Pause

Microsoft Solutions Partner
Modernes Arbeiten

amexus® Informationstechnik

Herzlich Willkommen

Sicherheit im Fokus

-

Best Practices für M365 Security & Compliance

Wer bin ich?

Dirk Schönfeld

Head of Consulting

amexus Informationstechnik GmbH & Co. KG
Von-Braun-Str. 34
48683 Ahaus

+49 2561 /9303-727

dschoenfeld@amexus.com

"Stillstand bedeutet Rückschritt!"

Was erwartet Sie in den nächsten Minuten?

Teil 1: Bedrohungslandschaft und Herausforderungen

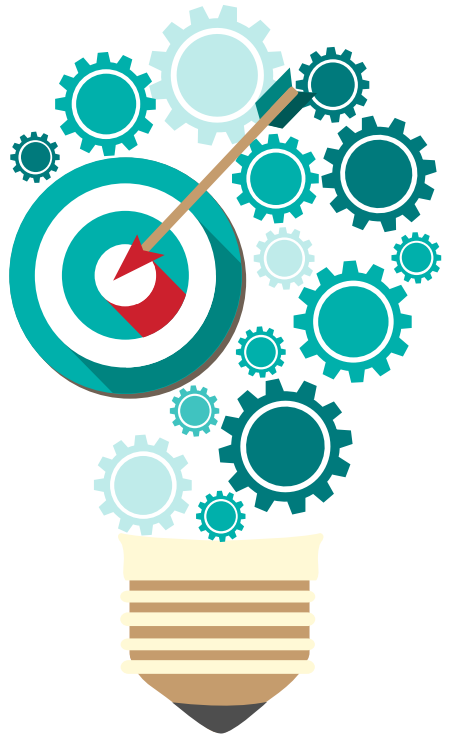
- Aktuelle Bedrohungen
- Herausforderungen für Unternehmen

Teil 2: Best Practices für M365 Security

- Sechs bewährte Methoden zum Schutz Ihrer M365-Umgebung

Teil 3: Best Practices Datenschutz & Compliance

- Drei zentrale Strategien für den datenschutzkonformen Umgang mit Informationen



amexus®
Informationstechnik

Teil1

Bedrohungslandschaft & Herausforderungen

shz.de

Cyberattacke auf Stadtwerke Neumünster: Hacker bereiteten Angriff ein Jahr lang vor

Cyberangriff auf die Stadtwerke Neumünster: Wie eine schnelle Reaktion und eine IT-Umstrukturierung 2023 einen Ransomware-Angriff verhinderten.

vor 24 Stunden

it- it-daily

Gezielte Cyberangriffe: Bedrohungsakteure missbrauchen Microsoft 365

Gezielte Cyberangriffe: Bedrohungsakteure missbrauchen Microsoft 365 ... Sophos X-Ops hat eine raffinierte Angriffskampagne entdeckt, bei der Cyberkriminelle...

vor 1 Monat

it- it-daily

31 Prozent der Cyberangriffe erfolgen über kompromittierte Accounts

Cyberkriminelle setzen verstärkt auf gestohlene, aber gültige Account-Daten, um ihre Angriffe zu starten.

vor 2 Stunden

HNA

„Mensch ist größte Schwachstelle“: Hackerangriffe im Kreis Kassel steigen

Lahmgelegte IT-Anlagen, Erpressung und Datenklau: Cyberangriffe auf Kommunen kommen immer häufiger vor. Auch der Kreis Kassel ist betroffen.

vor 6 Stunden

heise online

Vertrauensdiensteanbieter D-Trust informiert über Datenschutzvorfall

Vertrauensdiensteanbieter D-Trust informiert über Datenschutzvorfall. Bei D-Trust kam es zu einem Datenschutzvorfall. Betroffen ist das...

17.01.2025

Microsoft

Cyberangriffe verdoppeln sich nahezu von Jahr zu Jahr

Cyberangriffe verdoppeln sich nahezu von Jahr zu Jahr ... Die Zahl der Cyberangriffe auf Microsoft hat sich im vergangenen Jahr fast verdoppelt und unterstreicht...

