen Bürger jetzt wissen

Cyberangriff auf Heinsberg: Massive technische Probleme beeinträchtigen Steuerbescheide und Abrechnungen. Erfahren Sie, welche Fristen sich...

vor 4 Stunden

SWR

Nach Cyberattacke erholt sich Mineralwasser-Abfüller langsam

Der Betrieb beim Mineralwasser-Abfüller Romina in Reutlingen-Rommelsbach war durch eine Cyberattacke tagelang komplett lahmgelegt.

vor 2 Tagen

Golem.de

Cyberangriffe auf Europa: Russische Hacker attackieren Office-Nutzer

Die dem russischen Militär zugeordnete Hackergruppe APT28 hat es auf Nutzer von Microsoft Office abgesehen und schleust durch eine Lücke...

vor 3 Tagen

tagesschau.de

Cyberangriff auf Flughafenprogramm - auch BER betroffen

Cyberangriff auf Dienstleister. Laut den Flughäfen BER und London Heathrow ist die Firma Collins Aerospace betroffen. Das Unternehmen bestätigte...

20.09.2025

Bitkom-Studie 2025: 87 % der Unternehmen in Deutschland wurden in den letzten 12 Monaten Opfer von Cyberangriffen. Der wirtschaftliche Schaden beläuft sich auf 289,2 Milliarden Euro. (58% des Bundeshaush.)

Herausforderungen

Verantwortung und Haftung

Geschäftskontinuität und Resilienz

Vertrauen, Reputation und Marke

Compliance und Erwartungshaltung

Führung, Kultur und Awareness

Wettbewerbsfähigkeit und Zukunftssicherheit

Warum Cloud-Sicherheit Chefsache ist

amexus® Informationstechnik

Die meisten Unternehmen glauben, sie haben ein IT-Thema.

–

In Wahrheit haben sie ein Führungs-Thema.

Die Rolle der Geschäftsführung

Rechtliche Verantwortung:

- die Geschäftsführung ist für angemessene Schutzmaßnahmen verantwortlich (Organisationspflicht)
- DSGVO, BSI-Gesetz, GoBD, NIS-2 – auch KMUs sind betroffen

Haftung und Reputationsschäden:

- Datenverlust oder Betriebsstillstand schaden der „Marke“ und dem Vertrauen

Geteilte Verantwortung

Microsoft:

- Infrastruktur
- Plattform
- Rechenzentren
- Verfügbarkeit

Unternehmen:

- Identitäten
- Daten
- Konfigurationen
- Compliance

Microsoft 365

Azure

3 Strategische Hebel

3 Strategische Hebel

1. Identitäten

Wer darf was?

2. Governance

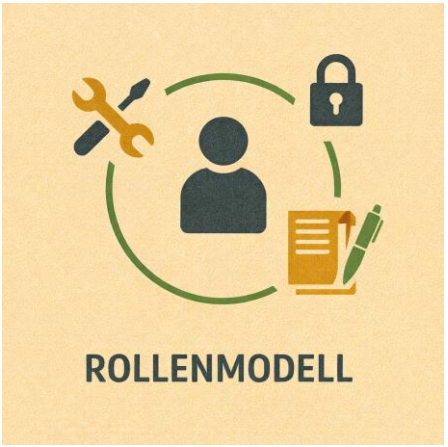
Welche Regeln gelten?

