

Beispiel Präsentation - Musterfirma



Security Assessment

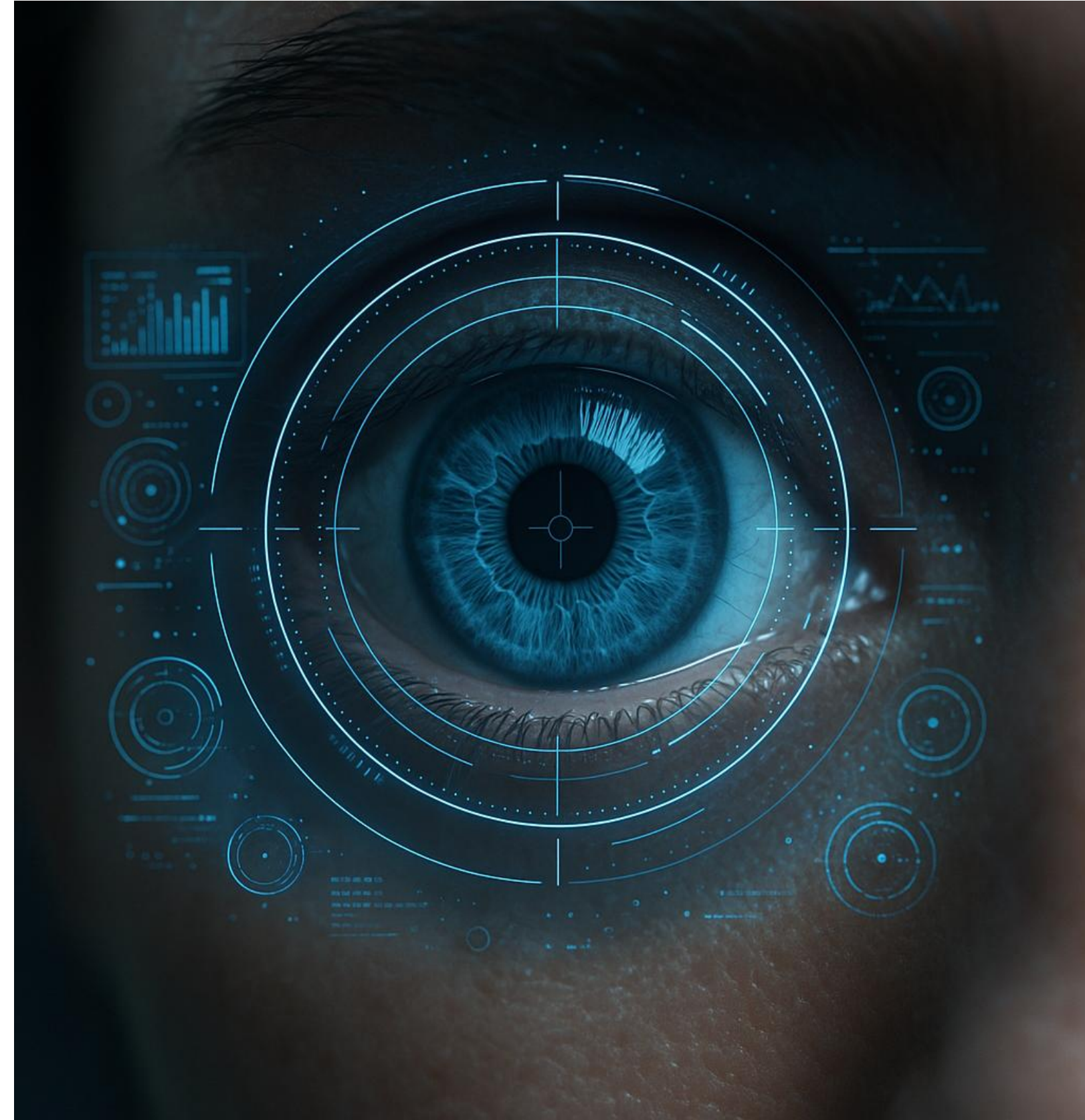
für:

Muster AG
Mustergasse 12
XXXX Musterhausen

Datum: 31.01.2026

Ersteller: Daniel Wittwer

Rev.No: 1.0, 30.03.2026



Inhalt



1. Einleitung
2. Bewertungsansatz
3. Zusammenfassung
4. Ansatzplan
5. Zusammenfassung der Ergebnisse
6. Nächste Schritte

Einleitung | Zweck des Berichts



Die Cybersecurity-Bewertung zielt darauf ab, ein umfassendes Verständnis der aktuellen Cybersicherheitslage Ihrer Organisation sowie umsetzbare Massnahmen zur Minderung entdeckter Risiken zu vermitteln. Der Bericht zielt nicht darauf ab, eine umfassende Sicherheitsüberprüfung oder -prüfung zu liefern, sondern vielmehr ein umfassendes Verständnis der Cybersicherheitsreife Ihrer Organisation. Ziel ist es, das Bewusstsein für die aktuelle Sicherheitslage zu erhöhen und praktische sowie spezifische Empfehlungen für die weitere Entwicklung zu geben.