15.10.2024

Angriffsvektoren – Einstiegspunkte zu einem System

E-Mail

Phishing

Ransomware

Kompromittierte Zugangsdaten

Schwache Passwörter

Böswillige Mitarbeiter

Geräte

Falsche Konfiguration

Unzureichende Verschlüsselung

Softwareschwachstellen

Herausforderungen für Unternehmen

Fehlende Sicherheitsstrategie

Hohe Anforderungen an Datenschutz (z. B. DSGVO)

Fehlendes spezialisiertes Know-how

Begrenzte personelle & finanzielle Ressourcen

Komplexität der Cloud-Sicherheit

Mangel an Sicherheitsbewusstsein bei Mitarbeitenden

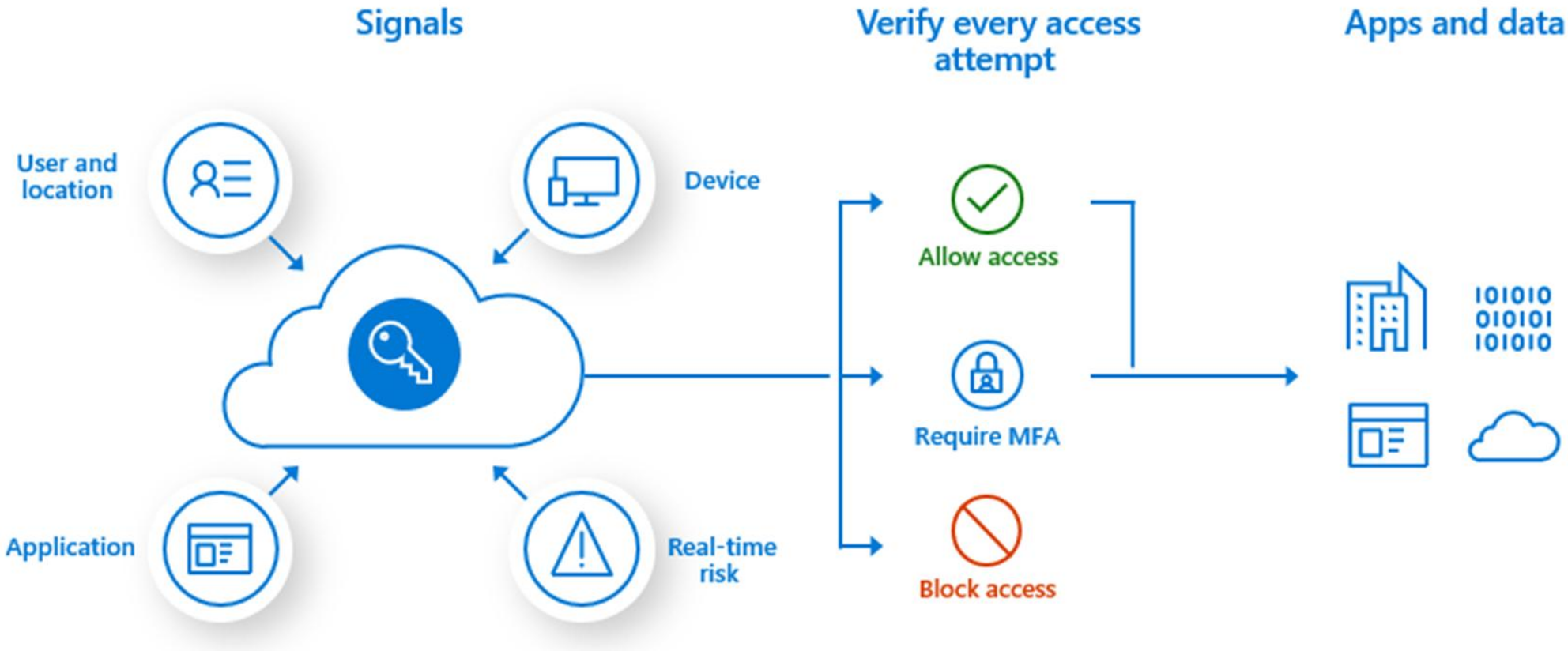
Unternehmen stehen vor der Herausforderung, mit begrenzten Ressourcen ein zunehmend komplexes Bedrohungsumfeld zu bewältigen.