Compliance

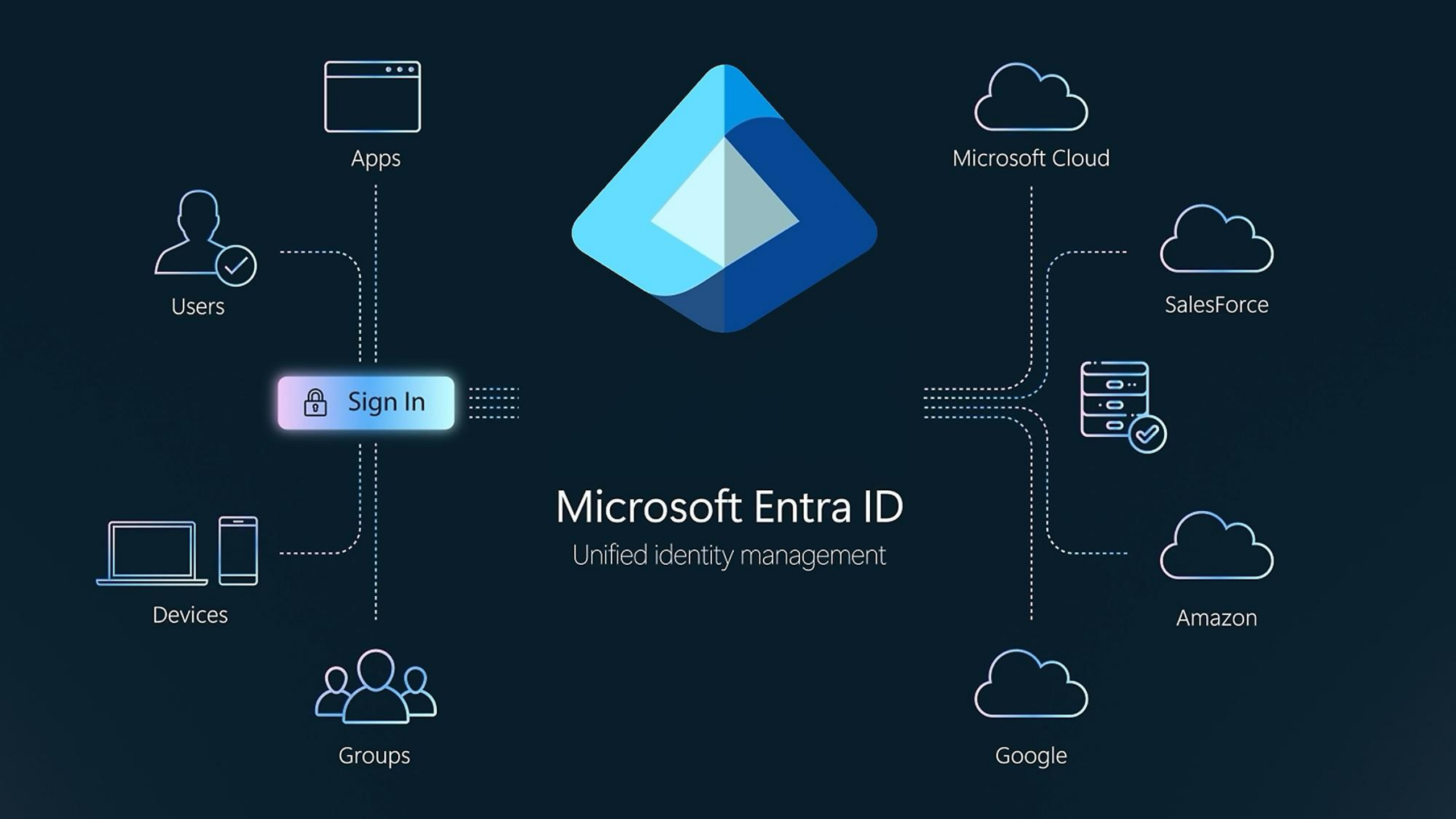
Können wir das beweisen?

> „Cloud-Sicherheit entsteht nicht durch Technologie, sondern durch Steuerung: Identitäten kontrollieren, Regeln durchsetzen, Nachweise liefern."

1. Identitäten



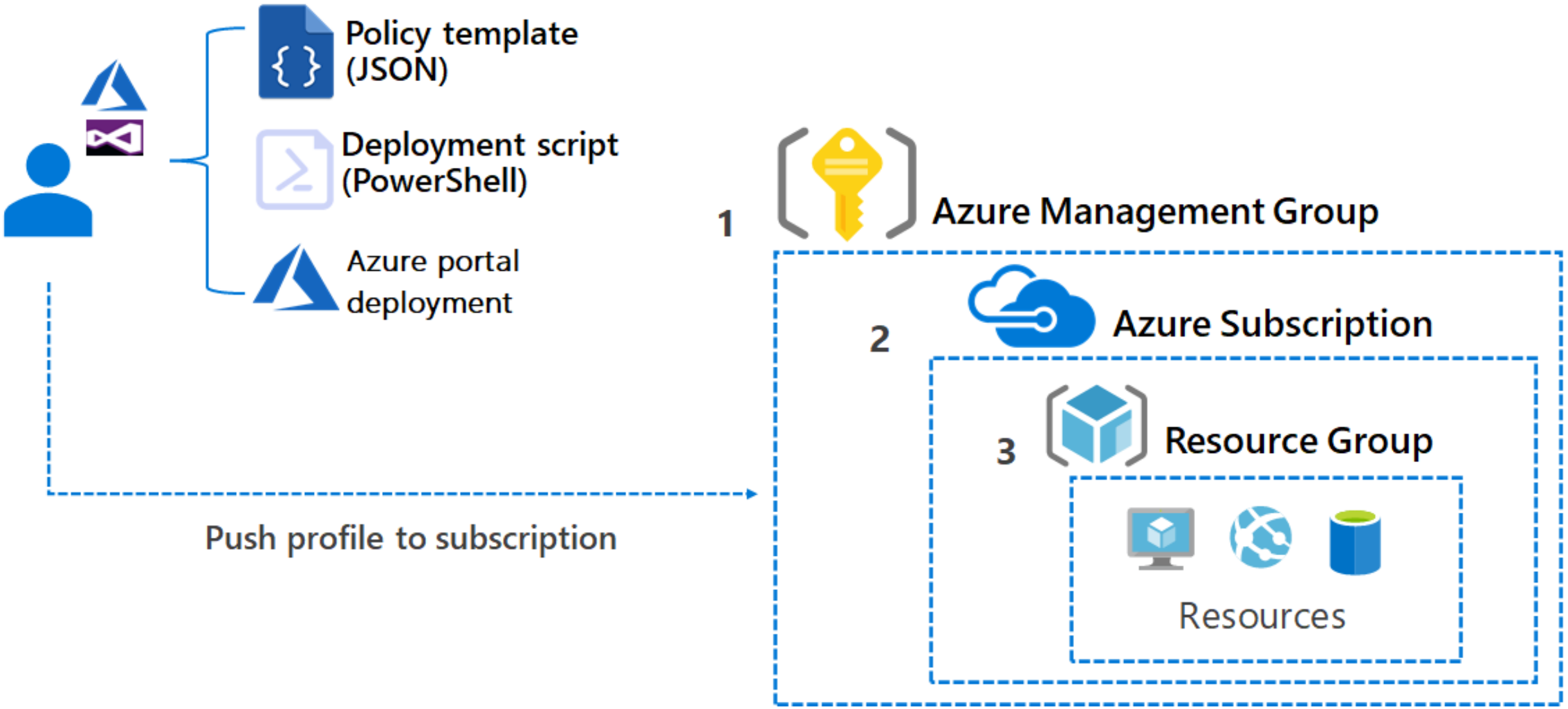
„Zero Trust als Leitprinzip."