Die Cybersecurity Assessment basiert auf dem international anerkannten Critical Security Controls (CSC) v8.1 Framework, das vom Center for Internet Security (CIS) veröffentlicht wurde. Weitere Informationen zum Framework finden Sie auf deren Website unter www.cisecurity.org.

Diese Präsentation ist eine Zusammenfassung der Ergebnisse, Analysen und Empfehlungen zur Stärkung Ihrer Sicherheitsresilienz. Weitere Details finden Sie unter CSAT.

Obwohl es sich weder um eine Überprüfung der Governance-Kontrolle noch um eine Sicherheitsprüfung handelt, können die Empfehlungen des Berichts genutzt werden, um die Organisation auf eine Prüfung vorzubereiten.



Assessment approach

Bewertungsübersicht | Stakeholder & Zeitplan



Firmen Name
Muster AG
Anzahl Beschäftigte
152
Anzahl der Endpunkte
154

Assessment Beteiligte Personen		
Name	Organization	Role
Daniel Wittwer	sec4it	Leitung
Peter Muster	Muster Firma	Security officer
Assessment start	2026-01-02	
Data collection and interview	2026-01-05	
Delivery month	2026-01-25	



Executive Summary

Executive Summary | CIS Maturity



CIS-Reifegrad

Ihr aktueller durchschnittlicher Reifegrad ist standardisiert.

Grosse Risiken

- Reputationsschaden

- Unbefugte Nutzung Ihrer E-Mail-Domain(n)

Finanzielle Schäden nach Ransomware-Angriffen

- Identitätsdiebstahl
- Nicht unterstützte Systeme
- **Durchgesickerte Unternehmensinformationen** (zum Beispiel personenbezogene Daten, vertrauliche Informationen, geistiges Eigentum)
- Third party Zugang zu IT-Systemen

Maturity Score

Maturity Score

1

2

3

4

Reactive

Strategic

Level 1
Basic

Level 2
Standardized

Level 3
Rationalized

Level 4
Dynamic

Der Fokus der Sicherheitsmassnahmen liegt auf der taktischen Ebene. Die Risiken eines Cybersicherheitsproblems sind gravierend.

Die Sicherheitsmassnahmen sind proaktiv ausgerichtet. Die Risiken im Zusammenhang mit Cybersicherheitsproblemen sind **erheblich**.

Die Sicherheitsmassnahmen erfolgen auf ganzheitlicher Ebene. Die Risiken im Zusammenhang mit einem Cybersicherheitsproblem sind moderat.

Die Sicherheitsmassnahmen erfolgen auf strategischer Ebene. Die Risiken im Zusammenhang mit Cybersicherheitsproblemen sind gering.



Unternehmensübersicht

Microsoft 365 Secure Score	74.69%
Cloud secure score	46.00%
Number of employees	152
Security aware employees	2
Employees without MFA on Entra ID	35

Strategische Empfehlungen

- Die Sicherheitsrisiken, denen die Organisation ausgesetzt ist, werden im Allgemeinen verstanden, wenn auch nicht auf eine kontrollierte Weise.
- Der Secure-Score liegt unter den vergleichbaren Unternehmensstandards und bietet Möglichkeiten für kurzfristige, kostengünstige Verbesserungen.
- Die Mitarbeiter der Organisation sind sich der heutigen (Cyber-)Sicherheitsbedrohungen nicht bewusst, und entsprechende Schulungen zu Sicherheit und Datenschutzbewusstsein fehlen.



Umsetzung- Massnahmen

Massnahmenplan



Der untenstehende Massnahmenplan ist unser Vorschlag, die Empfehlungen zu priorisieren. Die Priorität berücksichtigt die Dringlichkeit, den geschätzten Aufwand und die Komplexität.