amexus®
Informationstechnik

Teil 2

Best Practices für M365 Security

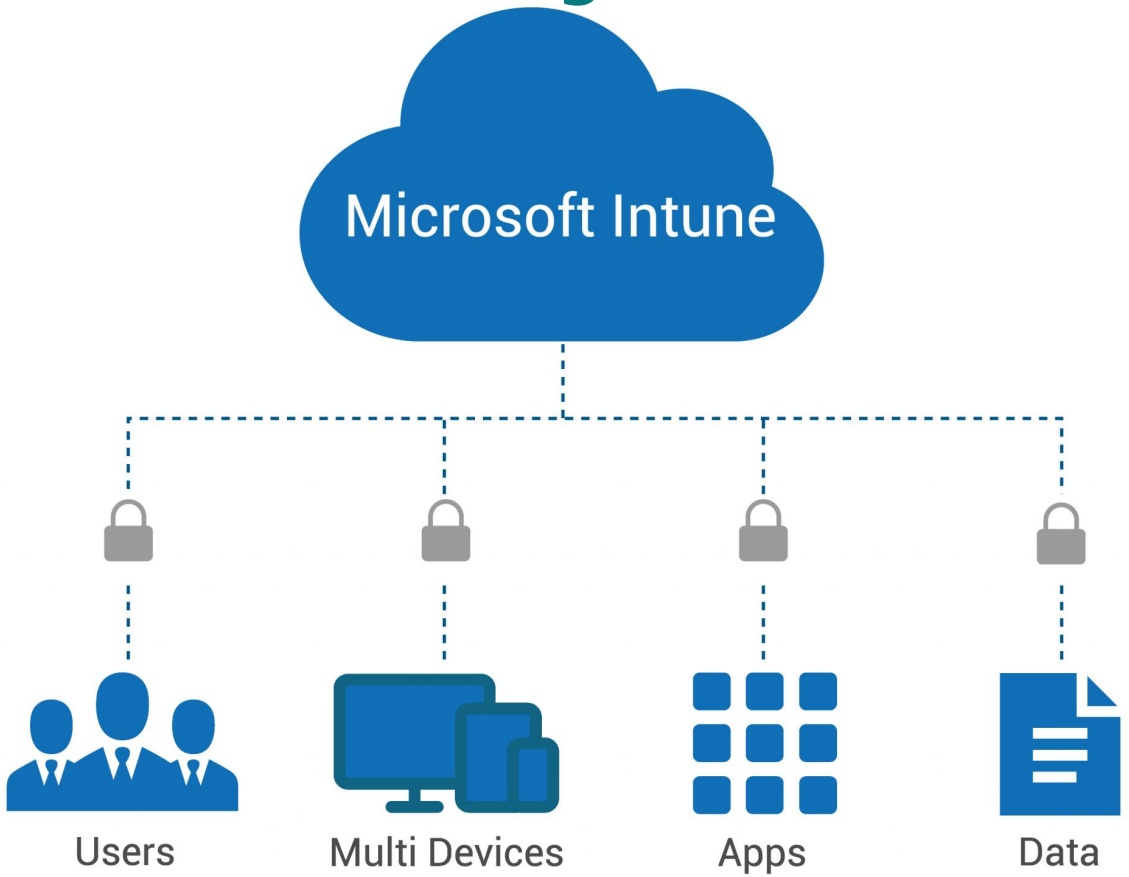
Methode 1 - Identitäts- & Zugriffschutz



Passwörter allein reichen nicht mehr aus.

MFA und Conditional Access verhindert, dass gestohlene Zugangsdaten direkt zu einem Sicherheitsvorfall führen – und sind damit mit die effektivsten Schutzmaßnahmen überhaupt.