Apps
Microsoft Cloud
Users
SalesForce
Sign In
Microsoft Entra ID
Unified identity management
Devices
Amazon
Groups
Google

2. Governance

„Vom Dokument zur technischen Realität."

Azure Policy

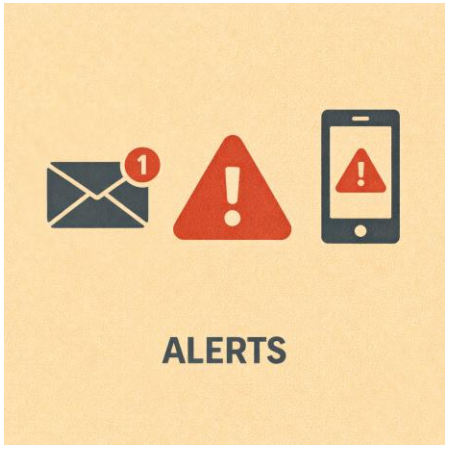


3. Compliance

Regulatorische Treiber:

- DSGVO
  - Schutz personenbezogener Daten
  - Zugriffskontrolle
  - Protokollierung
  - Löschkonzepte
- NIS-2
  - Risikomanagement
  - Incident Meldung
  - Zugriffskontrolle
  - Lieferketten-Absicherung
- DORA
  - Operative Resilienz
  - Protokollierung
  - Zugriffskontrolle
  - Incident Management

3. Compliance

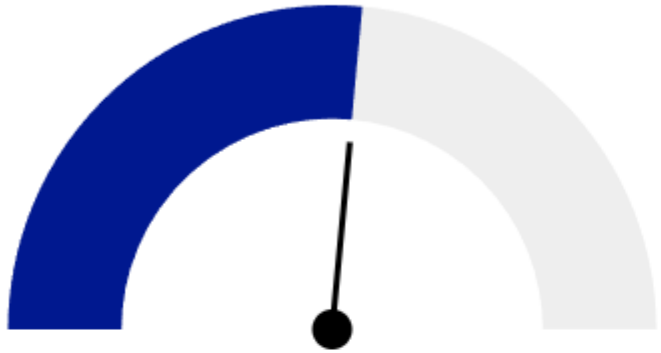


„Nachweisbarkeit statt Bauchgefühl."

Date (UTC)	IP Address	User	Record Type	Activity
Feb 20, 2026 1:28 PM	87.122.29.196	telbert@amexus.com	ExchangeItemGroup	Deleted messages from De...
Feb 20, 2026 1:27 PM	87.122.29.196	telbert@amexus.com	ExchangeItem	Created mailbox item
Feb 20, 2026 1:27 PM	87.122.29.196	telbert@amexus.com	SharePointFileOperation	Accessed file
Feb 20, 2026 12:49 PM	87.122.29.196	telbert@amexus.com	ExchangeItemAggregated	Accessed mailbox items
Feb 20, 2026 12:41 PM	87.122.29.196	telbert@amexus.com	AzureActiveDirectoryStsLo...	User logged in
Feb 20, 2026 12:41 PM	87.122.29.196	telbert@amexus.com	SharePoint	Viewed page
Feb 20, 2026 12:40 PM	87.122.29.196	telbert@amexus.com	ExchangeItemAggregated	Accessed mailbox items
Feb 20, 2026 12:39 PM	87.122.29.196	telbert@amexus.com	ExchangeItem	Sent message
Feb 20, 2026 12:28 PM	87.122.29.196	telbert@amexus.com	SharePointFileOperation	Accessed file