0-30 days

Wir empfehlen, sich in den 0-30 Tagen auf die sogenannten 'low-hanging fruit'-Funktionen zu konzentrieren (Funktionen, die relativ einfach zu implementieren sind, aber erheblichen Einfluss auf die Verhinderung von Sicherheitsvorfällen)

- Löschen Sie alte und ungenutzte Computerkonten aus dem Active Directory
- Deaktivieren Sie alte und ungenutzte Konten in allen Anwendungen
- Erstellen Sie einen Prozess, um sicherzustellen, dass alle Anwendungen aktuell bleiben
- Implementieren Sie Multi-Faktor-Authentifizierung (MFA) für alle Benutzerkonten

30-90 days

Die 30-90 Tage konzentrieren sich auf Funktionen, die Ihre IT-Umgebung weiter stärken, sowie auf die Implementierung von Governance- und Berichtsfunktionen.

- Erstellen Sie einen Prozess, um externe Nutzer regelmässig zu überprüfen
- Implementieren Sie Tools, um sicherzustellen, dass alle E-Mails auf Malware, Phishing und Spam gescannt werden
- Implementieren Sie Werkzeuge, um sicherzustellen, dass eine zentrale Zeitsynchronisationsquelle auf den im Unternehmen verwendeten Assets eingerichtet wird
- Sichern Sie die Backups der Organisation entweder durch physische oder technische Sicherheitsmassnahmen

90+ days

Abschliessend behandeln die 90+ Tage Punkte die Erstellung/Überarbeitung von Prozessen sowie die Umsetzung von Lösungen, die eine längere Vorbereitungszeit erfordern.

- Verbessern Sie den Risikobewertungsprozess, der regelmässig durchgeführt wird
- Stellen Sie die Hardening-Baseline auf alle Geräte der Organisation (einschliesslich Mobilgeräte) bereit. Dies verringert die Angriffsfläche aller Geräte der Organisation. Stellen Sie sicher, dass die Baselines alle sechs Monate aktualisiert werden
- Implementierung eines grundlegenden Risikomanagementprozesses

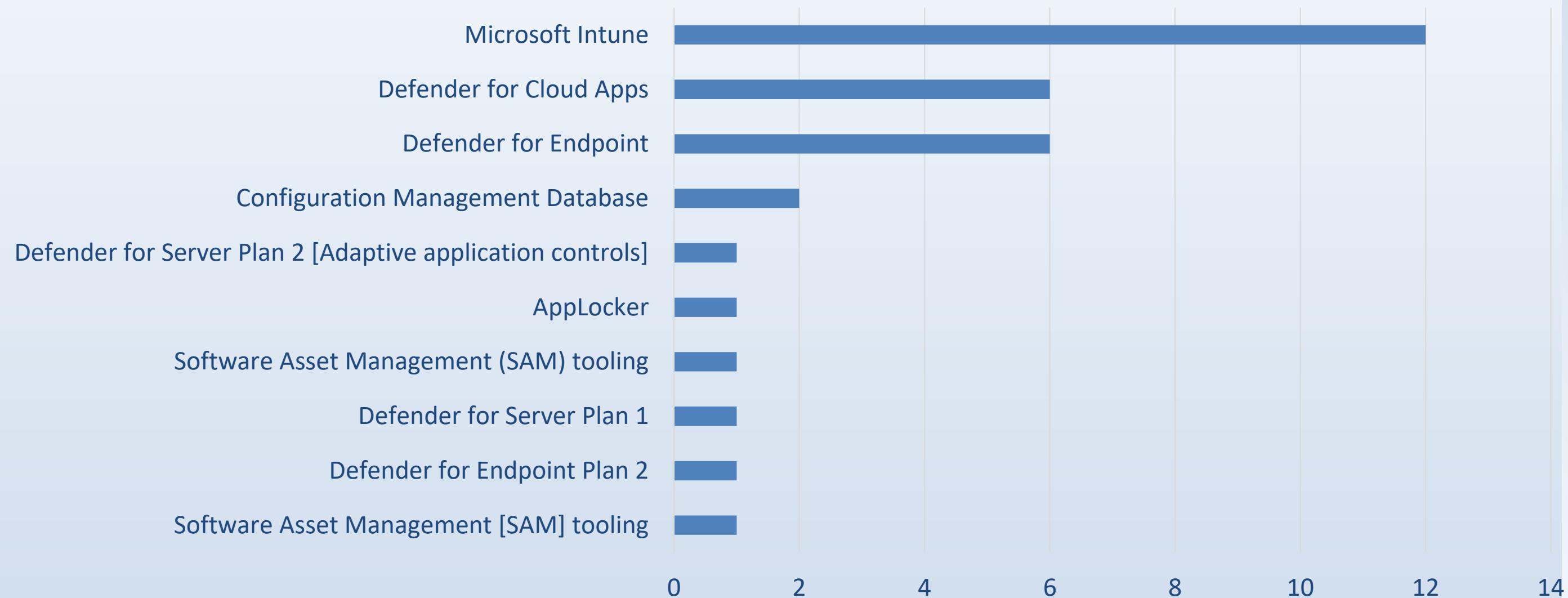
Vorgehensplan | geeignete technische Massnahmen