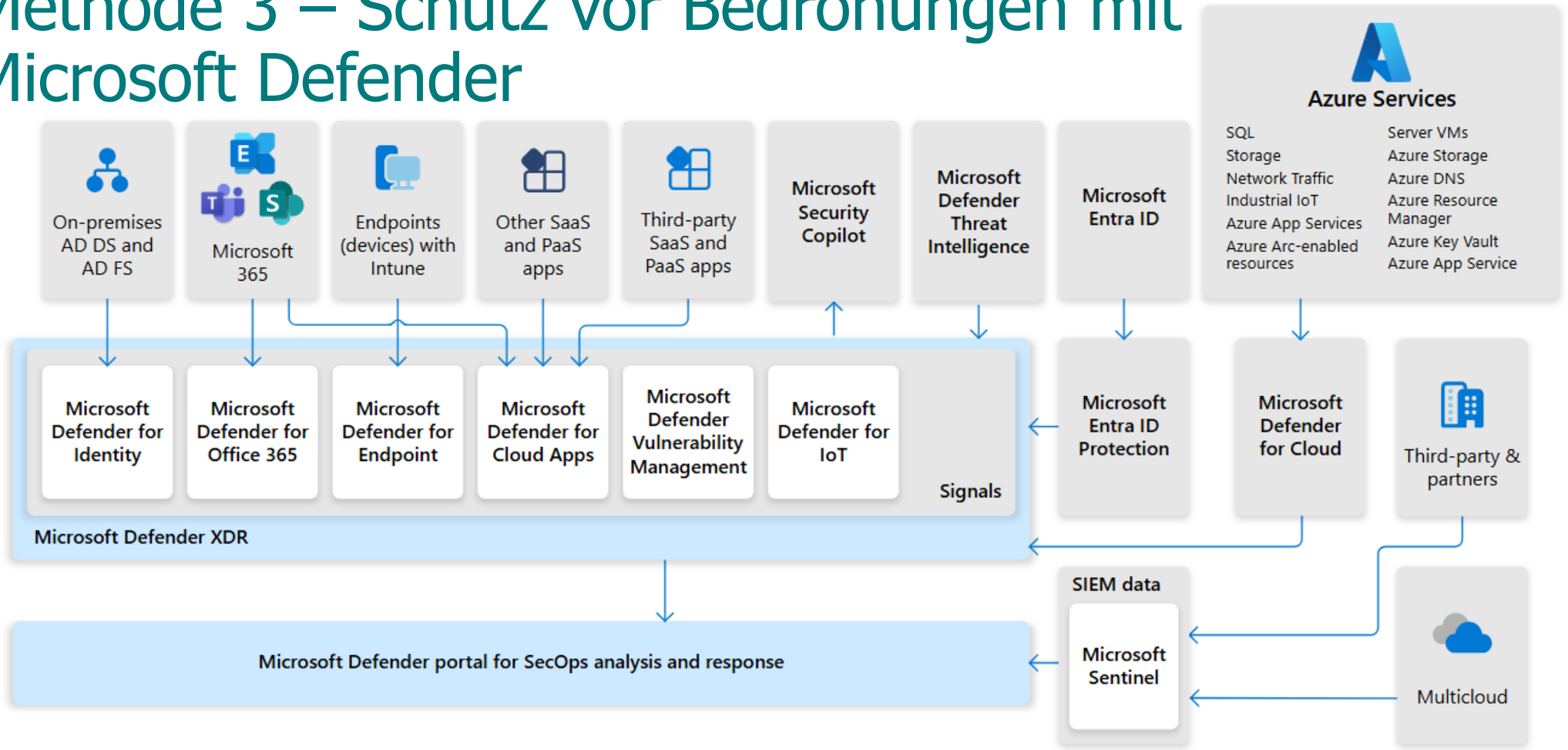
Methode 2 – Gerätemanagement mit Microsoft Intune



Mitarbeitende arbeiten heute mobil und auf verschiedenen Geräten.