Overall compliance score

Your compliance score: 53%



13689.24/25450 points achieved

Your points achieved
1,109.24/ 12,777

Microsoft managed points achieved
12,580/ 12,673

Compliance score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Learn how your Compliance score is calculated

Key improvement actions

Not completed	Completed	Out of scope
878	**39**	**0**

Improvement action	Impact	Test status	Group	Action type
Set User Account Control (UAC) to automatically ...	+27 points	Failed high risk	Default Group	Technical
Disable the local storage of passwords and crede...	+27 points	Failed high risk	Default Group	Technical
Disable 'Allow Basic authentication' for WinRM Cl...	+27 points	Failed high risk	Default Group	Technical
Require additional authentication at startup	+27 points	Failed high risk	Default Group	Technical
Use advanced protection against ransomware	+27 points	Failed high risk	Default Group	Technical
Disable 'Autoplay' for all drives	+27 points	Failed high risk	Default Group	Technical
Block all Office applications from creating child p...	+27 points	Failed high risk	Default Group	Technical
Protect against potentially unwanted applications	+27 points	Failed high risk	Default Group	Technical
Control data by restricting access to cloud service...	+27 points	Failed high risk	Default Group	Technical
Block executable files from running unless they m...	+27 points	Failed high risk	Default Group	Technical

View all improvement actions

Governance- und Policy-Framework


Governance
Was ist technisch erlaubt?
Microsoft
Identität
Wer darf was?
Compliance
Können wir es beweisen?

Use Case – Vom Wildwuchs zur sichereren Cloud-Governance

Unternehmen: GrauBau

- 150 Mitarbeitende (3 Admins)
- 3 Standorte
- M365 seit 5 Jahren im Einsatz
- Erste Azure-Ressourcen (Backup, VMs, Webanwendungen)

- 6 Global Admins
- Kein PIM
- MFA nur für Admins
- Azure-Subscriptions historisch gewachsen
- Kein Reporting an die Geschäftsführung
- DSGVO-Dokumentation vorhanden, aber nicht technisch umgesetzt

Das Problem

Die Geschäftsführung stellt 3 Fragen:

1. Wer hat Zugriff auf unsere kritischen Daten?
2. Können wir das im Audit belegen?
3. Sind wir NIS-2-konform?

Die IT kann keine belastbare Antwort geben.

Nur Einschätzungen.

1. Identitäten absichern

Maßnahmen:

- MFA verpflichtend für ALLE
- PIM einführen
- 6 permanente Global Admins -> 2
- Rollenmodell definieren
- Conditional Access Policies einführen

Ergebnis:

- Massive Senkung des Risikos

2. Governance strukturieren

Maßnahmen:

- Management Groups einführen
- Trennung: PROD / TEST / DEV
- Azure Policy Grundlage definieren

Ergebnis:

- Nur noch EU-Regionen erlaubt
- Verschlüsselung verpflichtend
- Keine ungewollten Ressourcen (Schatten-IT) mehr
- Audit-Report in 15 Minuten erzeugbar

3. Compliance messbar machen

Umsetzung:

- Sensitivity Labels einführen
- DLP-Regeln aktivieren
- Aufbewahrungsrichtlinien implementieren
- Audit Log aktivieren

Effekt:

- DSGVO nicht nur dokumentiert, sondern technisch umgesetzt
- Nachweisbarkeit gegenüber Großkunden
- NIS-2-Vorbereitung strukturiert gestartet

Ergebnis nach 6 Monaten

- 2 permanente Global Admins
- 100% MFA
- 70% weniger privilegierte Accounts
- Secure Score +30%
- Audit ohne kritische Funde
- Management bekommt monatliches Reporting

„Die Cloud war vorher produktiv.
Jetzt ist sie steuerbar.“

Management-Empfehlungen

Management-Empfehlungen

Sicherheit als KPI etablieren

Rollen klar definieren

Monatliches Security-Review

So wird Cloud-Sicherheit steuerbar.

amexus®
Informationstechnik

Abschluss

Microsoft gibt uns die Technologie.

-

Sicherheit entsteht durch Struktur.

Ihr nächster Schritt:

amexus® Informationstechnik

Lassen Sie uns Ihre Cloud gemeinsam sicherer machen.

www.amexus.com

Danke furs Zuhören!

Fragen? Wünsche? Anregungen?