Dieses Diagramm präsentiert die Top 10 Lösungsoptionen

Die Empfehlungen erfolgen herstellerunabhängig. Genannte Produkte dienen als Beispiele möglicher Umsetzungen.

Beispiel geeigneter technischer Lösungen





Zusammenfassung der Ergebnisse

Zusammenfassung der Ergebnisse | CIS-Kontrollen



Niedrigst bewertete Frageantworten

CIS-Kontrolle 3. - Datenschutz

Erstellen Sie ein Datenklassifizierungsschema und implementieren Sie Werkzeuge, um die entsprechenden Labels zu erleichtern. Weisen Sie die Nutzer an, wie sie die Labels verwenden sollen, um regulatorische Anforderungen zu erfüllen.

CIS-Kontrolle 4. - Sichere Konfiguration von Unternehmensanlagen und –software

Implementieren Sie einen Prozess, um die Standardpasswörter für alle Geräte/Geräte zu ändern, die an Ihre IT-Infrastruktur angeschlossen werden.

CIS v8

1. Inventory and Control of Enterprise Assets

2. Inventory and Control of Software Assets

3. Data Protection

4. Secure Configuration of Enterprise Assets and Software

5. Account Management

1 2 3 4

1 2 3 4

1 1.7 3 4

1 1.8 3 4

1 2.2 3 4



Niedrigst bewertete Frageantworten

CIS-Kontrolle 8. - Verwaltung von Audit-Logs

Erstellen Sie einen Prozess zur Analyse der Auditprotokolle.

CIS-Kontrolle 10. - Malware-Verteidigung

Implementieren Sie Anti-Exploitation-Tools auf den kritischsten Serversystemen.

6. Access Control Management

7. Continuous Vulnerability Management

8. Audit Log Management

9. Email and Web Browser Protections

10. Malware Defenses

1

2

3

4

1

2.3

3

4

1.3

2

3

4

1

2

3

4

1

1.7

3

4

Zusammenfassung der Ergebnisse | CIS-Kontrollen



Niedrigst bewertete Frageantworten

CIS control 11. - Data Recovery

Führen Sie automatisierte Backups für Ihre wichtigsten Vermögenswerte mindestens wöchentlich ein. Schützen Sie Backup-Daten vor Korruption durch Ausfälle oder Ransomware-Angriffe. Workloads auf Cloud-Dienste verlagern.

CIS control 14. - Security Awareness and Skills Training

Richten Sie ein grundlegendes Schulungsprogramm ein, wie man Sicherheitsvorfälle erkennt. Richten Sie eine einfache Methode zur Meldung von Vorfällen ein.



Scan Findings | Windows versions

Die Daten auf dieser Seite beziehen sich auf CIS Control 1, NIS2 Artikel 21.2.a, NIS2 Artikel 21.2.g und Zero Trust Zone 2



Ergebnisse

- **Eine Reihe von Geräten** in der MDM-Lösung ist länger als 30 Tage inaktiv
- **Mehrere Geräte** in Microsoft sind in Intune als nicht konform markiert

Damit verbundene Risiken

- Hardware-Inventar: Keine Kontrolle über die gebrauchte Hardware, veraltete TPM-Chips, das Wissen, welche Chipsätze verwendet werden (für Firmware-Updates).
- Risiko von Datenkorruption oder -verlust durch kompromittierte Systeme, die sich mit Unternehmensanwendungen verbinden.

Empfehlungen

- Implementierung einer Konfigurationsverwaltungsdatenbank
- Überprüfung und Durchsetzung der Richtlinien für nicht konforme Geräte

INTUNE DEVICES - EXPANDED.ONMICROSOFT.COM	
Computer accounts	5
Intune Devices active 30 days	0
Intune Devices inactive 30 days	5
Intune Devices marked as not compliant	5
Number of unsupported OSes found in Microsoft Intune	1

Scan Findings | Updates

Die auf dieser Seite enthaltenen Daten beziehen sich auf CIS Control 2, NIS2 Artikel 21.2.g und Zero Trust Zone 2



Ergebnisse

- Es ist weder ein kontinuierlicher Patch-Management-Prozess noch ein regelmässiges Reporting an das Management definiert.