Nur wenn diese **Geräte sicher verwaltet** werden, bleibt auch der Zugriff auf Unternehmensdaten geschützt.

Methode 3 – Schutz vor Bedrohungen mit Microsoft Defender

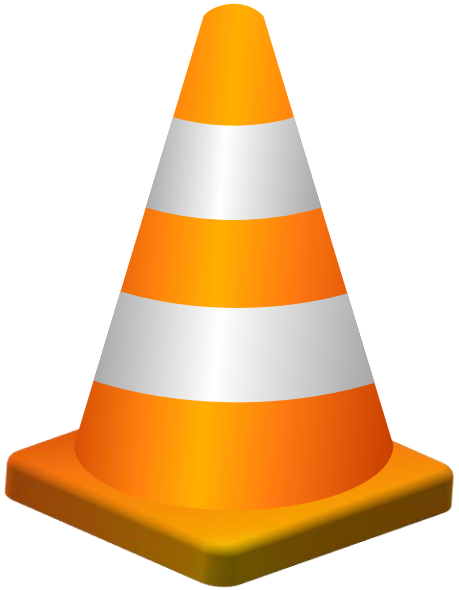


Angriffe werden immer raffinierter.

Microsoft Defender erkennt Bedrohungen frühzeitig und hilft, schnell und automatisiert zu reagieren – bevor Schaden entsteht.

Methode 4 – Admin Konten absichern

- ✓ **Reduzierung** der Anzahl von Admin Konten
- ✓ **Personalisierung** von Admin Konten
- ✓ Vergabe **granularer Berechtigungen** je Admin Konto
  - ✓ Nur Share Point Online
  - ✓ Nur Azure
  - ✓ Nur Teams



Admin Konten haben weitreichende Rechte – ein kompromittiertes Konto kann katastrophale Folgen haben. Deshalb müssen sie **besonders geschützt und überwacht** werden.

Methode 5 - Sichere Freigabe & Zusammenarbeit mit Externen

- ✓ **Verwaltung externer Benutzer**
  - ✓ On- und Offboardingprozess für den Umgang mit externen Benutzern
  - ✓ Einladungseinstellungen – um zu definieren, wer Gäste einladen darf
- ✓ **Freigabe in Teams und Gruppen kontrollieren**
  - ✓ Verwenden von Microsoft Teams-Richtlinien, um zu steuern, ob Gäste eingeladen werden dürfen
- ✓ **Unternehmensweite Freigaberichtlinien definieren**
  - ✓ Standardmäßig nur interne Freigabe von Dokumenten
  - ✓ Externe Freigabe nur an authentifizierte Gäste
  - ✓ Freigabe nur mit Ablaufdatum und Zugriffskontrolle

Die Zusammenarbeit mit Externen ist essenziell – aber ohne **klare Regeln und technische Kontrolle** kann sie schnell zum Sicherheitsrisiko werden.

Methode 6 – Sicherheitsbewusstsein der Mitarbeitenden stärken

- ✓ **Regelmäßige Awareness-Trainings**
  zu Themen wie Phishing, Social Engineering, Passwortsicherheit und Datenschutz
- ✓ **Simulierte Phishing-Kampagnen**
  um das Erkennen von Angriffen zu üben und Schwachstellen zu identifizieren
- ✓ **Klare Richtlinien und Meldewege**
  für verdächtige Vorfälle etablieren
- ✓ **Rollenbasierte Schulungen**
  IT, Management und Fachabteilungen benötigen unterschiedliche Inhalte
- ✓ **Gamification & interaktive Formate nutzen**,
  um das Lernen motivierend und praxisnah zu gestalten

Die beste Technik nützt nichts, wenn Menschen Fehler machen.

Geschulte Mitarbeitende sind die erste Verteidigungslinie gegen Cyberangriffe –
und oft die Entscheidende!

amexus®
Informationstechnik

Teil 3

Best Practices Datenschutz & Compliance

Methode 1 – Daten klassifizieren & schützen

- ✓ **Unternehmensweite Klassifizierungsrichtlinien**
  - ✓ Welche Daten fallen in welche Klassifizierungsstufe
  - ✓ Integration der Klassifizierung in Arbeitsprozesse, z.B. durch Vorlagen oder Workflows
- ✓ **Automatische Klassifizierung**
  - ✓ Erkenne sensible Informationen wie z.B. personenbezogene Daten, Finanzdaten oder Verträge
- ✓ **Unternehmensweite Sensitivitätslabels definieren**
  - ✓ Verknüpfung von Labels mit Schutzmaßnahmen wie Verschlüsselung, Wasserzeichen oder Zugriffbeschränkungen

Nur wenn **Daten richtig klassifiziert** sind, können sie auch **angemessen geschützt** werden.

Demo

Methode 2 - Datenverluste verhindern mit Data Loss Prevention (DLP)

- ✓ **DLP-Richtlinien auf Basis von Klassifizierungen erstellen**
  - ✓ Nutze die zuvor definierten Sensitivitätslabels als Grundlage für DLP-Regeln.

  Beispiel: Dateien mit dem Label „Vertraulich" dürfen nicht an externe Empfänger gesendet oder in OneDrive öffentlich geteilt werden.
- ✓ **Automatische Erkennung sensibler Inhalte aktivieren**
  - ✓ Automatische Erkennung von personenbezogenen Daten, Kreditkartennummern oder Gesundheitsinformationen
  - ✓ DLP-Richtlinien greifen in Echtzeit – z. B. beim Versand einer E-Mail oder beim Hochladen einer Datei in SharePoint.
- ✓ **Schutzmaßnahmen bei Regelverstößen definieren**
  - ✓ Aktionen wie Blockieren, Warnen, oder Überschreiben mit Begründung an die IT können automatisiert ausgelöst werden.
  - ✓ Benutzer erhalten kontextbezogene Hinweise, um ihr Verhalten anzupassen

DLP sorgt dafür, dass vertrauliche Daten **nicht nur richtig gekennzeichnet**, sondern auch **aktiv vor Verlust oder Missbrauch geschützt werden** – automatisch, nachvollziehbar und regelbasiert.

Methode 3 - Compliance überwachen mit Microsoft Purview

- ✓ **Compliance Manager zur Steuerung nutzen**
  - ✓ Verknüpfung von Sensitivitätslabels und DLP-Richtlinien mit konkreten Compliance-Kontrollen (z. B. DSGVO, ISO 27001).
  - ✓ Empfehlungen und Maßnahmenpläne zur Risikominimierung

- ✓ **Überwachung durch Audit Logs & Access Reviews**
  - ✓ Protokollierung von Aktivitäten rund um klassifizierte und geschützte Daten
  - ✓ Durchführung von regelmäßige Zugriffsüberprüfungen für sensible Inhalte und externe Benutzer

- ✓ **Berichte und Nachweise für Audits bereitstellen**
  - ✓ Erstellung von Compliance-Berichten zur internen Kontrolle und externen Prüfung
  - ✓ Dokumentierung, wie Klassifizierung und DLP-Richtlinien im Unternehmen umgesetzt werden

Nur was überwacht wird, kann auch verbessert werden. Microsoft Purview macht Compliance messbar, nachvollziehbar und auditierbar – und schafft damit die notwendige Transparenz über den Schutz sensibler Daten im Unternehmen.