Damit verbundene Risiken

- Geschäftsbewusstsein: Ohne Berichterstattung gibt es keine Einblicke in den Status möglicher Risiken
- Sicherheitslücken: Neu entdeckte Sicherheitsprobleme werden nicht behoben und könnten ausgenutzt werden

Empfehlungen

- Implementierung einer kontinuierlichen Patch-Management-Lösung
- Implementieren Sie ein Reporting an das Sicherheitsmanagement beim Patch-Management-Status

Endpoints with missing critical updates	0
Endpoints with missing cumulative updates	7

Scan Findings | Endpoint Secure Configuration



Die Daten auf dieser Seite beziehen sich auf CIS Control 4, NIS2 article 21.2.g, Zero Trust zone 2 and 6

Ergebnisse

- Es wird keine Sicherheitsbasislinie auf Endpunkte angewendet

Damit verbundene Risiken

- Sicherheitslücken: (ältere) Protokolle haben bekannte Sicherheitsrisiken, die oft missbraucht werden
- Zu viele Dienste sind aktiviert: Standardmässig gibt es Dienste, die nicht genutzt werden, aber sie sind aktiviert, wodurch ein möglicher Zugang für unerwünschte Personen entsteht

Empfehlungen

- Definieren Sie eine geeignete Security Baseline und wenden Sie diese konsequent auf Ihre Endpunkte an.

SECURE CONFIGURATION

Incoming RDP enabled with no NLA

2

Endpoints with LM Compatibility lower than 5

1

Autorun Enabled

1

PowerShell 2.0 Enabled

1

Scan Findings | Microsoft Entra ID account monitoring



Die Daten auf dieser Seite beziehen sich auf CIS Control 5, NIS2 article 21.2.g, 21.2.i, and Zero Trust zone 1

Ergebnisse

- Mehrere deaktivierte Konten wurden gefunden
- Mehrere Konten, die keine Multi-Faktor-Authentifizierung (MFA) oder Conditional Access verwenden

Damit verbundene Risiken

- Unüberwachte, ruhende (aktive) Konten neigen dazu, unbemerkt missbraucht zu werden
- Passwortangriff: Ohne MFA und Conditional Access ermöglichen nur ein Benutzername und Passwort den Zugriff auf Unternehmensdaten/-vermögen

Empfehlungen

- Implementieren Sie einen Prozess, um regelmässig/automatisch ungenutzte Konten zu bereinigen
- Erzwingen Sie MFA- und Conditional Access für alle Nutzer, die von nicht vertrauenswürdigen Standorten/Geräten auf Unternehmensinformationen zugreifen

MICROSOFT ENTRA ID INFORMATION - EXPANDED.ONMICROSOFT.COM

Enabled Internal Users	42
Disabled Internal Users	2
Enabled External Users	5
Disabled External Users	2
Enabled Internal Users Without MFA	35
Enabled External Users Without MFA	3
Guest Accounts Found With Non-Corporate Email Address	3
M365 Audit Log Search	Yes

Scan Findings | Microsoft Entra ID administrator accounts



Die Daten auf dieser Seite beziehen sich auf CIS Control 6, NIS2 article 21.2.i, 21.2.j, and Zero Trust zone 1

Ergebnisse

- Multi-Faktor-Authentifizierung und Conditional Access werden bei mehreren Admin-Konten nicht verwendet
- Damit verbundene Risiken
- Durchgesickerte Administrator-IDs gewähren uneingeschränkten Zugriff auf Ihre Umgebung
- Durchgesickerte Benutzerkonten werden missbraucht, um Administratorzugriff zu erhalten

Empfehlungen

- Überprüfen Sie alle Nutzer in den Admin-Gruppen auf Legitimität; begrenzen Sie diese Zahlen so weit wie möglich.
- Erzwingen Sie Multi-Faktor-Authentifizierung und bedingten Zugriff für alle Administratoren/privilegierten

Benutzer

- Implementieren Sie das Privileged Identity Management, um Just-in-Time-Zugriff für die Microsoft Entra ID-Administratoren bereitzustellen

MICROSOFT ENTRA ID ADMINISTRATORS - EXPANDED.ONMICROSOFT.COM

Number of enabled accounts with Microsoft Entra ID user roles without MFA	0
Total roles used with privileged identity management	8
Privileged identity management assignments without an end date	31
Users with the Global admin role active or eligible	4
Total of guest users with role assignments	0

Scan Findings | Microsoft 365 Secure Score



Der Microsoft Secure Score scannt mehrere Bereiche innerhalb von Microsoft 365 und Microsoft Entra ID. Der Wert basiert auf der Art der verwendeten Dienste und vergleicht sie mit einer von Microsoft festgelegten Basislinie. Die Bewertung zeigt, inwieweit Sie mit den empfohlenen Sicherheitspraktiken übereinstimmen.