amexus®
Informationstechnik

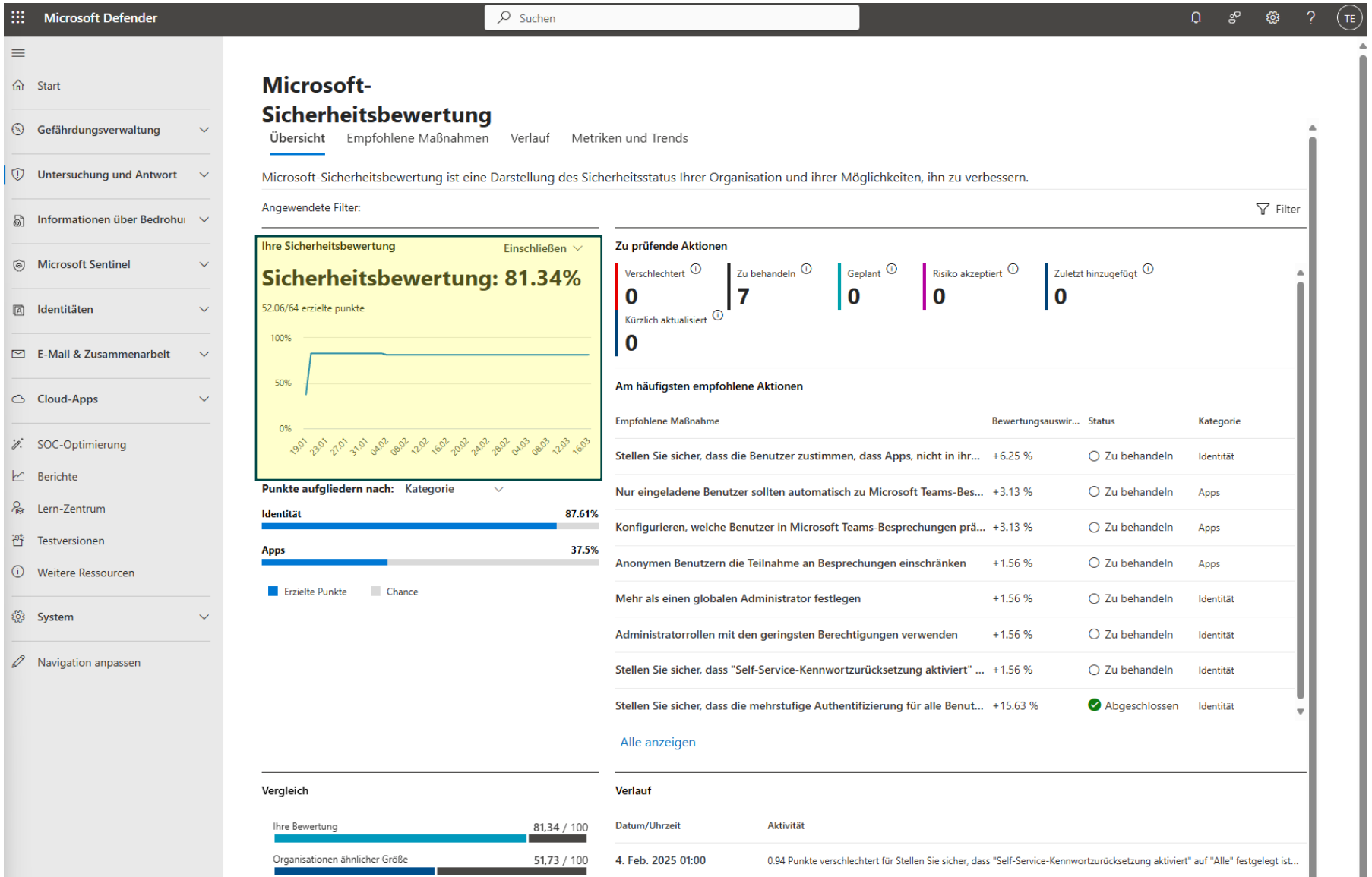
Zusammenfassung

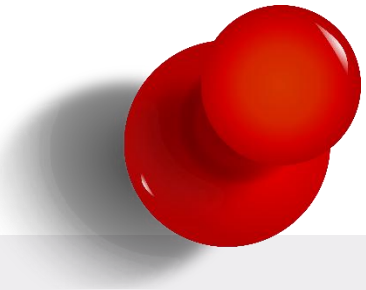
Ihre nächsten Schritte für mehr Sicherheit in Microsoft 365

- ✓ **Schritt 1:** Umfassende Bewertung und Etablierung einer Baseline
- ✓ **Schritt 2:** Schaffung klarer Regelwerke
- ✓ **Schritt 3:** Einrichtung der Grundlagen - MFA, E-Mail-Schutz und sichere Admin-Konten
- ✓ **Schritt 4:** Regelmäßiges Monitoring und Berichterstattung
- ✓ **Schritt 5:** Kontinuierliche Verbesserung und Anpassung

Sicherheit ist kein Produkt, sondern ein Prozess – und Microsoft 365 bietet die Werkzeuge, um ihn erfolgreich zu gestalten.