Wir empfehlen, mit den folgenden Themen zu beginnen.

- Für Verwaltungsaufgaben Mehrfaktor-Authentifizierung und Conditional Access erforderlich
- Aktivieren Sie die Anmelderrisiko-Richtlinie
- Richtlinie aktivieren, um die Legacy-Authentifizierung zu blockieren, aktivieren

ASSESSMENT 22-JUN-2023 MICROSOFT SECURE SCORE

Tenant Name: **expanded.onmicrosoft.com**

Secure Score: 74.69%

961.2/1287 points achieved

Microsoft Secure Score analyzes the protection state of your identities, data, devices, apps and infrastructure

Identity 85.35%

Protection state of your Microsoft Entra ID accounts and roles

Data 100.00%

Protection state of your Microsoft365 documents

Devices 72.44%

Protection state of your devices

Apps 74.92%

Protection state of your email and cloud apps

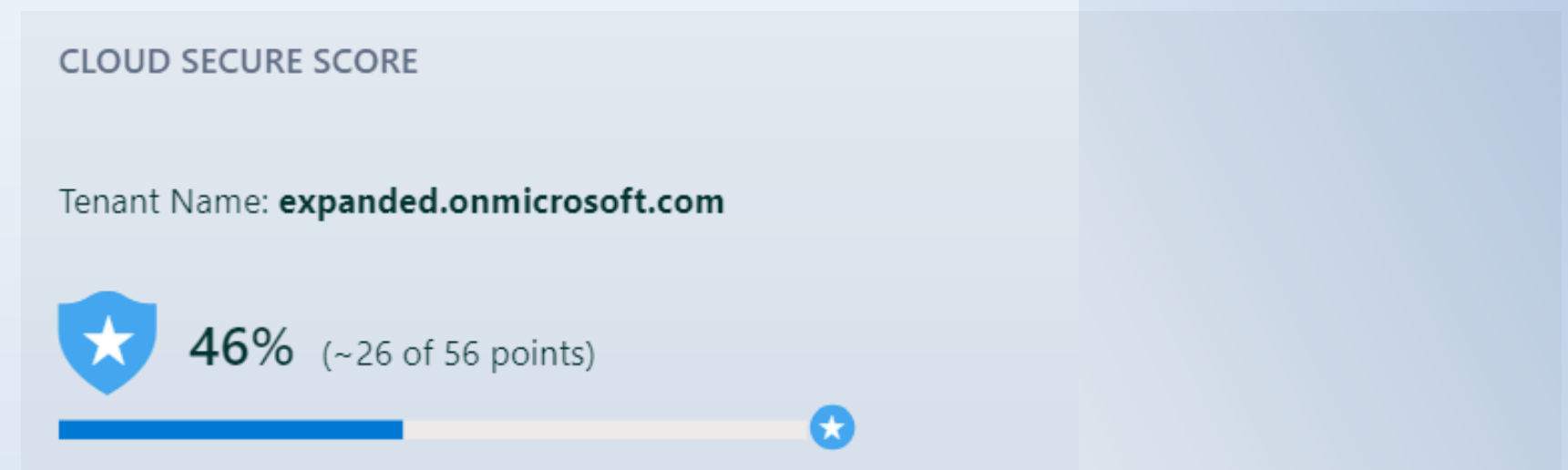
Scan Findings | Cloud Secure Score



Der Cloud Secure Score scannt alle Azure-Ressourcen innerhalb des Tenants. Der Secure Score basiert auf der Art der verwendeten Dienste und vergleicht sie mit den Sicherheitsbasislinien und empfohlenen Praktiken von Microsoft.

Wir empfehlen, mit den folgenden Punkten zu beginnen.

- Multi-Faktor-Authentifizierung und Conditional Access sollten auf Konten mit Schreibberechtigungen in Ihrem Abo aktiviert sein
- Webanwendungen sollten nur über HTTPS zugänglich sein





Weitere Möglichkeiten

Next steps | Wie können wir helfen?



Priorisierte Empfehlungen

Priorisieren und implementieren Sie 0-30-Tage-Aktionen

Regelmässige Neubewertung der Sicherheit

Definieren Sie Projektpläne basierend auf dem Vorgehensplan

Next steps | mögliche Folgemaassnahmen bei bestehender Microsoft-Infrastruktur



Vertrieb – Compliance- und Datenschutzrisiken mindern
Zeigen Sie, wie Microsoft Purview Sie dabei unterstützt, Risiken zu erkennen, zu untersuchen und Massnahmen zu ergreifen, um Risiken zu mindern und die Einhaltung der Vorschriften in ihrem modernen Arbeitsplatz sicherzustellen.

Nutzung – Sichere Identitäten und Zugriff
Helfen Sie Kunden, Identitätsrisiken zu finden und zu mindern, und schützen Sie ihre Organisation mit einer nahtlosen Identitätslösung.

Nutzung – Schützen und steuern Sie sensible Daten
Microsoft Purview kann Ihnen nutzen, indem Sie ihre sensiblen Daten schützen und sie über riskantes Verhalten informieren.

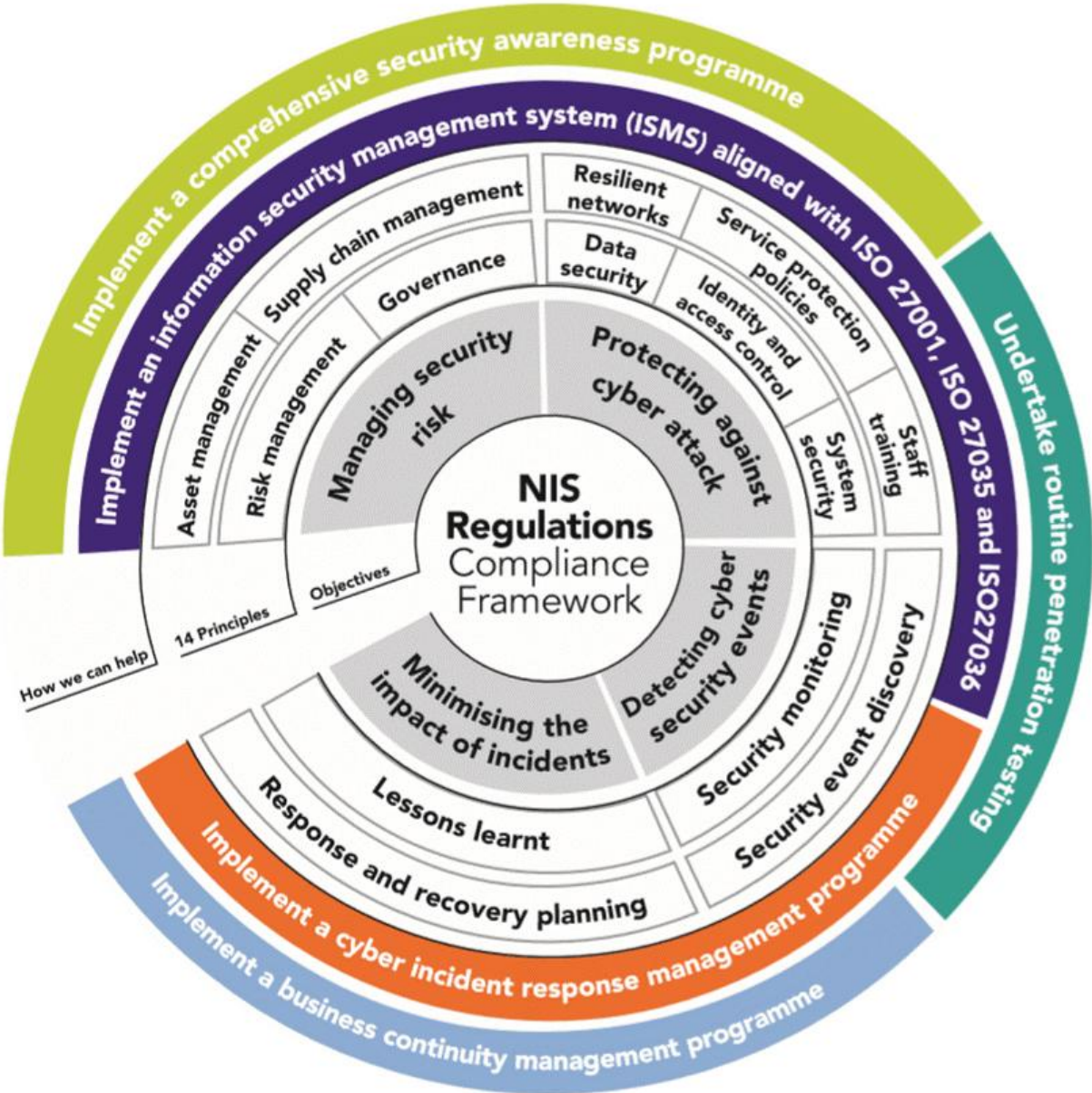
Bewertungsansatz – NIS 2



- Die NIS2-Richtlinie ist die EU-weite Gesetzgebung zur Cybersicherheit. Ziel von NIS2 ist es, das Gesamtniveau der Cybersicherheit in der EU zu verbessern.
- Ausgewählte Assessment-Fragen werden zusätzlich NIS2-Anforderungen und Zero-Trust-Prinzipien zugeordnet. Dadurch lassen sich technische und organisatorische Findings auch aus regulatorischer Sicht einordnen.
- Im Fragebogen verwenden wir diese Prinzipien

NIS Objectives							
A: Managing security risk		B: Protecting against cyber attack		C: Detecting cyber security incidents		D: Minimising the impact of cyber security incidents	

NIS Principles							
A1: Governance	A2: Risk management	B1: Service protection policies and processes	B2: Identity and access control	C1: Security monitoring	C2: Proactive security event discovery	D1: Response and recovery planning	D2: Lessons learned