Microsoft Sicherheitsbewertung





Microsoft 365 Security Basis Schulung (8 Stunden)

Unsere kompakte Microsoft 365 Schulung rund um Security-Basics vermittelt Ihnen die wichtigsten Grundlagen der Sicherheitsfunktionen von M365 – von Identitätsschutz und Zugriffskontrollen bis hin zu sicheren Arbeitsmethoden. Perfekt für IT-Admins und Sicherheitsverantwortliche, die ihr Unternehmen gegen Cyberbedrohungen wappnen möchten. Für die optimale Durchführung wird mindestens eine Business Premium Lizenz vorausgesetzt. Steigen Sie jetzt ein in die Welt der M365 Security und stärken Sie Ihre Abwehrmechanismen!

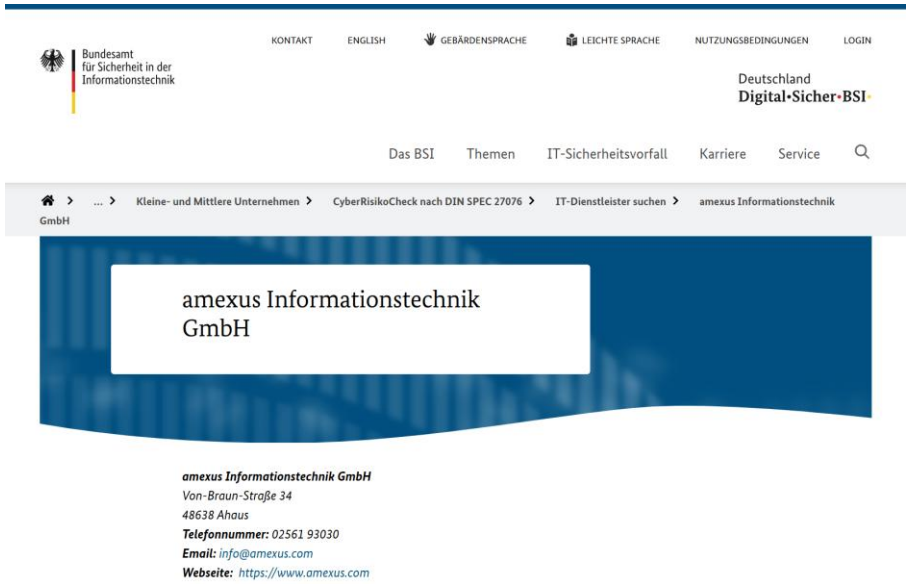
Schulungsinhalt:

- Entra ID
- Berechtigungen
- Multi-Faktor-Authentifizierung (MFA)
- Identity Protection
- Passwörter
- Self-Service Password Reset
- Enterprise Application
- Security/Defender
  - Security Score
- Auditlogs
- Exchange Online Protection
  - Exchange Regeln
- Sicherheit in SharePoint/OneDrive
- Sicherheit in Microsoft Teams

Jetzt anfragen

CyberRisikoCheck

- ✓ Offizielles BSI-Prüfverfahren zur Bewertung von Cyberrisiken
- ✓ Identifikation von Schwachstellen in der IT-Sicherheit
- ✓ Konkrete Handlungsempfehlungen zur Risikominimierung
- ✓ Verbesserung der IT-Sicherheitsstrategie Ihres Unternehmens
- ✓ Unterstützung bei der Umsetzung von Schutzmaßnahmen
- ✓ Erhöhung der Resilienz gegen Cyberangriffe



Bundesamt für Sicherheit in der Informationstechnik

?

Danke

Pause