A3: Asset management	A4: Supply chain	B3: Data security	B4: System security				
		B5: Resilient networks and systems	B6: Staff awareness and training				



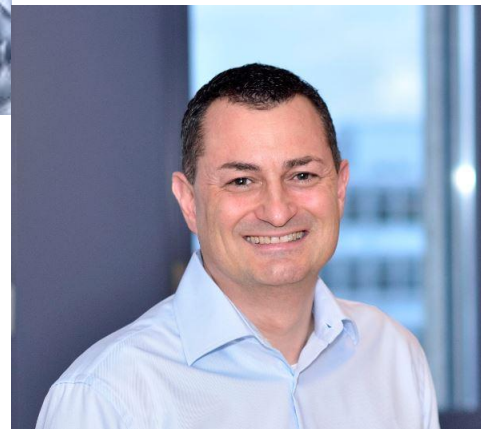
Über uns – drei Ansprechpartner



Beat
Brunschwiler,
CEO & Consulting



Daniel
Wittwer,
CTO & Consulting



Thomas
Fink,
Sales Manager

“

Unsere gemeinsamen Erfahrungen und Projekte brachten uns zusammen. Wir sind der Überzeugung gemeinsam unsere Leidenschaft von IT-Sicherheit und Kompetenz mit Ihnen zu teilen. Wir setzen ausnahmslos auf eine Europäische Software für Assessments und verkaufen keine Produkte.



“

Wir unterstützen Sie bei der Erstellung Ihrer individuellen Security-Roadmap, die auf den Fakten der hybriden Infrastruktur Ihres Unternehmens basiert. Damit können Sie beweisen, dass Sie Sicherheit ernst nehmen.

Unsere Kompetenzen

- Cybersecurity Assessments, Liz. Audits
- Cloud & Hybrid Infrastructure
- Datenschutz & Governance
- Security Roadmaps

Kanton ZH
Stadt Zürich
Aesch ZH
Pfaffhausen ZH

Kanton AG
Burg

Tessin*
Locarnese

*Mitglied ated
(Associazione Ticinese
Evoluzione Digitale)

Vielen Dank für Ihre Aufmerksamkeit



Ein Cybersecurity Assessment schafft die Grundlage für eine höhere Cyberresilienz.

Das Self-Service Assessment bietet einen einfachen Einstieg in die strukturierte Bewertung Ihrer Cybersecurity.

Link zum Scope (Self-Service):
<https://sec4it.selfserviceassessment.com>

Hauptsitz:
AGfB AG, Rotbuchstrasse 60, 8037 Zürich

Kontakte
Beat Brunschwiler, CEO 079 572 00 36
Daniel Wittwer, CTO 078 823 87 77
Thomas Fink, Sales Manager 078 323 96 42

Webseite: www.sec4it.ch
[www.sec4it.it /per ticinese](http://www.sec4it.it/per_ticinese)

E-Mails: