



Cybersecurity Report

Muster AG

Datum 2026

Version	1.0
Datum	XX.YY.2026
Kunde	Peter Muster Muster AG Musterstrasse CH- 8000 Muster
Zuständiger Consultant	Beat Brunschwiler



Inhalt

1. Zusammenfassung für das Management.....	4
1.1. Sicherheitsbewertung	4
1.2. Empfehlungen	5
2. Aktionsplan zur Verbesserung der Cybersicherheit.....	7
2.1. Dringende Massnahmen	7
2.2. Quickwins	8
3. Cybersicherheit - Ergebnisse und Empfehlungen	9
3.1. Basic CIS Controls	9
3.2. Foundational CIS Controls.....	13
3.3. Organizational CIS Controls.....	17
4. Gescannte Daten und deren Analyse.....	21
5. Zusammenfassung aller Massnahmen.....	53
5.1. CISv8- Basic Massnahmen nach Priorität.....	53
5.2. CISv8- Foundational Massnahmen nach Priorität.....	55
5.3. CISv8- Organizational Massnahmen nach Priorität	56
6. Anhang A - Überblick über empfohlene Security-Software-Produkte.....	57
6.1. Microsoft 365 Business und Microsoft 365 E3	57
6.2. Microsoft 365 E3 Add-ons.....	58
6.3. Microsoft 365 E5	59
7. Anhang B - Produkte, bei denen der Support ausläuft	60
8. Anhang C - Details Secure Score	61
8.1. Bewertete Elemente	61
9. Anhang D - Scope des Assessments	63
9.1. Ziele des Cybersecurity Assessments.....	64
9.2. Inventory Tools	64
9.3. Cyber Security Assessment Tool	64
10. Anhang E - Hintergrund des Assessments	66
10.1. Einführung.....	66
10.2. Hintergrund des Control Frameworks (CIS)	67
10.3. SOM-Modell	67
10.4. Abnahme und Empfehlung	70



Dokumenten-Historie:

Version	Datum	Autor	Bemerkungen
0.1	XX.YY.2026	Beat Brunswiler	Draft
0.9	XX.YY.2026	Beat Brunswiler	Besprechungs-Dokument
1.0 (Final)	XX.YY.2026	Beat Brunswiler	Dokument zur Unterschrift

Wunsch der Muster AG

Aus Datenschutzrechtlichen Gründen wurden Maschinendaten/-Bezeichnungen, User und Gäste schwarz eingefärbt. [REDACTED]

1. Zusammenfassung für das Management

Dieser Cybersecurity Report ist das Ergebnis eines Cybersecurity Assessments, das für die **Muster AG** von **der Sec4it** im Mustermanat 2024 ausgeführt wurde. Stand der Datenerhebung XX.YY.2026 unter dem Aspekt das laufend Änderungen vorgenommen wurden.

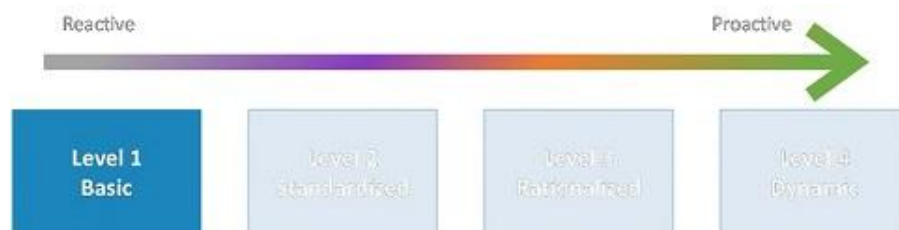
Der Cybersecurity Assessment Report liefert eine Gesamtbewertung der von der **Muster AG** verabschiedeten Richtlinien und geübten Praktiken zur Cybersicherheit. Der daraus abgeleitete Reifegrad der Cybersicherheit bei der **Muster AG** wurde durch die Beantwortung eines Fragebogens und die Durchführung eines automatisierten Scans sicherheitsrelevanter Daten ermittelt. Der Bericht stellt keine detaillierte Überprüfung und kein Security-Audit dar.

Neben dem Reifegrad liefert der Cybersecurity Report zusätzlich einen Aktionsplan mit vorgeschlagenen Massnahmen, die der **Muster AG** helfen werden, seinen Reifegrad kontinuierlich zu verbessern.

1.1. Sicherheitsbewertung

Die Überprüfung des Status im Hinblick auf jedes der so genannten CIS Controls™ (v8) und der Einhaltung der ISO/IEC 27001 Ergänzungen (später ausführlich erläutert) hat zu der folgenden Beurteilung des Reifegrades von **Muster AG** geführt:

- a) Auf Basis des niedrigsten Reifegrads aller untersuchten Positionen (schwächstes Glied in der Kette)



- b) Auf Basis des durchschnittlichen Reifegrads aller untersuchten Positionen

Unternehmens-Score



Die durchschnittliche Punktzahl ist eine sehr gute Kenngrösse, um Fortschritte bei zukünftigen Assessments zu dokumentieren.

Empfehlungen in diesem Cybersecurity Report beruhen auf den uns ermittelten Bewertungen. Im Einzelfall haben auch noch andere Einflussgrössen wie die Grösse und Branche der **Muster AG**, das regulatorische Umfeld und andere Risikofaktoren auf die abschliessenden Empfehlungen Einfluss genommen. Neben dem dokumentierten Status auf Basis der durchgeführten Einzelbewertungen wird auf die nachfolgenden generellen Aspekte in Bezug auf die aktuelle Situation der **Muster AG** und deren Verbesserung hingewiesen:



1.2. Empfehlungen

Hacker machen sich gerne verwaiste Accounts zu eigen. Um diesen Angriffsvektor einzuschränken, macht es Sinn, die Verantwortung für den Lebenszyklus von Benutzerkonten im Firmennetzwerk von der IT weg in die Fachbereiche hineinzuverlagern. Dazu gehört, dass jeder Account einen fachlichen Besitzer hat und dieser regelmässig bestätigt, dass die Konten, für die er verantwortlich ist, notwendig und mit den richtigen Zugriffsrechten ausgestattet sind. Auch hier kann eine erfolgreiche Umsetzung nicht ohne die Unterstützung seitens der Geschäftsführung erfolgen.

Wir empfehlen der Muster AG sich im Bereich der Führung mit den Empfehlungen im Bereich CISv8 „Organizational“ stärker zu Befassen.

Zusammenfassung der Massnahmen auf die untersuchten Punkte:

Die Basic Controls definieren eine Baseline für die Cybersecurity, während die Foundational Domäne grundlegende, wichtige Massnahmen zum Schutz der IT-Assets umfasst. Die Organizational Domäne bietet prozess- und verfahrenstechnische Anleitungen mit proaktiven und «mitigativen» Steuerelementen zum Schutz der Organisation vor Bedrohungen aus dem Internet.

Unten aufgeführt die Anzahl der Handlungsempfehlungen nach Dringlichkeiten in der Übersicht welche alle unter Punkt 5 im Detail als Zusammenfassung aufgeführt sind. Die einzelnen Findings finden sich im Bericht unter den einzelnen Erhebungen im Detail wieder. Als Grundlage diene der Scan als auch die Befragungen mit den Herren XY.

Gesamte Anzahl der Massnahmen die Empfohlen werden:

10 Dringend	19 Sehr wichtig	3 Wichtig	0 Empfohlen
----------------	--------------------	--------------	----------------

Aufstellung Domänen:

CISv8 Basic

3 Dringend	5 Sehr wichtig	3 Wichtig	0 Empfohlen
---------------	-------------------	--------------	----------------

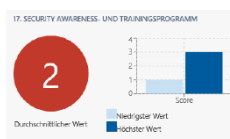
CISv8 Foundational

2 Dringend	8 Sehr wichtig	0 Wichtig	0 Empfohlen
---------------	-------------------	--------------	----------------

CISv8 Organisational

5 Dringend	6 Sehr wichtig	0 Wichtig	0 Empfohlen
---------------	-------------------	--------------	----------------

1.2.1. Empfehlungen auf Stufe Geschäftsleitung



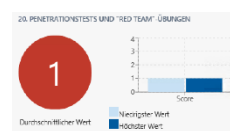
Setzen Sie ein grundlegendes Trainingsprogramm für die wichtigsten Rollen in Ihrer Organisation auf. Ein IT-Sicherheitsprogramm ist noch nicht umgesetzt. Eine Einführung in den Datenschutz und E-Learning wurde für die Mitarbeiter eingeführt und muss alle 2 Jahre wiederholt werden. Eine jährliche Schulung ist zu empfehlen. Ein Awareness Training ist für alle Abteilungen/ Standorte zu empfehlen und sollte auch auf die Gefahren



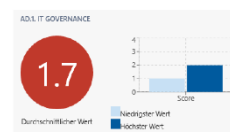
Starten Sie einen Code Review (oder führen Sie Werkzeuge dazu ein) für alle Eigenentwicklungen in Ihrer Organisation. Für einzelne Entwicklungen von Anwendungen wird die Sicherheit überprüft. Für Software von Microsoft werden die Sicherheitsempfehlungen beachtet und regelmässig aktualisiert. Bei Fremdsystemen oder Middleware muss die Verantwortlichkeit überprüft werden. Als Beispiel kann Java und 7-Zip erwähnt werden. Überprüfen Sie Regelmässig auch die Patches von dritt Herstellern. Der Zugriff für Entwickler ist für einige Systeme implementiert, auch bei Dritten ist darauf zu achten - wer bis wann und auch bei deren Fluktuationen diese regelmässig zu überprüfen und der Prozess mit Verantwortlichkeiten festzuhalten.



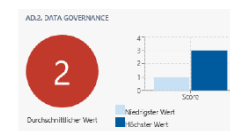
Setzen Sie einen grundlegende Incident Response Prozedur auf, die die häufigsten Szenarien abdeckt. Trainieren und leben Sie diesen Prozess. Verbessern Sie die Trennung von Pflichten, Aufgaben und Verantwortlichkeiten, indem Sie den Fokus auf eine übergeordnete Ebene legen. Das Vorgehen, die IT-Abläufe und die Definitionen sind beschrieben und wie vorzugehen ist. Ein Test und das Durchspielen eines Szenarios wurde jedoch noch nie durchgeführt. Wir empfehlen das «Worstcase» Szenario bei Möglichkeit zu üben.



Befauftragen Sie einen Spezialisten für dieses Thema mit der Durchführung eines Penetration Tests der von aussen sichtbaren Systemen der Organisation. Implementieren Sie einen Vulnerability Scanner in der IT-Infrastruktur der Organisation und verwenden diesen als Input für Penetration Tests. Intern werden Tests beim Aufsetzen von Neuen Systemen durchgeführt. Extern finden keine Prüfungen statt. Es sind auch keine Vulnerability Scans und Pentest zusammen eingesetzt. Anhand von solchen Tests können Ergebnisse wiederum als Input für weitere Penetrations-Tests genutzt werden. Es ist wichtig den Ergebnissen danach nachzugehen und Schwachstellen zu beheben. → **Penetrationstests und "Red Team"-Übungen**



Verbessern Sie die Trennung von Pflichten, Aufgaben und Verantwortlichkeiten, indem Sie den Fokus auf eine übergeordnete Ebene legen. Die Sicherheits- und Datenschutzrichtlinien sind vom Management definiert aber noch nicht komplett umgesetzt. Die Trennung von Pflichten, Aufgaben und Verantwortlichkeiten sind zu einer gewissen Grade nicht gegeben. Die Abläufe sind dokumentiert und ISO/IEC 27001 konform, aber nicht geschult. Es wird nach bestem Wissen und Gewissen auch in der IT umgesetzt. Dennoch fehlen in anderen Bereichen die notwendige Schulung und Regelung. Die regulatorischen und die gesetzliche Compliance als auch die Richtlinien, das Verhalten und die Prozesse sind festgehalten und werden zweijährig überprüft. **Führen Sie einen grundlegenden Risk Management Prozess ein.**



Datenklassifizierung und -kennzeichnung in allen Systemen
Personenbezogene Daten: Die Datenklassifizierung und der Schutz wurden in der Gruppe gemacht. Allein nur die Personen bezogenen Daten wurden als schützenswert definiert. Feststellung: nur mutwilliges Eingreifen kann als Risiko betrachtet werden. Zum System werden auch Verfahren von bezogenen Daten dokumentiert. Alle Softwaredienste sind aufgeführt. Bei Cloud-Diensten welche einzelnen Abteilungen oder einzelne Mitarbeiter verwenden könnte es Grenzwertig sein. (Teams, Trello und andere)
Es ist in der gesamten Organisation die Datenklassifizierungen und -Kennzeichnungen durchgeführt:
Es fehlt noch an regelmässigen Überprüfungen / Monitoring und Tracking dieser. Somit finden keine regelmässige Überprüfung und automatisierte Möglichkeit statt. Dies ist im Unternehmen derzeit organisatorisch geregelt.



2. Aktionsplan zur Verbesserung der Cybersicherheit

2.1. Dringende Massnahmen

Dies sind die Aktionen mit hoher Priorität, die durch das Assessment identifiziert wurden. Wir empfehlen, die folgenden Elemente mit oberster Priorität zu bewerten und wenn möglich anzugehen:

Thema	Aktion	Empfohlene Softwareprodukte
CISv8 - Basic		
4. Kontrollierte Nutzung von Administratorrechten	Implementieren Sie einen Prozess zur Genehmigung und regelmäßigen Bestätigung von Berechtigungen für Admin-Accounts. Bereinigen Sie alte / nicht genutzte Accounts.	Azure Privileged Identity Management (PIM), Azure AD Access Review
5. Sichere Konfiguration von Hard- und Software auf mobilen Geräten, Laptops, Workstations und Servern	Definieren Sie Hardening-Vorgaben für die wichtigsten Systeme, wobei diese standardmäßig so weit wie möglich abgeschlossen sein sollten.	Azure VMs, Azure CIS Hardened Images, Microsoft Endpoint Manager
6. Pflege, Überwachung und Analyse von Log-Dateien	Implementieren Sie einen Prozess zur Überwachung der Logs mit regelmäßiger Überprüfung auf kritische sicherheitsrelevante Einträge.	Die Einführung zu Überwachung von Log Files ist zu Empfehlen. Beispiel mit Azure Log Analytics
CISv8 - Foundation		
14. Zugriffskontrolle nach dem Need-to-Know-Prinzip	Führen Sie Netzwerk-Segmentierung für die wichtigsten Datenquellen der Organisation ein.	Beispiel: Die Klimasteuerung ist offen und sollte auch in einem Segment sein. Auf dem Campus werden alle durch geroutet, Versuchen die Trennung zu verfeinern und Netzwerk getriebene Devices zu segmentieren. (Gilt auch für den Service an einem Kaffeeautomaten)
16. Monitoring und Kontrolle von Benutzerkonten	Sorgen Sie dafür, dass die Fachbereiche die Verantwortung für ihre Benutzerkonten übertragen bekommen. Das schließt Prüfungen durch den fachlichen / funktionalen Besitzer des Benutzerkontos ein. Bereinigen Sie alte Accounts.	Azure AD Access Reviews
CISv8 - Organizational		
17. Security Awareness- und Trainingsprogramm	Setzen Sie ein grundlegendes Trainingsprogramm für die wichtigsten Rollen Ihrer Organisation auf.	Das können Sie mit Ihrem Softwarepartner und einem Tool wie Proofpoint mit Schulungen und Tests erweitern und durchsetzen
19. Incident Response und Management	Setzen Sie eine grundlegende Incident Response Procedure auf, die die häufigsten Szenarien abdeckt. Trainieren und leben Sie diesen Prozess	Office 365 Advanced Compliance: Advanced eDiscovery
20. Penetrationstests und "Red Team"-Übungen	Implementieren Sie einen Vulnerability Scanner in der IT-Infrastruktur der Organisation und verwenden diesen als Input für Penetration Tests.	Microsoft Endpoint Manager, Defender ATP, Azure Security Center + Pen testing tools
AD.1. IT Governance	Erweitern Sie die Policy zu Sicherheit und Datenschutz um branchenspezifische Themen und vereinheitlichen Sie sie in der ganzen Organisation.	Setzen Sie die Sicherheits- und Datenschutzrichtlinien anhand von internen Schulungen um. Die Trennung von Pflichten und Aufgaben müssen im Unternehmen klar sein.
AD.2. Data Governance	Führen Sie einen grundlegenden Risk Management Prozess ein.	Microsoft Compliance Manager (ermöglicht Workflow-basierte Risikobewertungen)



2.2. Quickwins

Die folgenden Aktionen sind Quickwins, die von **Muster AG** umgesetzt werden könnten. Empfohlene Massnahmen und Produkte im Überblick:

Thema	Aktion	Empfohlene Softwareprodukte
Quickwins		
Active Directory Accounts	• Überprüfen Sie Konten mit riskanten UAC-Flags (siehe 4.1.16) und ändern Sie diese Einstellungen. • Löschen Sie alte / nicht verwendete (Benutzer- und Computer-) Konten	
Azure AD Accounts	• Implementieren Sie Multi-Faktor-Authentifizierung (MFA) für alle Benutzerkonten • Überprüfen Sie Externe Benutzer im AAD	• Azure MFA • Conditional Access
Administratoren	• Löschen Sie alte / nicht verwendete Accounts • Nutzen Sie ausschliesslich dedizierte persönliche Admin-Accounts • Bereinigen Sie die privilegierten Gruppen der Domäne	
Richtlinie	• Verbessern Sie die Kennwortrichtlinie (siehe 4.1.16)	• Azure MFA
Betriebssysteme	• Migrieren Sie die (fast) End-of-Life-Betriebssysteme	• Windows Server 2016 oder 2019 • Windows 10, Build 1909
Windows-Updates	• Rollen Sie die verfügbaren Sicherheitspatches auf allen Endpunkten aus.	• Intune • Azure Security Center
Antivirus	• Aktualisieren Sie veraltete Virendefinitionen	• Microsoft Defender ATP
Firewalls	• Aktivieren Sie die Firewalls auf allen Endpunkten.	• Windows Firewall
Festplattenverschlüsselung	• Aktivieren Sie Festplattenverschlüsselung auf allen Endpunkten, speziell mobilen Geräten.	• BitLocker
E-Mail	• Erstellen Sie DKIM-Records für alle Domänen	• Office 365 Advanced Threat Protection P1 und P2
Netzwerkgeräte	• Führen Sie einen Prozess zur regelmässigen Kontrolle des Patch-Standes der Netzwerkgeräte ein.	



3. Cybersicherheit - Ergebnisse und Empfehlungen

Wichtiger als die Gesamt-Bewertung der Organisation sind die spezifischen Bewertungen zu jedem Element der CIS Controls™ (v8) und des ISO/IEC 27001 Frameworks. Jede Bewertung reflektiert den aktuellen Zustand. Die Empfehlungen geben darüber hinaus Hinweise, wo die **Muster AG** in Zukunft mit seinem Programm zur Cybersicherheit stehen sollte.

3.1. Basic CIS Controls

Die Basic CIS Controls beziehen sich auf Inventarisierung, Abgrenzung und Kontrolle der gesamten IT-Umgebung. Die sechs Basic CIS Controls und deren Ziele sind:

Thema	Ziel
1. Bestandsaufnahme und Kontrolle der Hardware-Assets	Aktives Management (inventarisieren, nachverfolgen und korrigieren) sämtlicher Hardware im Netzwerk, so dass nur autorisierte Geräte Zugang haben und nicht autorisierte / nicht verwaltete Geräte gefunden werden und den Zugang verweigert bekommen.
2. Bestandsaufnahme und Kontrolle der Software-Assets	Aktives Management (inventarisieren, nachverfolgen und korrigieren) aller Software im Netzwerk, so dass nur autorisierte Software installiert ist und ausgeführt werden kann. Nicht autorisierte / nicht verwaltete Software wird gefunden und an der Installation oder Ausführung gehindert.
3. Kontinuierliches Schwachstellen-Management	Kontinuierliches Sammeln und Bewerten von Informationen mit daraus folgenden Aktionen, um Schwachstellen zu identifizieren und zu beheben und das "Window of Opportunity" für Angreifer zu minimieren.
4. Kontrollierte Nutzung von Administratorrechten	Prozesse und Tools, um die Verwendung, Zuordnung und Konfiguration von Administratorrechten an Computern, Netzwerken und Anwendungen zu verfolgen / kontrollieren / verhindern / korrigieren.
5. Sichere Konfiguration von Hard- und Software für mobile Geräte, Laptops, Workstations und Server	Rigore Prozesse für das Konfigurations- und Änderungsmanagement von mobilen Geräten, Laptops, Workstations und Servern, zusammen mit einer aktiven Verwaltung (verfolgen, berichten, korrigieren) um zu verhindern, dass Angreifer sich gefährdete Dienste und Einstellungen zu Nutze machen.
6. Pflege, Überwachung und Analyse von Audit-Protokollen	Sammeln, Verwalten und Analysieren von Ereignis-Protokollen, die helfen könnten, Angriffe zu erkennen und zu verstehen und sich von ihnen zu erholen.



3.1.1. Basic CIS Controls - Sicherheitsbewertung

Grundlage der Bewertung sind Einschätzungen auf Basis der Ziele der einzelnen Basic CIS Controls. Aus den Einschätzungen für die **Muster AG** zu den Positionen der Controls ergibt sich aggregiert das Rating:

CISv7 Basic



3.1.2. Basic CIS Controls - Ergebnisse und Empfehlungen

Die folgenden Empfehlungen für die **Muster AG** leiten sich aus den detaillierten Ergebnissen zu den sechs Basic CIS Controls ab:

Dringend				
Thema	Frage	Antwort	Empfehlung	Empfohlene Produkte
4. Kontrollierte Nutzung von Administratorrechten	Ist ein Prozess implementiert, durch den regelmässig für jede Person mit administrativen Rechten auf Servern, Desktops und Laptops diese Berechtigungen von übergeordneter Stelle überprüft werden?	Basic (1) Kein Prozess definiert	Implementieren Sie einen Prozess zur Genehmigung und regelmässigen Bestätigung von Berechtigungen für Admin-Accounts. Bereinigen Sie alte / nicht genutzte Accounts.	Azure Privileged Identity Management (PIM), Azure AD Access Review
5. Sichere Konfiguration von Hard- und Software auf mobilen Geräten, Laptops, Workstations und Servern	Verfügt die Organisation über eine implementierte sichere Hardening-Baseline für alle neuen Systeme? Werden alte NTLM- und SMB- und andere sicherheitsrelevante Registry-Schlüssel deaktiviert?	Basic (1) Nicht implementiert	Definieren Sie Hardening-Vorgaben für die wichtigsten Systeme, wobei diese standardmässig so weit wie möglich abgeschlossen sein sollten.	Azure VMs, Azure CIS Hardened Images, Microsoft Endpoint Manager
6. Pflege, Überwachung und Analyse von Log-Dateien	Kontrolliert und analysiert ein Sicherheits-Experte die Protokolle und Benachrichtigungen, um Anomalien aufzuspüren?	Basic (1) Kein Prozess definiert	Implementieren Sie einen Prozess zur Überwachung der Logs mit einer regelmässigen Überprüfung auf kritische sicherheitsrelevante Einträge.	



Sehr wichtig				
Thema	Frage	Antwort	Empfehlung	Empfohlene Produkte
1. Bestandsaufnahme und Kontrolle der Hardware-Assets	Ist eine Lösung für die Zutrittskontrolle auf Netzwerkebene (802.1x, NAC) implementiert, die Zertifikate fordert, um Geräte zu authentifizieren, bevor sie sich mit dem Netzwerk verbinden können?	Standardized (2) In begrenztem Umfang implementiert oder Implementierung einer Access Control Solution auf Port-Ebene ohne Zertifikate	Übernehmen Sie den 802.1x-Standard, um Geräte zu authentifizieren, bevor sie sich mit dem Netzwerk verbinden.	Microsoft Endpoint Manager, 802.1x
2. Bestandsaufnahme und Kontrolle der Software-Assets	Sind Discovery-Tools implementiert, um alle Software-Anwendungen in der gesamten Infrastruktur der Organisation zu identifizieren?	Standardized (2) In begrenztem Umfang implementiert	Erweitern Sie den Umfang des/der Discovery-Tools auf die gesamte IT-Infrastruktur.	Software Asset Management (SAM)-Tooling, Microsoft Endpoint Manager, Azure Security Center, Cloud App Security, Microsoft Defender ATP
3. Kontinuierliches Schwachstellen-Management	Sind Discovery-Tools implementiert, die Schwachstellen in Software auf den Systemen innerhalb der Infrastruktur der Organisation identifizieren?	Standardized (2) In begrenztem Umfang implementiert	Weiten Sie den Vulnerability Scan auf alles System aus.	Microsoft Endpoint Manager, Microsoft Defender ATP, Azure Security Center, Cloud App Security
5. Sichere Konfiguration von Hard- und Software auf mobilen Geräten, Laptops, Workstations und Servern	Sind Discovery-Tools implementiert, die in der Infrastruktur auf sämtlichen Systemen der Organisation nach falschen Sicherheits-Konfigurationen suchen?	Standardized (2) In begrenztem Umfang implementiert	Weiten Sie das Configuration Management auf die gesamte IT-Infrastruktur aus.	Microsoft Endpoint Manager, Microsoft Defender ATP, Azure Security Center, Cloud App Security
6. Pflege, Überwachung und Analyse von Log-Dateien	Sind alle Geräte und Server, einschliesslich Domain Controllern, Firewalls, Netzwerk-basierten IPS und Inbound und Outbound Proxies, so aufgesetzt und konfiguriert, dass sämtlicher Datenverkehr (sowohl erlaubter als auch blockierter) und fehlgeschlagene Anmeldungen ausführlich protokolliert werden? Werden Logs zentral abgelegt, gegen Manipulation gesichert und verwendet, um ständig verdächtige Aktivitäten aufzuspüren und zu melden?	Standardized (2) Auf einigen Netzwerk-Geräten implementiert	Legen Sie die Protokolle aller Geräte auf der zentralen Plattform ab. Verwenden Sie eine SIEM-Lösung zum Aggregieren der Daten aus allen Quellen die lokal oder in der Cloud ausgeführt werden, einschliesslich Benutzern, Anwendungen, Servern und Geräten.	Azure Sentinel, Azure Security Center, Azure Advanced Threat Protection (ATP), Microsoft Cloud App Security



Punkt 5 – Discovery Tools

Anhand der Befragung kann festgehalten werden, dass die Muster AG eine Vielfalt von heterogenem Server betreibt. Die Vielfalt ist derart gross, dass die Konfigurationen manuell gemacht werden. Als Konsequenz ist der Aufwand in der IT pro Mitarbeiter hoch und abhängig der Vorgaben der jeweiligen Owner's. Indirekt auch Apps Lieferant. → **Fachabteilungen zukünftig mehr dem Gewicht legen sollten. (Verantwortung der eigenen Applikation inkl. Details) für Drittsysteme sollte analog zu SAP (SAP-Basis) ein Verantwortlicher bestimmt sein. Falls Admin Rechte angefordert werden, muss sich der Zuständige durchführende Tätigkeiten bewusst sein.**

Empfehlung

Dem Prozess-Owner einer Fachabteilung muss die Verantwortung bewusst werden. Dh. Ein Awareness Training ist zwingend für alle Fachabteilungen durchzuführen. Ein Verantwortlicher muss im Unternehmen für diese Tätigkeit bestimmt werden und qualifiziert sein.

Punkt 6

Hintergrund:

Logs werden nur im Supportfall angeschaut.

Externe Zugriffe wie: Outlook WebAccess und VDI, werden analog protokolliert, und somit nicht aktiv protokolliert.

Pflege und Überwachung von Log-Dateien:

Hierbei werden Log-Informationen aus unterschiedlichen Quellen analysiert und ausgewertet. Zusatzparameter wie der zeitliche Zusammenhang fließen in die Auswertung mit ein. Ein einfaches Beispiel verdeutlicht den Nutzen der Korrelation:

Wenn Anwender sich remote mit einem falschen Passwort an einer geschützten Website anmelden, sind die daraus resultierenden Informationen im Ereignisprotokoll und im Router an sich nicht erwähnenswert. Mehrere falsche Anmeldungen innerhalb einer Minute hingegen können ein Indiz für eine versuchte Attacke sein. Die Korrelation in einem SIEM (Security und Event Management) erkennt solche Attacken quasi in Echtzeit und alarmiert die Verantwortlichen oder unterbricht die Verbindung der Website zum öffentlichen Netz, um so die Attacken zu unterbinden.

Gründe und Vorteil

Es ist aus Anwendersicht wünschenswert, dass die wichtigsten Grundregeln von der Log-Management-respektive SIEM-Lösung mitgeliefert werden, da das Erstellen von Regeln zur Log-Korrelation durchaus einige Zeit in Anspruch nimmt. Mithilfe eines Log-Managements lassen sich auch die Compliance-Anforderungen überwachen und vordefinierte Regeln erleichtern.



3.2. Foundational CIS Controls

Die Foundational CIS Controls fokussieren hauptsächlich auf die technische Sicherung von IT-Assets in der gesamten IT-Umgebung und auf das Erkennen von Bedrohungen. Die zehn Foundational CIS Controls und deren Ziele sind:

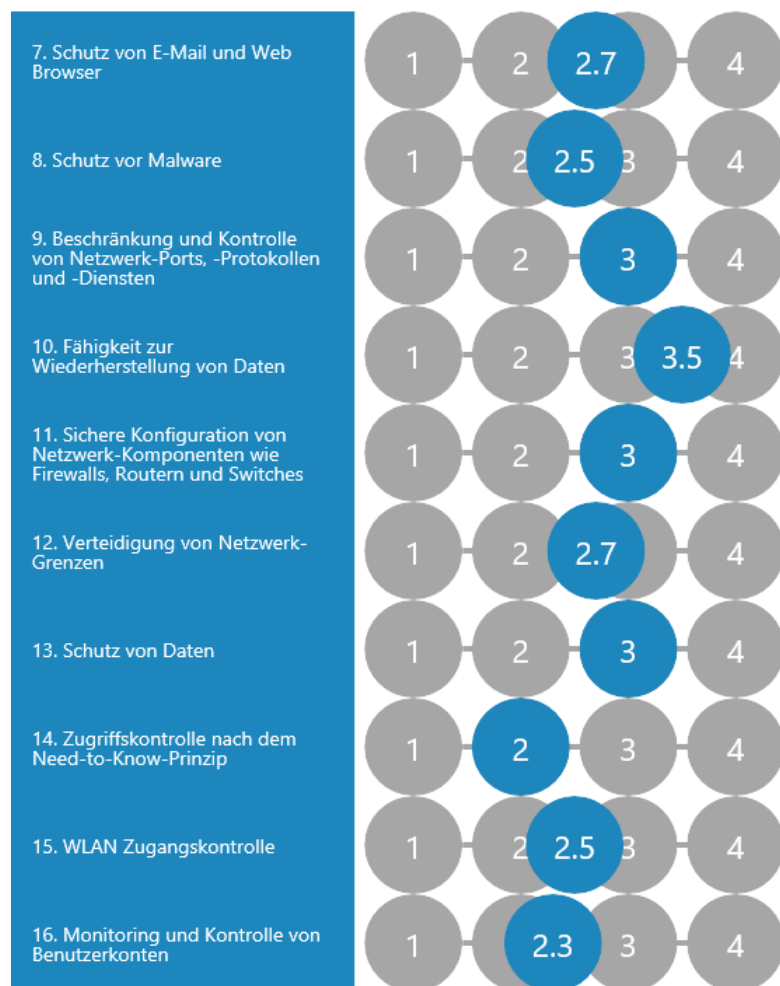
Thema	Ziel
7. Schutz von E-Mail und Web Browser	Minimieren der Angriffsfläche und der Möglichkeiten für Angreifer, menschliches Verhalten mittels Web-Browser und E-Mail-Systemen zu manipulieren.
8. Schutz vor Malware	Kontrolle der Installation, Verbreitung und Ausführung von böartigem Code an mehreren Stellen im Unternehmen. Nutzung und Optimierung von Automatismen, die eine schnelle Aktualisierung der Schutzmassnahmen, Sammeln von Informationen und korrigierende Aktionen ermöglichen.
9. Beschränkung und Kontrolle von Netzwerk-Ports, -Protokollen und -Diensten	Verwaltung (verfolgen / kontrollieren / korrigieren) der laufenden operativen Nutzung von Ports, Protokollen und Diensten auf vernetzten Geräten, um die für Angreifer verfügbaren Schwachstellen zu minimieren.
10. Fähigkeit zur Wiederherstellung von Daten	Prozesse und Werkzeuge, um kritische Informationen zu sichern und mit einer geprüften Vorgehensweise zeitnah wiederherstellen zu können.
11. Sichere Konfiguration für Netzwerkgeräte wie Firewalls, Router und Switches	Rigore Prozesse für das Konfigurations- und Änderungsmanagement von Netzwerk-Infrastruktur-Geräten zusammen mit einer aktiven Verwaltung (verfolgen, berichten, korrigieren) um zu verhindern, dass Angreifer sich gefährdete Dienste und Einstellungen zu Nutze machen.
12. Verteidigung von Netzwerk-Grenzen	Erkennen / Verhindern / Korrigieren des Datenflusses in informationsübertragenden Netzwerken unterschiedlicher Vertrauensstufen mit einem Schwerpunkt auf sicherheitsschädlichen Daten.
13. Datenschutz	Prozesse und Werkzeuge zur Verhinderung von Datenverlust verringern die Auswirkungen verlorener Daten und stellen Schutz und Integrität von sensiblen Informationen sicher.
14. Zugriffskontrolle nach dem Need-to-Know-Prinzip	Prozesse und Werkzeuge, um den sicheren Zugriff auf kritische Assets (z.B. Informationen, Ressourcen, Systeme) zu verfolgen / kontrollieren / verhindern / korrigieren. Basis ist die formale Definition welche Personen, Computer und Anwendungen die Notwendigkeit und das Recht haben, auf diese kritischen Assets gemäss einer genehmigten Klassifikation zuzugreifen.
15. Wireless Access Control	Prozesse und Werkzeuge, um die sichere Verwendung von drahtlosen lokalen Netzwerken (WLANs), Accesspoints und WLAN-Client-Systemen zu verfolgen / kontrollieren / verhindern / korrigieren.
16. Monitoring und Kontrolle von Benutzerkonten	Aktive Verwaltung des gesamten Lebenszyklus von System- und Anwendungs-Accounts (Anlage, Nutzung, Dormanz, Löschen), um die Möglichkeit zu minimieren, dass Angreifer diese nutzen.



3.2.1. Foundational CIS Controls - Sicherheitsbewertung

Grundlage der Bewertung sind Einschätzungen auf Basis der Ziele der einzelnen Foundational CIS Controls. Aus den Einschätzungen für die **Muster AG** zu den Positionen der Controls ergibt sich aggregiert das Rating:

CISv7 Foundational





3.2.2. Foundational CIS Controls - Ergebnisse und Empfehlungen

Die folgenden Empfehlungen für die **Muster AG** leiten sich aus den detaillierten Ergebnissen zu den zehn Foundational CIS Controls ab:

Sehr wichtig				
Thema	Frage	Antwort	Empfehlung	Empfohlene Produkte
7. Schutz von E-Mail und Webbrowser	Sind Netzwerk-basierte URL-Filter (inkl. DNS Filtering) implementiert, die Systeme daran hindern, Websites zu laden, die nicht von der Organisation genehmigt sind?	Standardized (2) Für einige Systeme implementiert	Stellen Sie sicher, dass der Proxy-Server / die IPS-Lösung von allen Systemen Ihrer IT-Infrastruktur genutzt wird.	Microsoft Defender ATP, Proxy-Server / IPS-Lösung
8. Schutz vor Malware	Werden Antivirus-Ereignisse zentral protokolliert mit Benachrichtigung an die IT, so dass Massnahmen ergriffen werden können?	Standardized (2) Für einige Systeme implementiert	Speichern Sie die AV-Logs zentral und nutzen Sie Benachrichtigungen, um Erkenntnisse zu gewinnen. Spüren Sie Trends auf.	Microsoft Defender ATP, Azure Security Center, Cloud App Security
12. Verteidigung von Netzwerk-Grenzen	Werden Systeme mit unterschiedlichen Aufgaben und Zugangs-Ebenen mittels Netzwerk-Segmentierung getrennt?	Rationalized (3) Alle Systeme sind mittels Rollen und Restriktionsstufen getrennt.	Implementieren Sie Firewalls, um den ein- und ausgehenden Traffic zwischen den Segmenten zu kontrollieren.	
12. Verteidigung von Netzwerk-Grenzen	Sind an allen Schnittstellen nach aussen Firewalls und netzwerk-basierte Intrusion Detection/Prevention Systeme (IDS / IPS) implementiert, die Angriffe und bösartigen Traffic erkennen und blockieren?	Standardized (2) Grundlegende Firewalls sind implementiert	Aktivieren Sie wenn möglich die Deep Packet Inspection (DPI) und Intrusion Detection/Prevention Funktionalität der Firewall. Andernfalls überlegen Sie, die Firewall durch ein besseres Modell zu ersetzen. Sorgen Sie dafür, dass Sie über verdächtige Aktivitäten benachrichtigt werden.	Firewall mit IDS/IPS
12. Verteidigung von Netzwerk-Grenzen	Erfordert jede Anmeldung von aussen die Verschlüsselung des Datenverkehrs und Multi-Faktor-Authentifizierung?	Rationalized (3) Verschlüsselung und MFA sind für alle Anmeldungen von ausserhalb implementiert und erzwungen.	Erzwingen Sie für alle Systeme bedingten Zugriff bei Anmeldung von ausserhalb.	Azure Multi-Factor Authentication (MFA)
13. Schutz von Daten	Werden Bewertungen von Daten durchgeführt, um sensible Informationen zu identifizieren, die Verschlüsselung und Prüfungen der Integrität erforderlich machen. Werden Klassifizierung und Kennzeichnung für alle sensiblen Dokumente durchgeführt?	Rationalized (3) Für alle Systeme implementiert	Wenden Sie Klassifizierung und Kennzeichnung an. Automatisieren Sie das Aufspüren von sensiblen Daten mittels Werkzeuge.	Azure Information Protection Scanner, Data Loss Prevention, Office 365 Advanced Data Governance, Azure Information Protection P2
14. Zugriffskontrolle nach dem Need-to-Know-Prinzip	Ist für alle Kommunikation von sensiblen Daten über weniger vertrauenswürdige Netzwerke die Verschlüsselung während der Übertragung implementiert?	Standardized (2) Für einen Teil der Netzwerk-Kommunikation umgesetzt	Aktivieren Sie Verschlüsselung für alle Kommunikation mit externen / öffentlichen Netzwerken. Für sensible Daten auch in internen Netzwerken.	Office 365 verwendet SSL/TLS für die Datenübertragung.
15. WLAN-Zugangskontrolle	Sind WLAN-Gastnetzwerke vom Unternehmensnetzwerk getrennt?	Standardized (2) Eingerichtet, aber nicht physisch von den Geräten der Firma getrennt.	Trennen Sie das Gast-WLAN physisch von den von aussen sichtbaren Geräten der Organisation. Weisen dem Gast-WLAN eine eigene Internetverbindung/VLAN zu.	



Zugriffskontrollen:

Das Beispiel von SAP mit Personaldaten; Es wird eine Liste per Mail versendet, die Erkennung und Unterbindung ist in der IT nicht möglich und muss händisch angepasst werden. Zusätzlich sind die Mails offen. **Beispiel:**

Personaleintritte über die Dritt-Firma (Neue Mitarbeiter werden hinzukommen und Mitarbeiter verlassen das Unternehmen. Hier stellen wir fest, dass der Prozess beziehungsweise Prozess verbessert werden muss. User sind zum Teil aktiv und belegen Lizenzen, obschon diese das Unternehmen in der Zwischenzeit verlassen haben. Die IT hängt dem Prozess hinten nach und ist demzufolge nie auf dem aktuellsten Stand. Dies bedingt auch gewisse Lücken in der Sicherheit solange der Prozess nicht klar definiert und kontrolliert werden.

Vorschlag: Definieren Sie den Prozess bei Austritten mit klaren Regelungen mit der externen Firma (XX) bis wann es gemeldet werden soll und mit einer Verantwortlichkeit (Zuständigkeitsbereich).

Beispiel mit den jeweiligen Mitarbeitern welche nicht zeit gerecht gemeldet wurden.

Anmeldename für ...	Name	Typ	Beschreibung	E-Mail-Adresse
FialJoA		Benutzer	Kreditoren Ausgelagert nach	
JasiuAga		Benutzer	Kreditoren Ausgelagert nach	
JemieAnn		Benutzer	Kreditoren Ausgelagert nach	
KapkaMag		Benutzer	Kreditoren Ausgelagert nach	
KwasnAgn		Benutzer	Debitoren Ausgelagert nach	
MazikAgn		Benutzer	Debitoren Ausgelagert nach	
MentriMar		Benutzer	Debitoren Ausgelagert nach	
MolawAga		Benutzer	Kreditoren Ausgelagert nach	
NiemcMag		Benutzer	Kreditoren Ausgelagert nach	
PiaseAnn		Benutzer	Kreditoren Ausgelagert nach	
PrzybPat		Benutzer	Debitoren Ausgelagert nach	
StaliDom		Benutzer	Kreditoren Ausgelagert nach	
SzatkaAnd		Benutzer	Debitoren Ausgelagert nach	
TekieDaw		Benutzer	Kreditoren Ausgelagert nach	

Dies gilt aber auch für externe Mitarbeiter:

		Typ	
Bielefeld		Benutzer	
Externe Agenten (Ohne Mail und ohne O365)		Benutzer	
Externe Dienstleister		Benutzer	
Externe Dienstleister (Ohne Mail und ohne O365)		Benutzer	
Atoss PEP Support		Benutzer	
generisch		Benutzer	
IT Systems		Benutzer	
PWC		Benutzer	
SAP-PEP Support		Benutzer	

Grundsätzlich funktioniert es in der Firma bei Ein-/Austritten, wenn diese indirekt über HR kommen, und es eine der Ländergesellschaften betrifft, die im SAP-HR geführt wird.

Als kritische Prozesse sind die Ländergesellschaften, die nicht im SAP-HR geführt werden zu betrachten, wie:

- Muster Filiale France
- Muster Filiale Portugal
- Muster Filiale Russland
- und andere
- auch externen Dienstleistern, egal welcher Art

Fazit: die IT übernimmt Aufgaben durch zufällige Rückfragen und versucht dem entgegenzuwirken und die Risiken zu minimieren, hierfür wird, aber Zeit aufwendet welche grundsätzlich den jeweiligen Prozessverantwortlichen / Vorgesetzten obliegen sollten.

Definieren Sie die Verantwortung klar mit entsprechenden Regeln und Definitionen.



3.3. Organizational CIS Controls

Die Organizational CIS Controls beziehen sich auf Prozesse und Abläufe der Organisation. Diese Controls werden um zwei High-Level-Controls (AD.1 und AD.2) aus dem ISO/IEC 27001:2013 Framework ergänzt. Die Fragen hierzu beziehen sich auf IT- und Data Governance und umfassen die Bereiche Richtlinien, Compliance, Risikomanagement und Datenschutz. Die vier Organizational CIS Controls mit den zwei ISO/IEC 27001: 2013 Controls und ihre Zielsetzung sind:

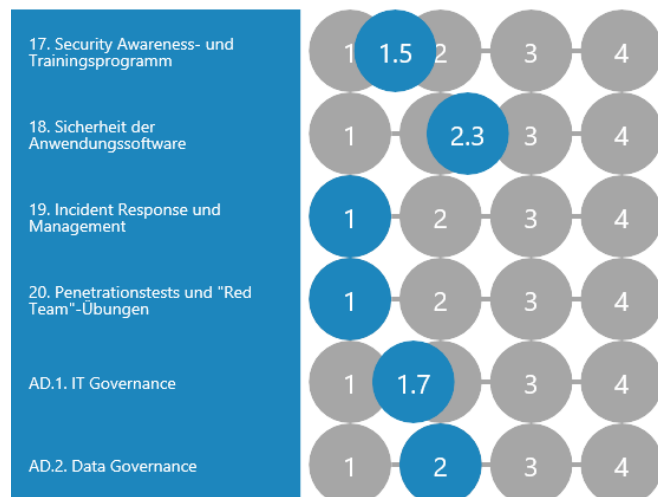
Thema	Ziel
17. Security Awareness- und Trainingsprogramm	Identifikation spezifischer Kenntnisse, Fähigkeiten und Fertigkeiten für alle Funktionen in der Organisation, die zur Unterstützung der Verteidigung des Unternehmens benötigt werden, beginnend mit den Funktionen, die für das Geschäft und die Sicherheit am wichtigsten sind. Entwicklung eines integrierten Plans, um organisatorische Richtlinien, Planung, Trainings und Sensibilisierungs-Programme zu beurteilen, sowie Lücken zu identifizieren und zu beheben.
18. Application Software Security	Verwaltung des Sicherheits-Lebenszyklus für alle in-house entwickelte oder erworbene Software, um Schwachstellen zu verhindern oder zu erkennen und zu korrigieren.
19. Incident Response und Management	Schutz der Unternehmensdaten - und des Rufs des Unternehmens - durch die Entwicklung und Umsetzung einer Incident-Response-Infrastruktur (z. B. Pläne, definierten Rollen, Ausbildung, Kommunikation, Übersichten für das Management), um Angriffe schnell zu entdecken und dann wirksame Schadensbegrenzung zu betreiben, den Angreifer zu entfernen und die Integrität des Netzwerks und der Systeme wiederherzustellen
20. Penetrationstests und "Red Team"-Übungen	Test der Gesamtstärke der Abwehrmassnahmen eines Unternehmens (Technologie, Prozesse und Menschen) indem Ziele und Aktionen eines Angreifers simuliert werden
AD.1. IT Governance	Schaffung organisatorischer Transparenz und Orientierung durch die Schaffung eines Sicherheits- und Datenschutz-Rahmenkonzepts unter Einhaltung der regulatorischen und rechtlichen Anforderungen an die Organisation.
AD.2. Data Governance	Umsetzung gesetzlicher Datenschutzanforderungen über einen risikobasierten Ansatz, mit Fokus auf dem Schutz personenbezogener Daten (PII).

3.3.1. Organizational CIS Controls - Sicherheitsbewertung

Grundlage der Bewertung sind Einschätzungen auf Basis der Ziele der einzelnen Organizational CIS

Controls und der Zusätze AD.1 und AD.2. Aus den Einschätzungen für die **Muster AG** zu den Positionen der Controls ergibt sich aggregiert das Rating:

CISv7 Organizational





3.3.2. Organizational CIS Controls - Ergebnisse und Empfehlungen

Die folgenden Empfehlungen für die Muster **AG** leiten sich aus den detaillierten Ergebnissen zu den vier Organizational CIS und zwei zusätzlichen Controls ab:

Dringend				
Thema	Frage	Antwort	Empfehlung	Empfohlene Produkte
17. Security Awareness- und Trainingsprogramm	Gibt es ein Trainingsprogramm zur Sensibilisierung für IT-Sicherheit über sichere Logins, Social Engineering, den Umgang mit sensiblen Daten, ungewollte Offenlegung von Daten und Identifikation von und Benachrichtigung bei Sicherheits-Vorfällen?	Basic (1) Kein Trainingsprogramm	Setzen Sie ein grundlegendes Trainingsprogramm für die wichtigsten Rollen Ihrer Organisation auf.	Ein Beispiel könnte Proof Point sein.
19. Incident Response und Management	Ist eine Prozedur zur Reaktion auf Sicherheits-Vorfälle (Incident Response Procedure) definiert mit den passenden Benachrichtigungen, Zusammenstellung von Daten, Verantwortlichkeiten, gesetzeskonformen Protokollierungen und Kommunikations-Strategie?	Basic (1) Keine Prozedur definiert	Setzen Sie eine grundlegende Incident Response Procedure auf, die die häufigsten Szenarien abdeckt. Trainieren und leben Sie diesen Prozess	Office 365 Advanced Compliance: Advanced eDiscovery
20. Penetrationstests und "Red Team"-Übungen	Werden Tools für Vulnerability Scans und Penetration Tests zusammen eingesetzt?	Basic (1) Nicht implementiert	Implementieren Sie einen Vulnerability Scanner in der IT-Infrastruktur der Organisation und verwenden diesen als Input für Penetration Tests.	Microsoft Endpoint Manager, Defender ATP, Azure Security Center + Pen testing tools
AD.1. IT Governance	Wie ist die Trennung von Pflichten, Aufgaben und Verantwortlichkeiten geregelt?	Basic (1) Die Trennung von Pflichten, Aufgaben und Verantwortlichkeiten erfolgt informell.	Formalisieren Sie die Trennung von Pflichten, Aufgaben und Verantwortlichkeiten, indem Sie eine Rollen-Matrix definieren.	
AD.2. Data Governance	Wird Data Risk Management auf allen Ebenen der Organisation durchgeführt?	Basic (1) Kein Risk Management oder keine Bewertung	Führen Sie einen grundlegenden Risk Management Prozess ein.	Microsoft Compliance Manager (ermöglicht Workflow-basierte Risikobewertungen)

Sehr wichtig				
Thema	Frage	Antwort	Empfehlung	Empfohlene Produkte
17. Security Awareness- und Trainingsprogramm	Ist ein Sicherheits- und Datenschutzprogramm etabliert?	Standardized (2) Es gibt ein einfaches Programm zur Sensibilisierung für IT-Sicherheit und Datenschutz, aber ohne technische Unterstützung.	Erweitern Sie das Programm zur Sensibilisierung für IT-Sicherheit und Datenschutz um für das Unternehmen und seine Branche relevante Themen. Verknüpfen Sie	



Sehr wichtig				
			die Inhalte dieses Programms mit technischen Hilfsmitteln und schulen Sie diese.	
18. Sicherheit der Anwendungssoftware	Ist eine sichere (interne) Entwicklung von Anwendungen, Makros, Skripten und sonstigen Workflows oder Anpassungen sichergestellt?	Standardized (2) Für einzelne Eigenentwicklungen umgesetzt	Starten Sie einen Code Review (oder führen Sie Werkzeuge dazu ein) für alle Eigenentwicklungen in Ihrer Organisation.	Code Review Solution
18. Sicherheit der Anwendungssoftware	Ist der Zugriff auf produktive Systeme für Entwickler streng limitiert oder komplett unterbunden?	Standardized (2) Für einige Systeme implementiert	Schränken Sie für Entwickler den Zugang zu allen produktiven Systemen ein.	
20. Penetrationstests und "Red Team"-Übungen	Werden regelmässig Penetrations-Tests auf allen Unternehmenssystemen durchgeführt?	Basic (1) Nicht oder nur bei Bedarf durchgeführt	Beauftragen Sie einen externen Spezialisten für dieses Thema mit der Durchführung eines Penetration Tests der von aussen sichtbaren Systemen der Organisation.	
AD.1. IT Governance	Gibt es eine Sicherheits- und Datenschutzrichtlinie, die vom Management definiert und durchgesetzt wird?	Standardized (2) Eine grundlegende Policy zu Sicherheit und Datenschutz ist definiert.	Erweitern Sie die Policy zu Sicherheit und Datenschutz um branchenspezifische Themen und vereinheitlichen Sie sie in der ganzen Organisation.	
AD.1. IT Governance	Wird die regulatorische und gesetzliche Compliance fortlaufend überprüft und sichergestellt?	Standardized (2) Lokale legislative und regulatorische Anforderungen sind umgesetzt und werden regelmässig überprüft.	Setzen Sie branchenspezifische Best Practice Ansätze um.	Microsoft Compliance Manager
AD.2. Data Governance	Werden von der gesamten Organisation Datenklassifizierung und -kennzeichnung für alle Dokumente durchgeführt?	Standardized (2) Eine Policy zur Klassifizierung ist umgesetzt. Die Kennzeichnung wird in den wichtigsten Systemen angewendet.	Wenden Sie Datenklassifizierung und -kennzeichnung in allen Systemen an.	Azure Information Protection Scanner, Data Loss Prevention, Azure Information Protection P2

Security Awareness Training

Mit einem Security Awareness Training schaffen Sie die Voraussetzungen, dass ein hohes Mass an Datenschutz und IT-Sicherheit erreicht werden kann, durch sensibilisierte und geschulte Mitarbeiter. In einem ersten Schritt erfolgt das Bewusstmachen möglicher Gefahren, gefolgt vom richtigen Umgang mit diesen potenziellen Bedrohungen. Allen Mitarbeitern sollte nach der Absolvierung des Security Awareness Trainings bekannt sein, was von ihnen, im Hinblick auf IT-Sicherheit erwartet wird und wie sie in sicherheitskritischen Situationen reagieren sollten.

Lösungsvorschlag:

Ein Trainingskonzept ermöglicht eine zeiteffiziente Schulung durch eine Kombination verschiedener Trainingsvarianten und Inhalte auf einer E-Learning-Plattform. Die realitätsnahe Anpassung an Gegebenheiten und Anforderungen ihres Unternehmens ermöglicht eine schnelle Identifikation mit dem Thema. Die Wirksamkeit des Security Awareness Trainings wird beispielsweise mit einer geplanten Phishing-Kampagne überprüft.



Test mit ausgewählten Mitarbeitern

Unser Einführungspaket beinhaltet sämtliche Dienstleistungen, damit Sie und Ihre Mitarbeiter (max. 30 Mitarbeiter) auf die Security Awareness Trainings Plattform zugreifen können. Die Demo-Phase erlaubt Ihnen während eines Monats, respektive 30 Tage, den Zugriff und die Nutzung der Security Awareness Trainings Plattform.

Vorschlag zu einer Herangehensweise:

- Aufschaltung von bis zu 30 Mitarbeitern auf einer Demo-Plattform. Die Mitarbeiterdaten werden in Form einer CSV-Datei vom Kunden angeliefert.
- Abbildung Ihrer aktuellen Unternehmens-Passwort-Policy, falls diese vom Kunden zur Verfügung gestellt wird.
- Grundkonfiguration der Demo-Plattform mit Einbindung Kundenlogo, Zeitzone, Benachrichtigungen in Deutsch oder Englisch und Einrichtung der Support-Mailadresse.
- Erstellung und Versand einer Phishing-Mail an die erfassten Mitarbeiter
- Nach 5 Tagen werden die Resultate aus der Phishing-Kampagne analysiert und der Schulungsbedarf und die Trainings-Module bestimmt.
- Interne Information an die erfassten Mitarbeiter über Teilnahme am Schulungsprogramm und Aufschaltung von 1-2 Trainings-Modulen, welche innerhalb von 10 Arbeitstagen durchgearbeitet werden sollen.
- Nach Ablauf der Trainingseinheiten erfolgt die Erstellung und Versand einer zweiten Phishing-Mail, um zu prüfen, ob sich die Situation verbessert hat.
- Abschliessend erfolgen **eine Nachbesprechung, ein Erfahrungsaustausch und Bestimmung weiteres Vorgehen.**

IT Governance:

Die festgelegten Richtlinien zu Sicherheit und Datenschutz müssen zusammen mit den abgeleiteten operativen Abläufen dokumentiert werden. ISO/IEC 27001: A.5.1.1 / A 5.1.2 / A.12.1.1. Sie die Muster AG hat die Richtlinien definiert aber noch nicht komplett umgesetzt. Wir empfehlen einen Verantwortlichen / Owner zu bestimmen, damit diese in einem angemessenen Zeitraum umgesetzt werden.

Wichtig:

Die Trennung von Pflichten, Aufgaben, Verantwortlichkeiten und Benachrichtigungsketten sollte für die ganze Organisation etabliert und dokumentiert sein. Diese ist derzeit, Stand Oktober / November 2020 nicht gegeben. Das Unternehmen ist 27001 konform, aber nicht geschult. Schriftlich ist es nicht festgehalten, die IT arbeitet nach bestem und gewissen und handelt danach. Für Notfälle sind Kommunikationsverhalten und Pläne vorhanden, durch Fluktuation könnten diese Pläne für Notfallnummern und Kommunikation zwar zum Einsatz kommen, die Frage nach der Bekanntheit des Kommunikationsplans und das Verhalten ist zu prüfen.

Grund:

Notfallnummern sind festgelegt und abgelegt. Der Notfall wurde aber nie durchgespielt

Die regulatorischen und gesetzlichen Anforderungen an die Organisation sind festgehalten und werden zweijährig geprüft. Die Verantwortung obliegt hierbei legal.



4. Gescannte Daten und deren Analyse

Dies ist eine auf Fakten basierende Zusammenfassung der aus der IT-Umgebung der **Muster AG** gescannten (Sicherheits-)Daten.

Diese Informationen wurden mit dem Cyber Security Assessment Tool (CSAT) gesammelt.

4.1.1. CIS-Control 1: Bestandsaufnahme und Kontrolle der Hardware-Assets

Keine gescannten Daten aus CSAT; Empfehlungen sind unter "Basic CIS Controls – Ergebnisse und Empfehlungen" zu finden.

Inventarisierung	Typ	Anzahl	Gesamt
Physische Server	Total Server	232	
	Wind Server 2003 Std.	10	
	Win Server 2008 R2 Std	2	
	Win Server 2012 R2 Std	92	
	Win Server 2012 R2 DC	4	
	Win Server 2016 Std	7	
	Win Server 2019 Std	31	
	Win Server 2019 DC	19	
	Linux oder andere		
Endanwender-Geräte	Total Windows	578	
	Windows 10 Ent.	511	
	Windows 8.1 Ent.	67	

Analyse und Empfehlungen:

- Mobile Geräte werden zukünftig mittels Intune verwaltet?
- Für mobile Geräte gibt es kein Tool, über das sie verwaltet würden.

➔ Endanwender auf W10 in 754 Total, davon

- Kassen auf W8.1, Kassen Lifecycle, anhand der Corona Situation werden die Kassen demnächst migriert bzw. abgelöst (10 davon bereits im Einsatz)



4.1.2. CIS-Control 2: Bestandsaufnahme und Kontrolle der Software-Assets

Ausgabe CSAT – Status Betriebssysteme

OS ERMITTELTE ENDPUNKTE

Microsoft Windows 10 Enterprise	519
Microsoft Windows 10 Enterprise	4
Microsoft Windows 8.1 Enterprise	67
Microsoft Windows Server 2008 R2 Standard	2
Microsoft Windows Server 2012 R2 Datacenter	5
Microsoft Windows Server 2012 R2 Standard	94
Microsoft Windows Server 2016 Standard	7
Microsoft Windows Server 2019 Datacenter	17
Microsoft Windows Server 2019 Standard	33
Microsoft Windows XP Professional	10
Microsoft(R) Windows(R) Server 2003 Standard Edition	10

INTUNE-GERÄTE

AD Computer	5
Intune-Geräte, 30 Tage aktiv	0
Intune-Geräte, 30 Tage inaktiv	5

Ausgabe CSAT - AD Computerkonten

AD COMPUTER ACCOUNT (ENABLED COMPUTER ACCOUNT) - NTDOMSTR

Aktivierte Accounts	1048
Deaktivierte Accounts	0
Client OS aktiv in den letzten 30 Tagen	821
Server OS aktiv in den letzten 30 Tagen	177
Client OS mehr als 30 Tage inaktiv	50
Server OS mehr als 30 Tage inaktiv	0

Analyse und Empfehlungen:

Die folgenden end-of-life Betriebssysteme: Microsoft(R) Windows(R) Server 2003 Standard-Edition / Win Server 2008 Std. Edition, und Microsoft Windows 8.1 Enterprise wurden erfasst und sollten so schnell wie möglich ersetzt werden:

- Server: Win Server 2003 Std Ed. **Anzahl 10 (Umfeld CAD, Telefonie)**
- Server Win Server 2008 Std Ed. Anzahl 2 (1er migriert Seeburger Edifact Converter) → **erledigt (Hinweis Owner und Verantwortung zukünftig Awareness auf techn. Unterbauch und security issues aufmerksam machen)**
- Clients: Ms Windows 8.1 Ent. Anzahl 67, Ende des erweiterten Supportes 10. Januar 2023, sofern Update 1 installiert ist



CAD:



Hinweis: die DB Console wird abgeschaltet, Ende Q1 2021

STRADM Admin wird nur für IT Admin verwendet und wird deaktiviert auch XP und der 2003 Svr werden abgelöst.



emake, kein Verantwortlicher

–Etikettendrucker SAP, Verantwortung für die Ablösung muss anhand der Awareness gefördert werden

optiplan im Verbund mit CAD sh oben

note install service (vorgänger SCCM) wird noch gebraucht um XP/2003 aufzusetzen

– TF Apps Server, Vermittler

TF Apps Server, Musik, Sprache

Werden entfernt PEDI wird am 12.11. deaktiviert, QEDI ist deaktiviert



Geräte und Bezeichnungen

Client Win 8.1	Client Win 8.1	Win Server 2003	Win Server 2008

- Für Windows Server 2008 erhalten Sie erweiterten Sicherheitssupport, wenn Sie diese Betriebssysteme nach Azure verschieben.
- Erstellen Sie einen Plan, um diese Betriebssysteme abzulösen.

Aktualisierung der Windows 10 Clients



- Die auf mehreren Endpunkten verwendeten Versionen von Windows 10 sind nicht auf dem neuesten Stand. Die aktuelle Version von Windows 10 ist Build 2004. Aktualisieren Sie alle Endpunkte auf die neueste Version.

Patch Fokus auf 20H2 – **Q2 2021 auf Herbstrelease- vermutlich auf Patch „2009“**

Version	Servicing option	Availability date	OS build	Latest revision date	End of service: Home, Pro, Pro Education, Pro for Workstations and IoT Core	End of service: Enterprise, Education and IoT Enterprise
20H2	Semi-Annual Channel	2020-10-20	19042.630	2020-11-10	2022-05-10	2023-05-09
2004	Semi-Annual Channel	2020-05-27	19041.630	2020-11-10	2021-12-14	2021-12-14
1909	Semi-Annual Channel	2019-11-12	18363.1198	2020-11-10	2021-05-11	2022-05-10
1903	Semi-Annual Channel	2019-05-21	18362.1198	2020-11-10	2020-12-08	2020-12-08
1809	Semi-Annual Channel	2019-03-28	17763.1577	2020-11-10	2020-11-10	2021-05-11
1809	Semi-Annual Channel (Targeted)	2018-11-13	17763.1577	2020-11-10	2020-11-10	2021-05-11
1803	Semi-Annual Channel	2018-07-10	17134.1845	2020-11-10	End of service	2021-05-11
1803	Semi-Annual Channel (Targeted)	2018-04-30	17134.1845	2020-11-10	End of service	2021-05-11

Microsoft empfiehlt



Ausgabe CSAT – Installierte Anwendungen

Analyse und Empfehlungen:

9 kritische Java Installationen

Java Installationen	Anzahl
Java 7 Update 25 (64-bit)	1
Java 7 Update 45	1
Java 7 Update 65	1
Java 7 Update 9	1
Java DB 10.6.2.1	1
Java (TM) 6 Update 31	1
Java (TM) 6 Update 38	1
Java (TM) SE Development Kit 6 Update 38	1
MySQL Notifier 1.1.7	1

Threat	Name	Version	First installation date	Publisher	#endpoints
Normal	Java 7 Update 25 (64-bit)	7.0.250	07.09.2013	Oracle	2
Normal	Java 7 Update 45	7.0.450	12.05.2013	Oracle	1
Normal	Java 7 Update 65	7.0.650	09/28/2015	Oracle	1
Normal	Java 7 Update 9	7.0.90	10/14/2015	Oracle	1
Normal	Java 8 Update 201	8.0.2010.9	10.04.2019	Oracle Corporation	1
Normal	Java 8 Update 201 (64-bit)	8.0.2010.9	10.04.2019	Oracle Corporation	1
Normal	Java 8 Update 221 (64-bit)	8.0.2210.11	12.11.2019	Oracle Corporation	2
Normal	Java 8 Update 251	8.0.2510.8	06.12.2020	Oracle Corporation	582
Normal	Java 8 Update 251 (64-bit)	8.0.2510.8	06.12.2020	Oracle Corporation	580
Normal	Java Auto Updater	2.8.251.8	06.12.2020	Oracle Corporation	581
Normal	Java Auto Updater	2.8.221.11	12.11.2019	Oracle Corporation	2
Normal	Java Auto Updater	2.8.201.9	10.04.2019	Oracle Corporation	1
Normal	Java DB 10.6.2.1	10.6.2.1	01/17/2013	Oracle	1
Normal	Java SE Development Kit 8 Update 221 (64-bit)	8.0.2210.11	12.11.2019	Oracle Corporation	2
Normal	Java(TM) 6 Update 31	6.0.310	10/14/2015	Oracle	1
Normal	Java(TM) 6 Update 38	6.0.380	01/17/2013	Oracle	1
Normal	Java(TM) SE Development Kit 6 Update 38	1.6.0.380	01/17/2013	Oracle	1
Normal	MySQL Connector/ODBC 5.3	05.03.2004	05/14/2019	Oracle Corporation	62
Normal	MySQL Connector/ODBC 5.3	05.03.2010	06.06.2018	Oracle Corporation	7
Normal	MySQL Installer - Community	1.4.25.0	06.06.2018	Oracle Corporation	4
Normal	MySQL Notifier 1.1.7	01.01.2007	06.06.2018	Oracle	1
Normal	MySQL Server 5.6	05.06.1940	06.06.2018	Oracle Corporation	66
Normal	MySQL Workbench 5.2 CE	05.02.1944	11/29/2012	Oracle Corporation	1
Normal	MySQL Workbench 6.3 CE	06.03.2010	06.06.2018	Oracle Corporation	68
Normal	Oracle Data Provider for .NET Help	10.2.000	07/22/2011	Oracle Corporation	1

ATOSS, Seeburger, BI-Objects (SAP) (Maschinen sh Liste)



7-Zip

Die alten 18.5 Versionen auf 19.0 upgraden

Im Release 19.0 wurde die Grösse des zufällig generierten Initialisierungsvektors von bisher 64 Bit auf jetzt 128 Bit erhöht. Ausserdem wurde der Pseudo-Zufalls-Nummerengenerator verbessert. Daneben gibt es noch einige Fehlerkorrekturen. Die 5 unten aufgeführten müssen durch den Verantwortlichen **Owner gemanaged werden! Die Einheitlichkeit im Applikations-Management fehlt noch.**

Name	Version	First installation date	Publisher	#endpoints
7-Zip 18.05 (x64 edition)	18.05.00.0	07/20/2018	Igor Pavlov	5
7-Zip 19.00 (x64 edition)	19.00.00.0	06.11.2020	Igor Pavlov	584
tp.gzip-1.2.3-core-32	14.2.6.2839	09/17/2020	SAP Business	18

NET-Framework 2.0 und 3.5

Der Support für .NET-Framework 2.0 endete **am 12. Juli 2011**. Nach diesem Termin ist .NET 3.5 SP1 die einzige unterstützte Service Pack-Version. Wir empfehlen dringend, auf .NET-Framework 3.5 SP1 umzustellen unter Berücksichtigung der Laufzeit. (sh unten folgende)

Lebenszyklusdaten gelten für .NET 3.5 SP1, wenn Windows 10 Version 1809, Windows Server 2019 oder höher ausgeführt wird. In älteren Windows-Versionen übernimmt .NET 3.5 SP1 den Lebenszyklus des zugrunde liegenden Windows-Betriebssystems.

Der Support für die .NET-Framework 3.x-Versionen vor 3.5 SP1 endete am 12. Juli 2011. .NET 3.5 SP1 ist die einzige unterstützte Service Pack-Version nach diesem Datum. Das Enddatum für den grundlegenden Support endet am 10.10.2023. Das Enddatum für den erweiterten Support am 09.01.2029

Name	Version	First installation date	Publisher	#endpoints
Hotfix for Microsoft .NET Framework 3.5 SP1 (KB953595)	1		Microsoft Corporation	10
Hotfix for Microsoft .NET Framework 3.5 SP1 (KB958484)	1		Microsoft Corporation	10
Microsoft .NET Framework 2.0 Service Pack 2	2.2.30729	05/13/2015	Microsoft Corporation	9
Microsoft .NET Framework 2.0 Service Pack 2 Language Pack	2.2.30729	02.01.2009	Microsoft Corporation	9
Microsoft .NET Framework 3.0 German Language Pack			Microsoft Corporation	1
Microsoft .NET Framework 3.0 Service Pack 2	3.2.30729	05/13/2015	Microsoft Corporation	9
Microsoft .NET Framework 3.0 Service Pack 2 Language Pack	3.2.30729	02.01.2009	Microsoft Corporation	9
Microsoft .NET Framework 3.5 Language Pack SP1 - deu	3.5.30729	02.01.2009	Microsoft Corporation	9
Microsoft .NET Framework 3.5 Language Pack SP1 - DEU			Microsoft Corporation	10
Microsoft .NET Framework 3.5 SP1			Microsoft Corporation	10
Microsoft .NET Framework 3.5 SP1	3.5.30729	10.11.2013	Microsoft Corporation	9

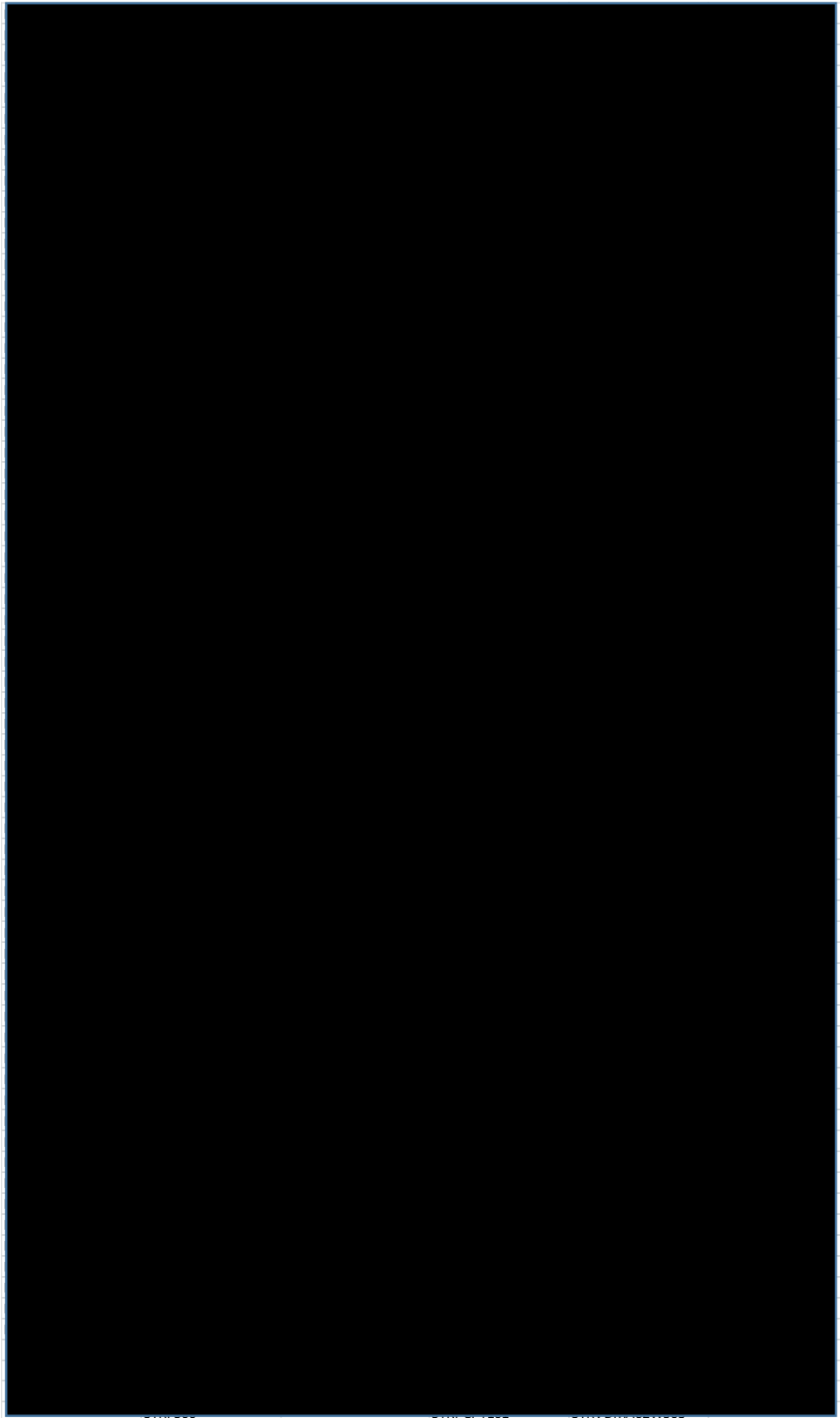


Bit Locker:

	Bit Locker	Microsoft Windows 10 Enterprise	Microsoft Windows 10 Enterprise	Microsoft Windows 8.1 Enterprise	Microsoft Windows Server 2008 R2 Standard	Microsoft Windows Server 2012 R2 Datacenter	Microsoft Windows Server 2012 R2 Standard	Microsoft Windows Server 2016 Standard	Microsoft Windows Server 2019 Datacenter	Microsoft Windows Server 2019 Standard	Microsoft(R) Windows(R) Server 2003 Standard Edition	Total der Geräte
aktiviert		400	3									403
keine Aktivierung		107	1	67	2	4	92	7	19	31	10	340
(Leer)												
Total der Geräte		507	4	67	2	4	92	7	19	31	10	743



Geräte ohne Bit Locker Aktivierung:





Mit AppLocker und/oder Windows Application Control oder Azure Security Center und Cloud App Security (für die Cloud) können Sie Anwendungen definieren, die in der Infrastruktur des Unternehmens installiert werden können.

Ausgabe CSAT – Lizenzen Office 365

Office 365 License Table				
Produkt	Konsumiert	Prepaid	Verfügbar	Status
MUSTER FILIALEAG.ONMICROSOFT.COM				
SKYPE FOR BUSINESS PSTN CONFERENCING	4	10	6	Enabled
POWERAPPS_VIRAL	10	10000	9990	Enabled
ENTERPRISEPACKWITHOUTPROPLUS	4	0	-4	Suspended
VISIO Online Plan 2	3	5	2	Enabled
MICROSOFT 365 E3	733	800	67	Enabled
STREAM	2	1000000	999998	Enabled
FLOW_PER_USER	1	1	0	Enabled
POWER BI PRO	0	5	5	Enabled
POWER_BI_STANDARD	6	1000000	999994	Enabled
OFFICE 365 PROPLUS	0	0	0	Suspended
FLOW_FREE	732	10000	9268	Enabled
SKYPE FOR BUSINESS CLOUD PBX	4	10	6	Enabled
CCIBOTS_PRIVPREV_VIRAL	1	10000	9999	Enabled
TEAMS_COMMERCIAL_TRIAL	734	0	-734	Enabled
TEAMS_EXPLORATORY	0	100	100	Enabled

Analyse und Empfehlungen:

Es wurden die folgenden nicht verwendeten Lizenzen gefunden:

6 Lizenzen Skype vor Business / 2 Vision Online, 5 Power BI, und Teams exploratory 100 verfügbar) - Weisen Sie diese Lizenzen Benutzern zu, um die Sicherheit zu erhöhen.

Rückbau Skype for Business. PoC Teams, direct routing, via Muster Filiale an Festnetz.



4.1.3. CIS-Control 3: Kontinuierliches Schwachstellen-Management

Ausgabe CSAT – Status Updates

Endpunkte mit fehlenden kritischen Updates

1

EndpointName	Critical	Important	Moderate	Low	Other
	1	0	0	0	1
	0	0	0	0	4

Analyse und Empfehlungen:

- Es wurden **1** Endpunkte mit fehlenden kritischen Sicherheitspatches gefunden. Rollen Sie die verfügbaren Sicherheitspatches so schnell wie möglich aus.
Überprüfen Sie optional, von wann die fehlenden Updates sind. Wenn Updates von WSUS oder SCCM verwaltet werden, kann es sein, dass die Windows Update Services für Endpunkte deaktiviert sind. Ist dies der Fall, kann CSAT die Informationen nicht ermitteln. Überprüfen Sie optional die Updateverwaltungstools, um herauszufinden, ob Endpunkte mit Updates hinterherhinken.

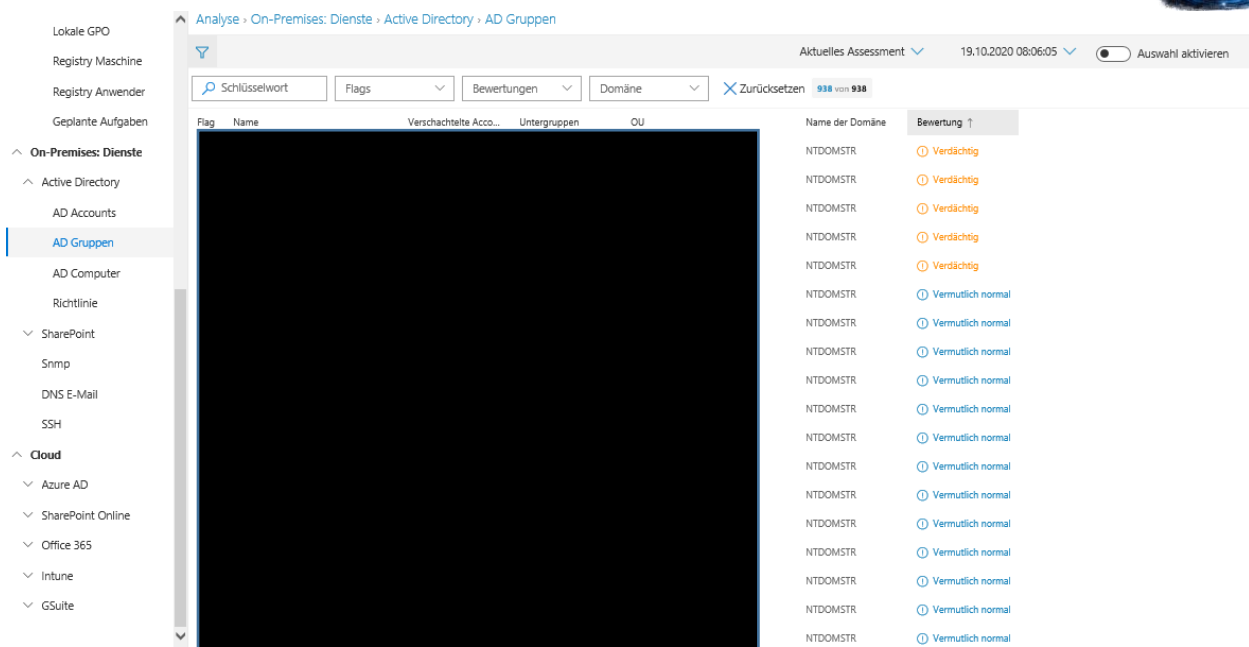
STRATLAS – ist bereinigt und erledigt zum Zeitpunkt 11.11.2020!

4.1.4. CIS-Control 4: Kontrollierte Nutzung von Administratorrechten

Ausgabe CSAT – Administrative Gruppen im Active Directory

AD ADMINISTRATOREN - NTDOMSTR

Eingebaute Domänen-Gruppe für Administratoren	13
Domänen-Administratoren	7
Enterprise-Administratoren	2
Schema-Administratoren	1
Benutzer mit Administrator-Rechten	11



- Es gibt eine klare Trennung zwischen Administratorkonten und normalen Benutzerkonten.
- Bei einigen Administratorkonten läuft das Passwort nie ab. Dies ist erkannt und bewusst.

Aktivieren Sie auch bei Administratoren die regelmässige Änderung des Passworts. Alternativ können Sie MFA einrichten und / oder die Anmeldungen der privilegierten Konten proaktiv **monitoren**.

- Der **Standard-Administrator** ist aktiv und **wird** sogar **verwendet**. Dieses Konto ist allgemein bekannt und wird daher gerne als erstes angegriffen. Es wird empfohlen, das Konto zu deaktivieren und ausschliesslich persönliche Konten zu verwenden.

- In zwei privilegierten Gruppen wurde ein **aktiver Account** für einen **externen DL** gefunden, welcher seit langer Zeit nicht benutzt worden ist. Gilt nur für einen Lokalen Account für ein Applikationssystem



Ausgabe CSAT – Azure Active Directory Rollen

STRELLSONAG.ONMICROSOFT.COM

User Administrator	2
Exchange Administrator	2
SharePoint Administrator	2
Service Administrator	2
Helpdesk Administrator	2
Teams Service Administrator	2
Globaler Administrator	7
Directory Synchronization Accounts	1

Inventarisierung	Gruppe	Anzahl
Administrator-Accounts	Mit MFA	deaktiviert
	Ohne MFA	Alle

Analyse und Empfehlungen:

Warum deaktiviert

- Idealerweise haben weniger als 5 Benutzer die Rolle **Global Administrator**. Überprüfen Sie, ob alle Konten diese höchste Berechtigungsstufe brauchen. Weisen Sie – wenn möglich – spezifischere Rechte zu.
- Die Multi-Faktor-Authentifizierung wurde deaktiviert; aus dem Grunde, der nicht Unterstützung für Skype for Business und dem Einsatz von Teams, welche der Admin nur mit Powershell „connecten“ kann.**

Administratorkonten stellen ein hohes Risiko für ein Unternehmen dar, da sie Zugriff auf das Netzwerk, Systeme und vertrauliche Daten haben. Daher wird empfohlen, die Anzahl der Administratoren so weit wie möglich zu begrenzen. Unser Rat ist es, das Prinzip der geringsten Privilegien und Just-in-Time-Zugriff zu implementieren und Multi-Faktor-Authentifizierung für alle privilegierten Konten zu aktivieren. Ebenfalls empfohlen wird ein Prozess der regelmässigen Berechtigungen für privilegierte Konten überprüft.

- ➔ Die sieben Global Admins müssen von der IT der Einfachheit verwendet werden. Somit besteht kein direkter Handlungsbedarf in Bezug auf die Sicherheit des Unternehmens.

Das **Prinzip der geringsten Berechtigungen** ist eine empfohlene Sicherheitspraxis, bei der der Zugriff auf diejenigen beschränkt ist, die dies benötigen und dafür autorisiert sind, und indem nur der für die Aufgabe erforderliche Zugriff zugelassen wird. **Just-in-Time-Zugriff** gewährt Benutzern temporäre Berechtigungen, um privilegierte Aufgaben nach Bedarf auszuführen.

Azure Privileged Identity Management (PIM) (in Azure Active Directory Plan 2) ermöglicht es, das Prinzip des geringsten Berechtigungszugriffs und Just-in-time-Zugriffe durchzusetzen, und hilft Ihnen grundlegend, den Zugriff auf wichtige Ressourcen zu verwalten, zu kontrollieren und zu überwachen.



4.1.5. CIS-Control 5: Sichere Konfiguration von Hard- und Software auf mobilen Geräten, Laptops, Workstations und Servern

Ausgabe CSAT – AD-Domänen- und Gesamtstrukturfunktionsebenen

DOMÄNEN-LEVEL - NTDOMSTR

Name der Domäne	NTDOMSTR
Domänen-Level	WINDOWS SERVER 2012 R2
Forest-Level	WINDOWS SERVER 2012 R2

Analyse und Empfehlungen:

Es wird empfohlen, die Active Directory-Domäne und die Funktionsebenen des Forest auf das höchste verfügbare Niveau zu aktualisieren. Jede neue Version von Active Directory auf Windows Server enthält neue (Sicherheits-) Funktionen, die nur dann genutzt werden können, wenn alle Domänencontroller (DC) in der Domäne oder im Forest auf dieselbe Version aktualisiert wurden. Beispiel: Windows Server 2008 R2 führt den AD-Papierkorb ein, ein Feature, das es dem Administrator ermöglicht, gelöschte Objekte aus Active Directory wiederherzustellen. Allerdings beschränkt es sich auf den letzten Server Release **von Microsoft 2012 R2**

Einschränkungen bei einem Upgrade auf 2016:

Es stehen keine Probleme zu erwarten, wenn man eine Active-Directory-Domäne hat, die sowohl aus Windows Server 2012 R2 als auch aus Windows Server 2016 Domänen-Controllern besteht. Allerdings wird man dann die Funktionsebene nicht anheben und mithin die neuen Möglichkeiten nicht nutzen können, bis sämtliche Domänen-Controller in der Bereitstellung auf den Stand von Windows Server 2016 gebracht sind.

Ausgabe CSAT – Sichere Konfiguration von Endpunkten

Endpoints with LM Compatibility are lower than five	743
Endpoints with RDP enabled without NLA	57
Endpoints with PowerShell execution set to Unrestricted	4
Endpoints with SMB V1 enabled	177

Alle Endgeräte 743 müssen

Zu NLA: die ersten System wurden bewusst ausgeschaltet der Task wird an

Alle die Powershell aktivierten Endpunkte sind in der IT

Die Endpoints mit SMBv1 müssen im Rahmen eines IT-Projektes angepasst werden.



Ausgabe CSAT – Registry Machine

Flag	Registry Key	Wert(e)	Daten	Zusammenstellung Endpunkt	Bewertung ↑
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa	Imcompatibilitylevel			Kritisch
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa	Imcompatibilitylevel	2		Kritisch
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManWorkstation\Parameters	enableplaintextpassword	1		Kritisch
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManWorkstation\Parameters	RequireSecuritySignature	0		Kritisch
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell	ExecutionPolicy	Bypass		Kritisch
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell	ExecutionPolicy	Unrestricted		Kritisch

Sichere Konfiguration verwundbarer Dienste

- **566** Endpunkte mit **aktiviertem SMBv1** gefunden. Stellen Sie sicher, dass **SMBv1 auf allen Systemen deaktiviert** ist. Es wird empfohlen, **neuere Versionen von SMBv2 oder SMBv3 zu verwenden, um die Sicherheit zu erhöhen**. SMBv1 kann mittels GPO, Windows PowerShell oder Intune deaktiviert werden.

Systeme	Anzahl
Microsoft Windows 10 Enterprise Sh. Liste im Anhang	506
Microsoft(R) Windows(R) Server 2003 Standard Edition 	10
Microsoft Windows Server 2019 Standard 	31
Microsoft Windows Server 2019 Datacenter 	19



In Microsoft-Umgebungen kommt das alte SMBv1-Protokoll kaum noch zum Einsatz, stattdessen stehen hier neuere Versionen zur Verfügung (**SMBv2 und SMBv3**). Vor allem sicherheitsrelevante Features, wie beispielsweise die Möglichkeit, SMB-Pakete zu signieren, sind für viele Anwender interessant. Leider ist aber SMBv1 in vielen Installationen immer noch aktiv und Verbindungen können immer noch auf Basis dieses veralteten Protokolls aufgebaut werden. Dies ist deshalb nicht wünschenswert, da die besten Security-Features neuerer SMB-Versionen nichts bringen, wenn das alte SMB-Protokoll immer noch aktiv ist.

SMBv1 hat Sicherheitslücken

Microsoft weist schon seit langer Zeit darauf hin, dass das SMBv1-Protokoll eine Vielzahl von Schwachstellen besitzt und daher abgeschaltet werden sollte. Seit Windows 2012 gilt das Protokoll bereits als "deprecated" und auch die empfohlene "Security baseline" für aktuelle Windows-Versionen enthält die Empfehlung, das Protokoll **zu deaktivieren**.

Warum

Windows-Benutzer, die diesem Ratschlag nicht gefolgt sind, hatten spätestens mit WannaCry ein böses Erwachen. Der Verschlüsselungstrojaner hat sich nämlich eine altbekannte Schwachstelle im SMBv1-Protokoll zu Nutze gemacht, um darüber Windows-Systeme zu infizieren.

Mit dem aktuellen Update für Windows 10 und Windows 2016 wird es damit nun aber vorbei sein. Mit dem Redstone-3-Update wird SMBv1 standardmäßig nicht mehr installiert. Da Microsoft die SMB-Funktionen jetzt nach Client und Server getrennt verwaltet, steht in den Home- und Pro-Versionen von Windows ein SMB-Client jedoch nach wie vor zur Verfügung und wird nur dann deinstalliert, wenn er nicht aktiv verwendet wird. Die Unterscheidung wurde einfach deshalb vorgenommen, um es Anwendern zu ermöglichen, immer noch auf SMB-Server zugreifen zu können, die lediglich SMBv1 unterstützen. Microsoft pflegt sogar eine Liste der Hersteller, die in ihren Produkten noch SMBv1 einsetzen [4]. Die Liste ist sicherlich nicht vollständig, aber dennoch erstaunlich lang. Auf der anderen Seite wird es aber nun nicht mehr möglich sein, als Anwender eine Verbindung mittels SMBv1 aufzubauen, wenn das System zuvor auf Redstone 3 aktualisiert wurde. Somit gehören Angriffe, die SMBv1 als Einfallstor verwenden, nun hoffentlich der Vergangenheit an.



177 Endpunkte mit **de-aktiviertem SMBv1** gefunden

Systeme mit deaktiviertem SMBv1	Anzahl
Microsoft Windows 8.1 Enterprise	67
Microsoft Windows 10 Enterprise	5
Microsoft Windows Server 2008 R2 Standard [REDACTED]	2
Microsoft Windows Server 2012 R2 Datacenter [REDACTED]	4
Microsoft Windows Server 2012 R2 Standard [REDACTED]	92
Microsoft Windows Server 2016 Standard [REDACTED]	7



Überprüfen Sie eine Reihe von Maschinen- und Benutzerregistrierungsschlüsseln. Es wird empfohlen, die folgenden Schlüssel zu ändern.

- Ändern Sie das LMCompatibilityLevel für Server auf 4 oder 5 und auf Workstations auf 2 oder 3.
 - Die NTLM-Version (0-5) sollte für eine bessere Sicherheit erhöht werden.
- Ändern Sie die RequireSecuritySignature auf 1.
 - Die Clientrichtlinie sollte so eingestellt werden, dass Pakete immer signiert werden.
- Ändern Sie AutoAdminLogon auf 0.
 - Automatische Anmeldungen müssen deaktiviert sein.
- Ändern Sie den Wert für 'LimitBlankPasswordUse' in 1.
 - Auf dem System sollte kein Konto mit leerem Kennwort vorhanden sein
- Ändern Sie ScreenSaverActive und ScreenSaverIsSecure auf 1.
Sperren Sie ein System, wenn es nicht verwendet wird. Ein kennwortgeschützter Bildschirmschoner, der sich nach einem bestimmten Zeitraum aktiviert, schützt kritische und vertrauliche Daten vor der Exposition gegenüber nicht autorisiertem Personal mit physischem Zugriff auf den Computer.

4.1.6. CIS-Control 6: Pflege, Überwachung und Analyse von Audit-Protokollen

UNGÜLTIGE ANMELDEVERSUCHE (AKTIVE AD ACCOUNTS, TOP 5) - NTDOMSTR

S-1-5-21-573608003-847915640-206043333-7560	162
S-1-5-21-573608003-847915640-206043333-9796	153
S-1-5-21-573608003-847915640-206043333-87244	150
S-1-5-21-573608003-847915640-206043333-13876	135
S-1-5-21-573608003-847915640-206043333-7734	109

Analyse und Empfehlungen:

- Es wurde eine grosse Anzahl von fehlerhaften Anmeldeversuchen gefunden. Dies könnte bedeuten, dass ein Angriff erfolgt ist oder der Anwender mehrfach genutzt wird. Wir erachten es als wichtig diese direkt zu kontaktieren und nachzufragen.

UNGÜLTIGE ANMELDEVERSUCHE (AKTIVE AD ACCOUNTS, TOP 5)

	162
	153
	150
	135
	109

Um das Risiko gehackt zu werden zu verringern, sollten verdächtige Anmeldungen überwacht werden. Es wird empfohlen, **Azure ATP** oder **Advanced Threat Analytics (ATA)** zu implementieren, um frühzeitige Warnungen vor möglichen Angriffen zu erhalten. Diese Sicherheitslösungen ermöglichen die Überwachung gegen verschiedene (AD) Angriffe. Kombinieren Sie dies mit **Azure AD Identity Protection** für die Cloudbenutzer.



Die Verwendung von integrierten Überwachungstools von Anbietern von Firewalls und Netzwerkgeräte ist eine kosteneffiziente Methode zum Erfassen von Protokollen auf solchen Geräten. Dieses Vorgehen deckt möglicherweise jedoch nicht das gesamte Netz und nicht alle Systeme im Unternehmen ab. Heutzutage kommen Cyberbedrohungen aus dem Inneren der Organisation. Intrusion Detection- und Prevention-Systeme (IDS/IPS) allein werden nicht in der Lage sein, Malware zu erkennen oder zu verhindern, weshalb eine SIEM-Lösung so wichtig ist. Daher ist es ratsam, die Einführung von **Azure Sentinel** zu erwägen und die Erfassung von Protokollen auf allen Cloud- und On-Premise-Systemen zu erzwingen. Die Lösung bietet intelligente Sicherheitsanalysen und Threat Intelligence im gesamten Unternehmen mit einer einheitlichen Plattform für die Erkennung von Alerts, das Aufspüren von Bedrohungen, die proaktive Jagd und die Reaktion auf Bedrohungen.

4.1.7. CIS-Control 7: Schutz von E-Mail und Web-Browser

Ausgabe CSAT - DNS-E-Mail

Inventory	Value	Notes
MusterGroup.com		
SPF record		
DKIM record		DKIM_NOT_FOUND
DMARC record		DMARC_NOT_FOUND
windsor.de		
SPF record		
DKIM record		DKIM_NOT_FOUND
DMARC record		DMARC_NOT_FOUND
Muster Filiale.com		
SPF record		
DKIM record		DKIM_NOT_FOUND
DMARC record		DMARC_NOT_FOUND
joop.com		
SPF record		
DKIM record		DKIM_NOT_FOUND
DMARC record		DMARC_NOT_FOUND

Analyse und Empfehlungen:

- **Es wurden folgende SPF-Einträge gefunden (Muster, Betrieb, Filiale Muster).** SPF ist eine Möglichkeit für Empfänger, die Identität des Absenders einer eingehenden E-Mail zu bestätigen. Mit einem SPF-Eintrag legen Sie fest, welche E-Mail-Server berechtigt sind, E-Mails mit Ihrer Domäne als Absender zu senden. Es ist ein Protokoll, um den Spam zu reduzieren, der im Web gesendet wird.

Fehlende Möglichkeiten



- **Es wurde kein DKIM-Eintrag gefunden.** Mit DKIM wird jede E-Mail, die Sie senden, mit einer digitalen Signatur signiert. Diese Signatur wird verwendet, um zu beweisen, dass Sie der Absender der E-Mail sind. DKIM gibt einer Organisation die Möglichkeit, während der Übertragung die Verantwortung für eine Nachricht zu übernehmen. Ohne dies könnte es zu unentdecktem E-Mail-Spoofing führen und es Hackern ermöglichen, den Inhalt von E-Mails zu manipulieren oder zu kompromittieren.
- **Es wurde kein DMARC-Datensatz gefunden.** DMARC ist ein Protokoll, das SPF und DKIM verwendet, um die Authentizität einer E-Mail-Nachricht zu bestimmen. Ohne dies sind E-Mail-Domänenbesitzer nicht in der Lage, zu kontrollieren, wie ihre E-Mails verarbeitet werden. Das erleichtert es Kriminellen, Nachrichten so zu fälschen, als ob sie von einer vertrauenswürdigen Adresse stammen. DMARC bietet eine Verknüpfung mit dem Domännennamen des Autors, veröffentlichte Richtlinien für die Behandlung von Authentifizierungsfehlern durch Empfänger und die Meldung von Empfängern an Absender.
- **Der DMARC-Datensatz ist ohne Richtlinie konfiguriert.** Die DMARC-Richtlinie bestimmt, was mit Nachrichten passiert, wenn die DMARC-Prüfung fehlschlägt. Es wird empfohlen, die Richtlinie auf 'Zurückweisen' ('Reject') zu setzen. Mit der Policy 'Reject' werden nicht autorisierte Mails gelöscht.

Wir empfehlen die Implementierung der entsprechenden **DKIM- und DMARC-Datensätze**, um eine unbefugte Nutzung Ihrer E-Mail-Domain(en) zu verhindern und Ihre Mitarbeiter vor Spam, Betrug und Phishing zu schützen.

4.1.8. CIS-Control 8: Schutz vor Malware

Ausgabe CSAT – Übersicht Antivirus

Serverendpunkte ohne Windows Defender	108
Clientendpunkte ohne Antivirus	0
Endpunkte mit veralteter Viren-Definition	1

Ausgabe CSAT - Anti Virus Expired

MachineName	AvName	AvDefinition
[REDACTED]	Windows Defender	OUT_OF_DATE
Ist ein PC in einem Besprechungsraum, magels Disk Grösse		

Ausgabe CSAT - Anti Virus deaktiviert

EndpointName	AvName	AvStatus	AvType
[REDACTED]	*No AV API*	OFF	NONE
	No AV API	OFF	NONE
	No AV API	OFF	NONE
	No AV API	OFF	NONE
	No AV API	OFF	NONE

Alle oben aufgeführten 2012 Server und älter sind Produkte die installiert ausgeliefert wurden.



Ein Antivirenprogramm ist eine der kostengünstigsten Möglichkeiten, Angriffe und Viren aus Ihrer Umgebung fernzuhalten. Es wird empfohlen, Microsoft Defender ATP zu implementieren und auf allen Endpunkten zu erzwingen. Es handelt sich um eine vollständige EDR-Lösung (Endpoint Detection and Response), die vorbeugenden Endpunktschutz und eine automatisierte Untersuchung und Sanierung bei Angriffen bietet. Dieses Tool ermöglicht Ihnen auch Einblicke in Sicherheitslücken und Fehlkonfigurationen auf Endpunkten.

Eine Endpoint Protection und Thread Prevention wird empfohlen. (Microsoft, TrendMicro, Checkpoint) nicht nur VPN wie aufgeführt:

Name	Version	First installation date	Publisher	#endpoints
Check Point SmartConsole R80.40	6.7.0	09/08/2020	Check Point Software Technologies Ltd.	2
Check Point VPN	98.61.672	09/09/2019	Check Point Software Technologies Ltd.	12

Die externen VPN-Zugriffe gehen alle über Check Point Capsule und werden somit gesichert.

4.1.9. CIS-Control 9: Beschränkung und Kontrolle von Netzwerk-Ports, -Protokollen und -Diensten

Ausgabe CSAT – Status Firewalls

Endpunkte mit deaktivierten Firewalls	12
---------------------------------------	----

FQDN	Domain	Private	Public	Threat
	Deaktiviert	Deaktiviert	Deaktiviert	PRIVATE_FIREWALL_DISABLED DOMAIN_FIREWALL_DISABLED PUBLIC_FIREWALL_DISABLED
	Deaktiviert	Deaktiviert	Deaktiviert	PRIVATE_FIREWALL_DISABLED DOMAIN_FIREWALL_DISABLED PUBLIC_FIREWALL_DISABLED
	Deaktiviert	Deaktiviert	Deaktiviert	PRIVATE_FIREWALL_DISABLED DOMAIN_FIREWALL_DISABLED PUBLIC_FIREWALL_DISABLED
	Deaktiviert	Deaktiviert	Deaktiviert	PRIVATE_FIREWALL_DISABLED DOMAIN_FIREWALL_DISABLED PUBLIC_FIREWALL_DISABLED
	Deaktiviert	Deaktiviert	Deaktiviert	PRIVATE_FIREWALL_DISABLED DOMAIN_FIREWALL_DISABLED PUBLIC_FIREWALL_DISABLED
	Deaktiviert	Deaktiviert	Deaktiviert	PRIVATE_FIREWALL_DISABLED DOMAIN_FIREWALL_DISABLED PUBLIC_FIREWALL_DISABLED
	Deaktiviert	Deaktiviert	Deaktiviert	PRIVATE_FIREWALL_DISABLED DOMAIN_FIREWALL_DISABLED PUBLIC_FIREWALL_DISABLED
	Deaktiviert	Deaktiviert	Deaktiviert	PRIVATE_FIREWALL_DISABLED DOMAIN_FIREWALL_DISABLED PUBLIC_FIREWALL_DISABLED
	Deaktiviert	Deaktiviert	Deaktiviert	PRIVATE_FIREWALL_DISABLED DOMAIN_FIREWALL_DISABLED PUBLIC_FIREWALL_DISABLED
	Deaktiviert	Deaktiviert	Deaktiviert	PRIVATE_FIREWALL_DISABLED DOMAIN_FIREWALL_DISABLED PUBLIC_FIREWALL_DISABLED
	Deaktiviert	Deaktiviert	Deaktiviert	PRIVATE_FIREWALL_DISABLED DOMAIN_FIREWALL_DISABLED PUBLIC_FIREWALL_DISABLED
	Deaktiviert	Deaktiviert	Deaktiviert	PRIVATE_FIREWALL_DISABLED DOMAIN_FIREWALL_DISABLED PUBLIC_FIREWALL_DISABLED



Analyse und Empfehlungen:

- Es wurden **10** Endpunkte mit einer oder mehreren deaktivierten Windows-Firewalls gefunden. Es wird empfohlen, die Firewalls auf diesen Computern zu aktivieren.

Windows-Firewall bietet Schutz vor Angriffen aus dem Netz wie Trojaner, Würmer oder jede andere Art von Schadprogrammen, die durch unerwünschten eingehenden Traffic verbreitet werden. Jeder infizierte Computer, der Zugriff auf Ihr Unternehmensintranet erhält, kann möglicherweise eine Verbindung zu ungeschützten Endpunkten oder Servern herstellen und diese gefährden, indem eine Sicherheitslücke in einem Windows-Dienst oder einer Drittanbieteranwendung ausgenutzt wird. Daher wird empfohlen, die Windows-Firewalls für eine tiefe Verteidigung aktiviert zu haben. Falls die Software-/Hardware-Firewall inaktiv ist, übernimmt die Windows-Firewall und schützt den Endpunkt. Es wird auch empfohlen, einen Prozess zu implementieren, um den Firewallstatus regelmässig zu überprüfen und Richtlinien im AD mithilfe von GP zu erzwingen.

Es wird empfohlen, **Microsoft Defender ATP** zu implementieren und auf allen Endpunkten zu erzwingen. Es handelt sich um eine vollständige EDR-Lösung (Endpoint Detection and Response), die vorbeugenden Endpunktschutz und eine automatisierte Untersuchung und Sanierung bei Angriffen bietet.

4.1.10. CIS-Control 10: Fähigkeit zur Wiederherstellung von Daten

Keine gescannten Daten aus CSAT; Empfehlungen sind unter "Foundational CIS Controls – Ergebnisse und Empfehlungen" zu finden.

4.1.11. CIS-Control 11: Sichere Konfiguration von Netzwerk-Komponenten

Keine gescannten Daten aus CSAT; Empfehlungen sind unter "Foundational CIS Controls – Ergebnisse und Empfehlungen" zu finden.

4.1.12. CIS-Control 12: Verteidigung von Netzwerk-Grenzen

Keine gescannten Daten aus CSAT; Empfehlungen sind unter "Foundational CIS Controls – Ergebnisse und Empfehlungen" zu finden.



4.1.13. CIS-Control 13: Schutz von Daten

Ausgabe CSAT – Status Verschlüsselung mit BitLocker (Stand per Ende September)

ENDPUNKTE

Client-Endpunkte ohne BitLocker-Verschlüsselung	175
Server-Endpunkte ohne BitLocker-Verschlüsselung	165

Analyse und Empfehlungen:

Eine unverschlüsselte Festplatte birgt die Gefahr, Daten zu verlieren, falls das Gerät/System verloren geht oder gestohlen wird. Dies gilt insbesondere für Laptops. Die Festplattenverschlüsselung mit BitLocker ist eine kostengünstige Möglichkeit, die Daten auf gestohlenen oder verlorenen Geräten zu schützen. Die Festplattenverschlüsselung verhindert unbefugten Zugriff auf den Datenspeicher. Einige Vorschriften, z. B. PCI-DSS und die EU-DSGVO, erfordern die Verwendung von Datenverschlüsselung.

Es wird empfohlen, BitLocker auf Endpunkten, die sensible Daten enthalten, zu aktivieren, sie mit **Intune** zu integrieren, um Wiederherstellungsschlüssel zentral zu verwalten und Einblick in den Status der Verschlüsselung zu erhalten.

Ausgabe CSAT – potenzielle personenbezogene Daten

Keine relevanten Informationen für Sharepoint entdeckt.

Ausgabe CSAT – Übersicht Office 365

OFFICE 365

PII Dokumente	0
Externe Benutzer (aktiviert)	78
Extern geteilte Elemente	0

Um Einblicke zu erhalten, welche Dokumente vertrauliche Daten enthalten, verwenden Sie **Azure Information Protection Scanner** (für on Premise) und **Data Loss Prevention** (für die Cloud).

4.1.14. CIS-Control 14: Zugriffskontrolle nach dem Need-to-Know-Prinzip

Ausgabe CSAT – Freigaben auf Endpunkten

Prüfen Sie die 55 Geräte in der unten aufgeführten Liste in Bezug auf die Freigabe in den jeweiligen Verzeichnissen der Geräte.

Analyse > On-Premises: Endpunkte > Freigaben

Schlüsselwort

Flags

Bewertungen

BitLocker

Typ

X Zurücksetzen

3814 von 3814

Aktuelles Assessment

Aggregierte Sicht

Auswahl aktivieren

Flag	Pfad	Name der Freigabe	Servername	Size	Beschreibung	Typ	BitLocker	Bewertung ↑
	D:\TEMP	TEMP		0 Bytes	Temporary	Laufwerk	Nein	Verdächtig
	D:\TEMP	TEMP		0 Bytes	Temporary	Laufwerk	Nein	Verdächtig
	D:\TEMP	TEMP		0 Bytes	Temporary	Laufwerk	Nein	Verdächtig
	D:\TEMP	TEMP		0 Bytes	Temporary	Laufwerk	Nein	Verdächtig
	D:\TEMP	TEMP		0 Bytes	Temporary	Laufwerk	Nein	Verdächtig
	D:\TEMP	TEMP		0 Bytes	Temporary	Laufwerk	Nein	Verdächtig
	D:\TEMP	TEMP		0 Bytes	Temporary	Laufwerk	Nein	Verdächtig
	D:\TEMP	TEMP		0 Bytes	Temporary	Laufwerk	Nein	Verdächtig
	D:\TEMP	TEMP		0 Bytes	Temporary	Laufwerk	Nein	Verdächtig
	D:\TEMP	TEMP		0 Bytes	Temporary	Laufwerk	Nein	Verdächtig



Geräte	

Analyse und Empfehlungen:

Freigaben könnten vertrauliche Daten enthalten. Wir empfehlen, für die Fachbereiche Prozeduren zu definieren, über die Berechtigungen überprüft und bestätigt werden. Die Verantwortlichkeiten für diese Überprüfungen müssen klar definiert sein. Über diese regelmässige Prüfung kann sichergestellt werden, dass Anwender die Berechtigungen haben, die sie benötigen und keine Daten sehen, die sie nicht sehen müssen / sollten.

Suchen Sie regelmässig nach benutzerdefinierten Freigaben. Benutzer könnten Daten entgegen den Unternehmensrichtlinien freigeben. Überprüfen Sie auch, ob OneDrive, Dropbox und andere Sharing-Anwendungen unreguliert verwendet werden.

Hintergrund

Jeder USER, der authentifiziert ist, kann auf dem D-Share zugreifen. (Dies gilt für alle Aussensysteme)

[REDACTED] werden von Herrn Muster überprüft.

4.1.15. CIS-Control 15: WLAN-Zugangskontrolle

Alle Zugänge (A Firmen eigene Geräte zugewiesen, B durch jeweiligen Sponsor) für die Muster Filiale AG (MusterGroup) werden via Zertifikate sichergestellt. Der Zugang ins Internet wird durch den jeweiligen Verantwortlichen Sponsor frei gegeben, das heisst der Mitarbeiter ist selbstverantwortlich. Das Gastnetzwerk ist logisch getrennt jedoch nicht physisch. Alle Client betreute Geräte werden eingebucht. Gäste wie BYOD können



4.1.16. CIS-Control 16: Monitoring und Kontrolle von Benutzerkonten

Ausgabe CSAT – Status AD Accounts

AD ACCOUNTS - NTDOMSTR

Aktivierte Accounts	947
Deaktivierte Accounts	337
Aktive Accounts ohne Anmeldung für mehr als 30 Tage	115
Aktive Accounts ohne Anmeldung für mehr als 90 Tage	93
Aktive Accounts ganz ohne Anmeldung	71
Als 'kritisch' geflaggte Accounts	0

Ausgabe CSAT – AD User Account Control Flags

UAC DETAILS AKTIVE AD ACCOUNTS - NTDOMSTR

Partial Secrets Account (Konto ist ein schreibgeschützter Domänencontroller - RODC)	0
Trusted To Auth For Delegation (Konto wird für Delegierungszwecke aktiviert)	0
Nur DES Schlüssel verwenden	0
Smartcard erforderlich	0
Passwort läuft nie ab	239
Umkehrbares Textpasswort	0
PreAuth nicht erforderlich	0
Kann Passwort nicht ändern	0
Kein Passwort erforderlich	61

Anmerkung:

Deaktivierte User werden im UAC gesondert verschoben und einen Tag später gelöscht.

Passwörter, die nicht ablaufen beinhalten gelöschte und deaktivierte User.



Analyse und Empfehlungen:

- **93** Konten haben **sich 90 Tage lang nicht angemeldet** und **71** Konten haben **sich noch nie angemeldet**. Überprüfen Sie diese Accounts und bereinigen Sie die, die nicht verwendet werden.
- **337** Konten sind **deaktiviert**. Bereinigen Sie diese Konten.
- **239** Konten **können ihre Kennwörter nicht** ändern. Überprüfen Sie diese Konten und entfernen diese Einstellung nach Möglichkeit.
- Für **61** Konten ist die Einstellung **Kennwort nicht erforderlich** aktiviert. Mit diesem Flag kann sich ein Konto mit einem leeren Kennwort anmelden. Überprüfen Sie diese Konten und entfernen Sie, wenn möglich, diese Einstellung. (Anm.: Das geht nur über PowerShell.)
- **239** Konten haben die Einstellung **Kennwort läuft nie ab**. Ältere Kennwörter sind anfälliger für Hackerangriffe. Überprüfen Sie diese Konten und entfernen Sie, wenn möglich, diese Einstellung.



Ausgabe CSAT – AD Passwort-Richtlinie

PASSWORT-RICHTLINIE - NTDOMSTR

Dauer der Sperre in Minuten	30
Komplexes Passwort erforderlich	true
Maximale Gültigkeit von Passwörtern	10675199
Minimale Gültigkeit von Passwörtern	0
Minimale Passwort-Länge	10
Passwort-Historie	5
Schwellwert Sperre	0

Analyse und Empfehlungen:

Die Kennwortrichtlinie sollte in den folgenden Punkten angepasst werden:

- Maximales Kennwortalter: **60** oder **90** Tage
- Schwellwert Kontosperre: **4** oder **5** ungültige Anmeldeversuche
- Passwort-Historie / gespeicherte Kennwörter: sollte von 5 auf mindestens **10** oder **24** Passwörter gesetzt werden
- Das Minimale Kennwortalter: von 0 auf **1, 3** oder **7** Tage setzen

Bereits vorhandene Einstellungen

- Die Kontosperrdauer: ist mit **30** oder **60** Minuten richtig gesetzt
- Ein Komplexes Passwort wird gefordert: **ist Aktiviert (true)**
- Minimale Passwort-Länge: **ist mit 10 Zeichen als Mittelwert von 8 bis 12 Zeichen richtig gesetzt**



Ausgabe CSAT – Azure Active Directory – Externe Benutzer

Analyse und Empfehlungen:

- In Azure Active Directory wurden 78 externe Benutzer gefunden, die mit ihrer persönlichen E-Mail-Adresse eingeladen wurden. Überprüfen Sie diese Konten und deaktivieren Sie sie wo erforderlich.

<u>Firma</u>	<u>Anzahl User (Mitarbeiter)</u>	<u>Firma</u>	<u>Anzahl User (Mitarbeiter)</u>
	7		1
	16		2
	5		2
	6		1
	6		1
	13		1
	2		1
	8		1
	4 (einer Doppelt)		1

Es wird dringend empfohlen, die externen Benutzer und ihre Zugriffsberechtigungen regelmässig zu überprüfen, insbesondere Konten mit persönlichen E-Mail-Adressen wie Outlook, Gmail, Hotmail, Gmx usw. Wenn diese externen Benutzer ihr Unternehmen verlassen und Ihr Unternehmen nicht darüber benachrichtigt wird, haben sie über ihr persönliches E-Mail-Konto weiterhin Zugriff auf ihre Arbeitskonten.

Lokale Konten auf gescannten Endpunkten

Inventarisierung	Geräte Anzahl
Lokales Administratorkonto aktiviert	685

Analyse und Empfehlungen:

Lokale Konten sollten in einem Firmennetzwerk mit zentralisierter Authentifizierungsplattform nicht verwendet werden. Manchmal ist ein lokaler Administrator dennoch erforderlich. Wir empfehlen dann die Implementierung von Local Administrator Password Solutions (LAPS). LAPS ist ein Tool zur automatischen Verwaltung der lokalen Admin-Passwörter auf Domain-verbundenen Windows-Rechnern. Es speichert sie im AD, wo sie bei Bedarf wieder nachgeschaut werden können. **LAPS wurde im Frühjahr 2021 umgesetzt.**



4.1.17. CIS Control 17: Security Awareness- und Trainingsprogramm

Security Awareness Training

Mit einem Security Awareness Training schaffen Sie die Voraussetzungen, dass ein hohes Mass an Datenschutz und IT-Sicherheit erreicht werden kann, durch sensibilisierte und geschulte Mitarbeiter. In einem ersten Schritt erfolgt das Bewusstmachen möglicher Gefahren, gefolgt vom richtigen Umgang mit diesen potenziellen Bedrohungen. Allen Mitarbeitern sollte nach der Absolvierung des Security Awareness Trainings bekannt sein, was von ihnen, im Hinblick auf IT-Sicherheit erwartet wird und wie sie in sicherheitskritischen Situationen reagieren sollten.

Lösungsvorschlag:

Ein Trainingskonzept ermöglicht eine zeiteffiziente Schulung durch eine Kombination verschiedener Trainingsvarianten und Inhalte auf einer E-Learning-Plattform. Die realitätsnahe Anpassung an Gegebenheiten und Anforderungen ihres Unternehmens ermöglicht eine schnelle Identifikation mit dem Thema. Die Wirksamkeit des Security Awareness Trainings wird beispielsweise mit einer geplanten Phishing-Kampagne überprüft.

Test mit ausgewählten Mitarbeitern

Unser Einführungspaket beinhaltet sämtliche Dienstleistungen, damit Sie und Ihre Mitarbeiter (max. 30 Mitarbeiter) auf die Security Awareness Trainings Plattform zugreifen können. Die Demo-Phase erlaubt Ihnen während eines Monats, respektive 30 Tage, den Zugriff und die Nutzung der Security Awareness Trainings Plattform.

Vorschlag zu einer Herangehensweise:

- Aufschaltung von bis zu 30 Mitarbeitern auf einer Demo-Plattform. Die Mitarbeiterdaten werden in Form einer CSV-Datei vom Kunden angeliefert.
- Abbildung Ihrer aktuellen Unternehmens-Passwort-Policy, falls diese vom Kunden zur Verfügung gestellt wird.
- Grundkonfiguration der Demo-Plattform mit Einbindung Kundenlogo, Zeitzone, Benachrichtigungen in Deutsch oder Englisch und Einrichtung der Support-Mailadresse.
- Erstellung und Versand einer Phishing-Mail an die erfassten Mitarbeiter
- Nach 5 Tagen werden die Resultate aus der Phishing-Kampagne analysiert und der Schulungsbedarf und die Trainings-Module bestimmt.
- Interne Information an die erfassten Mitarbeiter über Teilnahme am Schulungsprogramm und Aufschaltung von 1-2 Trainings-Modulen, welche innerhalb von 10 Arbeitstagen durchgearbeitet werden sollen.
- Nach Ablauf der Trainingseinheiten erfolgt die Erstellung und Versand einer zweiten Phishing-Mail, um zu prüfen, ob sich die Situation verbessert hat.
- Abschliessend erfolgt eine Nachbesprechung, ein Erfahrungsaustausch und Bestimmung weiteres Vorgehen.

4.1.18. CIS-Control 18: Sicherheit der Anwendungssoftware

Generell wurde festgestellt, dass die Applikationsverantwortlichen sich im Wesentlichen nicht um die unterliegende Middleware (Java, Tomcat, MySQL....) kümmern und release Patches dieser vernachlässigt werden, hier muss die Verantwortlichkeit definiert und festgehalten werden. Wenn die Systeme nicht aktualisiert sind, herrscht eine Lücke im Gesamtsystem der Betriebssysteme.

Applikationen wie Exchange als Beispiel



Es wird vertrauenswürdigen Herstellern wie Microsoft vertraut und regelmässig in der Infrastruktur dementsprechend die Patches aktualisiert.

4.1.19. CIS Control 19: Incident Response und Management

Keine gescannten Daten aus CSAT; Empfehlungen sind unter "Organizational CIS Controls – Ergebnisse und Empfehlungen" zu finden.

Beschrieben ist das Sicherheits Vorgehen. IT-Abläufe sind geregelt und definiert wie vorzugehen ist. Eine Versicherung ist auch abgeschlossen. Test und durchgespielt wurde es noch nie. Das Thema ist der Geschäftsleitung bekannt. Derzeit sind keine KPIs bezüglich Incident Response und Management vorhanden.

Interner IT-Backup

Für SAP wird in regelmässigen Abständen 1- bis 2-mal im Jahr ein Testsystem immer wieder aufgebaut.

Interne Messkriterien

Intern sind keine SLAs vorhanden, die Gewichtung obliegt der IT. Anlaufstelle ist Herr Peter Muster

Frei nach dem Prinzip: „Es muss Funktionieren“. Der Eigene Standard der IT ist für den Gesamtbetrieb zweckmässig aufgesetzt.

4.1.20. CIS-Control 20: Penetrationstests und "Red Team"-Übungen

Bei neuen Systemen wird intern einmalig ein Test durchgeführt. Von Externer Seite werden keine Tests durchgeführt.

Es werden keine Tools für Vulnerability Scans und Penetration Tests eingesetzt.

4.1.21. Microsoft Secure Score

Der Microsoft Secure Score wertet verschiedene Elemente aus Office 365 und Azure aus. Der Score ist abhängig von den in Office 365 verwendeten Diensten und vergleicht diese mit einer von Microsoft definierten Baseline. Er zeigt, wo man im Vergleich zu Best Practices der Cybersicherheit steht.



Der Microsoft Secure Score von Muster AG für den Microsoft Tenant:

MICROSOFT SECURE SCORE

Mandantenname: **strellsonag.onmicrosoft.com**

Gesamtpunktzahl: 38/238

Microsoft Secure Score analysiert den Schutzstatus Ihrer Identitäten, Daten, Geräte, Apps und Infrastruktur

Identität 33 / 203

Schutzstatus Ihrer Azure AD-Konten und -Rollen

Daten 5 / 35

Schutzstatus Ihrer Office365-Dokumente

Geräte Keine anzuzeigenden Daten

Schutzzustand Ihrer Geräte

Apps Keine anzuzeigenden Daten

Schutzstatus Ihrer E-Mail- und Cloud-Apps

Infrastruktur Keine anzuzeigenden Daten

Schutzstatus Ihrer Azure-Ressourcen

Unter diesem [Link](#) finden Sie weitere Infos zum Microsoft Secure Score. Oder überprüfen Sie den Score direkt unter <https://security.microsoft.com/securescore/>



5. Zusammenfassung aller Massnahmen

5.1. CISv8- Basic Massnahmen nach Priorität

3 Dringend	5 Sehr wichtig	3 Wichtig	0 Empfohlen
---------------	-------------------	--------------	----------------

Dringend				
Topic	Question	Answer	Advice	Advised Products
4. Kontrollierte Nutzung von Administratorrechten	Ist ein Prozess implementiert, durch den regelmäßig für jede Person mit administrativen Rechten auf Servern, Desktops und Laptops diese Berechtigungen von übergeordneter Stelle überprüft werden?	Basic (1) Kein Prozess definiert	Implementieren Sie einen Prozess zur Genehmigung und regelmäßigen Bestätigung von Berechtigungen für Admin-Accounts. Bereinigen Sie alte / nicht genutzte Accounts.	Azure Privileged Identity Management (PIM), Azure AD Access Review
5. Sichere Konfiguration von Hard- und Software auf mobilen Geräten, Laptops, Workstations und Servern	Verfügt die Organisation über eine implementierte sichere Hardening-Baseline für alle neuen Systeme? Werden alte NTLM- und SMB- und andere sicherheitsrelevante Registry-Schlüssel deaktiviert?	Basic (1) Nicht implementiert	Definieren Sie Hardening-Vorgaben für die wichtigsten Systeme, wobei diese standardmäßig so weit wie möglich abgeschlossen sein sollten.	Azure VMs, Azure CIS Hardened Images, Microsoft Endpoint Manager
6. Pflege, Überwachung und Analyse von Log-Dateien	Kontrolliert und analysiert ein Sicherheits-Experte die Protokolle und Benachrichtigungen um Anomalien aufzuspüren?	Basic (1) Kein Prozess definiert	Implementieren Sie einen Prozess zur Überwachung der Logs mit regelmäßiger Überprüfung auf kritische sicherheitsrelevante Einträge.	

Sehr wichtig				
Topic	Question	Answer	Advice	Advised Products
1. Bestandsaufnahme und Kontrolle der Hardware-Assets	Ist eine Lösung für die Zutrittskontrolle auf Netzwerkebene (802.1x, NAC) implementiert, die Zertifikate fordert, um Geräte zu authentifizieren, bevor sie sich mit dem Netzwerk verbinden können?	Standardized (2) In begrenztem Umfang implementiert oder Implementierung einer Access Control Solution auf Port-Ebene ohne Zertifikate	Übernehmen Sie den 802.1x-Standard, um Geräte zu authentifizieren, bevor sie sich mit dem Netzwerk verbinden.	Microsoft Endpoint Manager, 802.1x
2. Bestandsaufnahme und Kontrolle der Software-Assets	Sind Discovery-Tools implementiert, um alle Software-Anwendungen in der gesamten Infrastruktur der Organisation zu identifizieren?	Standardized (2) In begrenztem Umfang implementiert	Erweitern Sie den Umfang des/der Discovery-Tools auf die gesamte IT-Infrastruktur.	Software Asset Management (SAM) -Tooling, Microsoft Endpoint Manager, Azure Security Center, Cloud App Security, Microsoft Defender ATP
3. Kontinuierliches Schwachstellen-Management	Sind Discovery-Tools implementiert, die Schwachstellen in Software auf den Systemen innerhalb der Infrastruktur der Organisation identifizieren?	Standardized (2) In begrenztem Umfang implementiert	Weiten Sie den Vulnerability Scan auf alle System aus.	Microsoft Endpoint Manager, Microsoft Defender ATP, Azure Security Center, Cloud App Security
5. Sichere Konfiguration von Hard- und Software auf mobilen Geräten, Laptops, Workstations und Servern	Sind Discovery-Tools implementiert, die in der Infrastruktur auf sämtlichen Systemen der Organisation nach falschen Sicherheits-Konfigurationen suchen?	Standardized (2) In begrenztem Umfang implementiert	Weiten Sie das Configuration Management auf die gesamte IT Infrastruktur aus.	Microsoft Endpoint Manager, Microsoft Defender ATP, Azure Security Center, Cloud App Security
6. Pflege, Überwachung und Analyse von Log-Dateien	Sind alle Geräte und Server, einschließlich Domain Controllern, Firewalls, Netzwerk-basierten IPS und inbound und outbound Proxies, so aufgesetzt und konfiguriert, dass sämtlicher Datenverkehr (sowohl erlaubter als auch blockierter) und fehlgeschlagene Anmeldungen ausführlich protokolliert werden? Werden Logs zentral abgelegt, gegen Manipulation gesichert und verwendet um ständig verdächtige Aktivitäten aufzuspüren und zu melden?	Standardized (2) Auf einigen Netzwerk-Geräten implementiert	Legen Sie die Protokolle aller Geräte auf der zentralen Plattform ab. Verwenden Sie eine SIEM-Lösung zum Aggregieren der Daten aus allen Quellen die lokal oder in der Cloud ausgeführt werden, einschließlich Benutzern, Anwendungen, Servern und Geräten.	Azure Sentinel, Azure Security Center, Azure Advanced Threat Protection (ATP), Microsoft Cloud App Security



Wichtig				
Topic	Question	Answer	Advice	Advised Products
1. Bestandsaufnahme und Kontrolle der Hardware-Assets	Sind Discovery-Tools (aktiv und passiv) implementiert, um alle Geräte zu identifizieren, die mit der Infrastruktur der Organisation verbunden sind?	Rationalized (3) In der gesamten Infrastruktur der Organisation implementiert	Automatisieren Sie die Discovery von Geräten und führen Sie sie regelmäßig / kontinuierlich durch.	Microsoft Endpoint Manager, Network Discovery-Lösung
3. Kontinuierliches Schwachstellen-Management	Ist eine automatisierte Lösung für das Patch Management implementiert, die die fortlaufende Aktualisierung aller Systeme der Organisation sicherstellt?	Rationalized (3) Für alle Systeme implementiert. Alle Maschinen sind gepatcht und auf dem neuesten Stand.	Richten Sie Zeitfenster ein, in denen Patches automatisiert und fokussiert verteilt werden. Patchen Sie basierend auf möglichen Risiken.	Microsoft Endpoint Manager, Azure Security Center
4. Kontrollierte Nutzung von Administratorrechten	Hat jeder Administrator einen persönlichen Administrator-Account zusätzlich zu seinem normalen Benutzer-Account? Ist für jeden administrativen Zugriff Multi-Faktor-Authentifizierung eingerichtet? Werden die standardmäßigen Zugriffsrechte von Administrator-Accounts mit Hilfe von Just-in-time Regeln beschränkt?	Rationalized (3) Für alle administrativen Accounts implementiert	Wenden Sie die Prinzipien "Just enough permissions" und "Just in time permissions" an und beschränken Sie so die Zugriffsrechte administrativer Zugänge.	Azure AD Privileged Identity Management (PIM), Privileged Access Management (PAM), Azure Multi-Factor Authentication



5.2. CISv8- Foundational Massnahmen nach Priorität

2 Dringend	8 Sehr wichtig	0 Wichtig	0 Empfohlen
---------------	-------------------	--------------	----------------

Dringend				
Topic	Question	Answer	Advice	Advised Products
14. Zugriffskontrolle nach dem Need-to-Know-Prinzip	Erfolgt die Netzwerk-Segmentierung aufgrund der Kennzeichnung oder des Klassifizierungs-Levels der auf den Servern gespeicherten Informationen?	Basic (1) Keine Netzwerk-Segmentierung	Führen Sie Netzwerk-Segmentierung für die wichtigsten Datenquellen der Organisation ein.	
16. Monitoring und Kontrolle von Benutzerkonten	Wird die Account-Verwaltung von den Fachbereichen betrieben? Hat jeder Account einen verantwortlichen Besitzer? Werden ungenutzte Accounts nach einer bestimmten Zeit gesperrt? Verfallen Accounts automatisch?	Basic (1) Keine Benutzerverwaltung oder ad hoc von der IT betrieben.	Sorgen Sie dafür, dass die Fachbereiche die Verantwortung für ihre Benutzerkonten übertragen bekommen. Das schließt Prüfungen durch den fachlichen / funktionalen Besitzer des Benutzerkontos ein. Bereinigen Sie alte Accounts.	Azure AD Access Reviews

Sehr wichtig				
Topic	Question	Answer	Advice	Advised Products
7. Schutz von E-Mail und Web Browser	Sind Netzwerk-basierte URL-Filter (inkl. DNS Filtering) implementiert, die Systeme daran hindern, Websites zu laden, die nicht von der Organisation genehmigt sind?	Standardized (2) Für einige Systeme implementiert	Stellen Sie sicher, dass der Proxy-Server / die IPS-Lösung von allen Systemen Ihrer IT Infrastruktur genutzt wird.	Microsoft Defender ATP, Proxy-Server / IPS-Lösung
8. Schutz vor Malware	Werden Antivirus-Ereignisse zentral protokolliert mit Benachrichtigung an die IT, so dass Maßnahmen ergriffen werden können?	Standardized (2) Für einige Systeme implementiert	Speichern Sie die AV-Logs zentral und nutzen Sie Benachrichtigungen um Erkenntnisse zu gewinnen. Spüren Sie Trends auf.	Microsoft Defender ATP, Azure Security Center, Cloud App Security
12. Verteidigung von Netzwerk-Grenzen	Werden Systeme mit unterschiedlichen Aufgaben und Zugangs-Ebenen mittels Netzwerk-Segmentierung getrennt?	Rationalized (3) Alle Systeme sind mittels Rollen und Restriktionsstufen getrennt.	Implementieren Sie Firewalls um den ein- und ausgehenden Traffic zwischen den Segmenten zu kontrollieren.	
12. Verteidigung von Netzwerk-Grenzen	Sind an allen Schnittstellen nach außen Firewalls und netzwerk-basierte Intrusion Detection/Prevention Systeme (IDS / IPS) implementiert, die Angriffe und bösartigen Traffic erkennen und blockieren?	Standardized (2) Grundlegende Firewalls sind implementiert	Aktivieren Sie wenn möglich die Deep Packet Inspection (DPI) und Intrusion Detection/Prevention Funktionalität der Firewall. Andernfalls überlegen Sie, die Firewall durch ein besseres Modell zu ersetzen. Sorgen Sie dafür, dass Sie über verdächtige Aktivitäten benachrichtigt werden.	Firewall mit IDS/IPS
12. Verteidigung von Netzwerk-Grenzen	Erfordert jede Anmeldung von außen die Verschlüsselung des Datenverkehrs und Multi-Faktor-Authentifizierung?	Rationalized (3) Verschlüsselung und MFA sind für alle Anmeldungen von außerhalb implementiert und erzwungen.	Erzwingen Sie für alle Systeme bedingten Zugriff bei Anmeldung von außerhalb.	Azure Multi-Factor Authentication (MFA)
13. Schutz von Daten	Werden Bewertungen von Daten durchgeführt, um sensible Informationen zu identifizieren, die Verschlüsselung und Prüfungen der Integrität erforderlich machen. Werden Klassifizierung und Kennzeichnung für alle sensiblen Dokumente durchgeführt?	Rationalized (3) Für alle Systeme implementiert	Wenden Sie Klassifizierung und Kennzeichnung an. Automatisieren Sie das Aufspüren von sensiblen Daten mittels Werkzeugen.	Azure Information Protection Scanner, Data Loss Prevention, Office 365 Advanced Data Governance, Azure Information Protection P2
14. Zugriffskontrolle nach dem Need-to-Know-Prinzip	Ist für alle Kommunikation von sensiblen Daten über weniger vertrauenswürdige Netzwerke die Verschlüsselung während der Übertragung implementiert?	Standardized (2) Für einen Teil der Netzwerk-Kommunikation umgesetzt	Aktivieren Sie Verschlüsselung für alle Kommunikation mit externen / öffentlichen Netzwerken. Für sensible Daten auch in internen Netzwerken.	Office 365 verwendet SSL/TLS für die Datenübertragung.
15. WLAN Zugangskontrolle	Sind WLAN-Gastnetzwerke vom Unternehmensnetzwerk getrennt?	Standardized (2) Eingerichtet, aber nicht physisch von den Geräten der Firma getrennt.	Trennen Sie das Gast-WLAN physisch von den von außen sichtbaren Geräten der Organisation. Weisen dem Gast-WLAN eine eigene Internetverbindung/VLAN zu.	



5.3. CISv8- Organizational Massnahmen nach Priorität

5 Dringend	6 Sehr wichtig	0 Wichtig	0 Empfohlen
---------------	-------------------	--------------	----------------

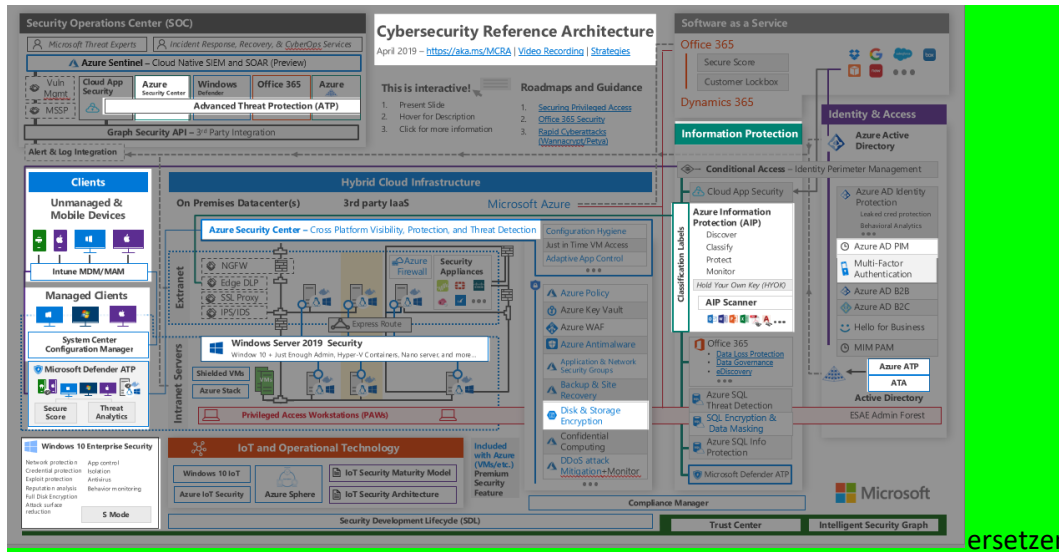
Dringend				
Topic	Question	Answer	Advice	Advised Products
17. Security Awareness- und Trainingsprogramm	Gibt es ein Trainingsprogramm zur Sensibilisierung für IT-Sicherheit über sichere Logins, Social Engineering, den Umgang mit sensiblen Daten, ungevolte Offenlegung von Daten und Identifikation von und Benachrichtigung bei Sicherheits-Vorfällen?	Basic (1) Kein Trainingsprogramm	Setzen Sie ein grundlegendes Trainingsprogramm für die wichtigsten Rollen Ihrer Organisation auf.	
19. Incident Response und Management	Ist eine Prozedur zur Reaktion auf Sicherheits-Vorfälle (Incident Response Procedure) definiert mit den passenden Benachrichtigungen, Zusammenstellung von Daten, Verantwortlichkeiten, gesetzeskonformen Protokollierungen und Kommunikations-Strategie?	Basic (1) Keine Prozedur definiert	Setzen Sie eine grundlegende Incident Response Procedure auf, die die häufigsten Szenarien abdeckt. Trainieren und leben Sie diesen Prozess	Office 365 Advanced Compliance: Advanced eDiscovery
20. Penetrationstests und "Red Team"-Übungen	Werden Tools für Vulnerability Scans und Penetration Tests zusammen eingesetzt?	Basic (1) Nicht implementiert	Implementieren Sie einen Vulnerability Scanner in der IT Infrastruktur der Organisation und verwenden diesen als Input für Penetration Tests.	Microsoft Endpoint Manager, Defender ATP, Azure Security Center + Pen testing tools
AD.1. IT Governance	Wie ist die Trennung von Pflichten, Aufgaben und Verantwortlichkeiten geregelt?	Basic (1) Die Trennung von Pflichten, Aufgaben und Verantwortlichkeiten erfolgt informell.	Formalisieren Sie die Trennung von Pflichten, Aufgaben und Verantwortlichkeiten, indem Sie eine Rollen-Matrix definieren.	
AD.2. Data Governance	Wird Data Risk Management auf allen Ebenen der Organisation durchgeführt?	Basic (1) Kein Risk Management oder keine Bewertung	Führen Sie einen grundlegenden Risk Management Prozess ein.	Microsoft Compliance Manager (ermöglicht Workflow-basierte Risikobewertungen)

Sehr wichtig				
Topic	Question	Answer	Advice	Advised Products
18. Sicherheit der Anwendungssoftware	Ist eine sichere (interne) Entwicklung von Anwendungen, Makros, Skripten und sonstigen Workflows oder Anpassungen sichergestellt?	Standardized (2) Für einzelne Eigenentwicklungen umgesetzt	Starten Sie einen Code Review (oder führen Sie Werkzeuge dazu ein) für alle Eigenentwicklungen in Ihrer Organisation.	Code Review Solution
18. Sicherheit der Anwendungssoftware	Ist der Zugriff auf produktive Systeme für Entwickler streng limitiert oder komplett unterbunden?	Standardized (2) Für einige Systeme implementiert	Schränken Sie für Entwickler den Zugang zu allen produktiven Systemen ein.	
20. Penetrationstests und "Red Team"-Übungen	Werden regelmäßig Penetrations-Tests auf allen Unternehmenssystemen durchgeführt?	Basic (1) Nicht oder nur bei Bedarf durchgeführt	Beauftragen Sie einen externen Spezialisten für dieses Thema mit der Durchführung eines Penetration Tests der von außen sichtbaren Systeme der Organisation.	
AD.1. IT Governance	Gibt es eine Sicherheits- und Datenschutzrichtlinie, die vom Management definiert und durchgesetzt wird?	Standardized (2) Eine grundlegende Policy zu Sicherheit und Datenschutz ist definiert.	Erweitern Sie die Policy zu Sicherheit und Datenschutz um branchenspezifische Themen und vereinheitlichen Sie sie in der ganzen Organisation.	
AD.1. IT Governance	Wird die regulatorische und gesetzliche Compliance fortlaufend überprüft und sichergestellt?	Standardized (2) Lokale legislative und regulatorische Anforderungen sind umgesetzt und werden regelmäßig überprüft.	Setzen Sie branchenspezifische Best Practice Ansätze um.	Microsoft Compliance Manager
AD.2. Data Governance	Werden von der gesamten Organisation Datenklassifizierung und -kennzeichnung für alle Dokumente durchgeführt?	Standardized (2) Eine Policy zur Klassifizierung ist umgesetzt. Die Kennzeichnung wird in den wichtigsten Systemen angewendet.	Wenden Sie Datenklassifizierung und -kennzeichnung in allen Systemen an.	Azure Information Protection Scanner, Data Loss Prevention, Azure Information Protection P2



6. Anhang A - Überblick über empfohlene Security-Software-Produkte

In diesem Bericht finden sich Verweise auf Microsoft-Produkte, die helfen können, benannte Schwachstellen aufzulösen. Eine Übersicht finden Sie in der von Microsoft veröffentlichten "**Cybersecurity Reference Architecture**" unten. Die hervorgehobenen Elemente sind die Produkte, die in diesem Bericht empfohlen werden.



Quelle: <https://aka.ms/mcra>

In diesem Bericht gibt es mehrere empfohlene Produkte zur Verbesserung der Cybersicherheit. Die Microsoft Cloud bietet in verschiedenen Lizenzen eine Vielzahl von Cybersecurity-Lösungen.

6.1. Microsoft 365 Business und Microsoft 365 E3

Microsoft 365 Business oder Microsoft 365 E3 bieten die Basissicherheitsuite für Office 365 und Azure. Microsoft beschreibt Microsoft 365 Business wie folgt: "Microsoft 365 Business ist ein Abonnement, bei dem Sie Ihre Organisation in der Cloud betreiben können und Microsoft sich für Sie um die IT kümmert durch die Verwaltung der Geräte, Schutz vor realen Bedrohungen und der Bereitstellung der neuesten Business-Software."

Die folgenden Sicherheitsprodukte sind in Microsoft 365 Business verfügbar. Bitte beachten Sie, dass das Microsoft 365 Business nur maximal 300 Seats haben kann. Wenn mehr als 300 Seats benötigt werden, ist die Microsoft 365 E3 Lizenz notwendig.

Die mit einem Stern (*) gekennzeichneten Elemente sind nur in Microsoft 365 E3 enthalten. Die mit zwei Sternchen (**) markierten Elemente sind nur in Microsoft 365 Business enthalten.

- EM+S - Azure Active Directory P1
- EM+S - Azure Information Protection Plan 1
- EM+S - Conditional Access
 - bietet differenzierte Zugriffssteuerung, um Ihre Unternehmensdaten sicher zu halten. Dabei ermöglicht es Benutzern ihre Arbeit bestmöglich von jedem Gerät und von jedem Ort aus zu erledigen.
- EM+S - Multifaktor-Authentifizierung



- EM+S - Microsoft Intune
 - fokussiert auf Mobile Device Management (MDM) und Mobile Application Management (MAM) für Windows, Android und iPhone
- EM+S - Microsoft Advanced Threat Analytics (On-premise-Lösung) *
- EM+S - Self Service Passwort-Reset für AD
- Office 365 ATP - Anti-Phishing**
- Office 365 ATP - Anti-Spoofing**
- Office 365 ATP - Malware Detection
- Office 365 ATP - Safe Attachments**
- Office 365 ATP - Sichere Links**
- Windows 10 - BitLocker
- Windows 10 - Hello for Business
- Windows 10 - Windows Defender Application Control Guard
- Windows 10 - Windows Defender Credential Guard
- Add-ons - Data Loss Prevention*
- Add-ons - Office 365 MFA

6.2. Microsoft 365 E3 Add-ons

Für Microsoft 365 E3 stehen mehrere Add-Ons zur Verfügung. Das erste Add-on, das wir erklären möchten, ist "**E5 Security**". Dieses Add-on vereint den Sicherheitswert von Office 365, Windows 10 und EMS in einem einzigen Angebot. Die folgende Liste zeigt die Sicherheitsfunktionen, die nicht in "Microsoft 365 E3", aber in "Microsoft 365 E3 + E5 Security" verfügbar sind.

- EM+S - Azure Active Directory Plan 2
- EM+S - Azure Advanced Threat Protection für Benutzer
- EM + S - Microsoft Cloud App Security
- Office 365 ATP - Anti-Phishing
- Office 365 ATP - Anti-Spoofing
- Office 365 ATP - Safe Attachments
- Office 365 ATP - Safe Links
- Office 365 ATP - Attack Simulator
- Office 365 ATP - Automatisierte Untersuchung und Reaktion
- Office 365 ATP - Threat Intelligence
- Windows 10 - Microsoft Defender Advanced Threat Protection

Das zweite Add-on, das wir erklären möchten, ist "**E5 Compliance**". Dieses Paket kombiniert Office 365 Advanced Compliance und Azure Information Protection. Es wurde entwickelt, um Compliance- und IT-Teams bei der Durchführung laufender Risikobewertungen für alle Microsoft Cloud-Dienste zu unterstützen, vertrauliche Daten während des gesamten Lebenszyklus automatisch zu schützen und zu steuern und effizient auf regulatorische Anforderungen zu reagieren. Die folgende Liste zeigt die Sicherheitsfunktionen, die nicht in "Microsoft 365 E3", aber in "Microsoft 365 E3 + E5 Compliance" verfügbar sind.

- EM+S - Azure Information Protection Premium P2
- Add-ons - Advanced Compliance



6.3. Microsoft 365 E5

Die Lizenz "Microsoft 365 E5" enthält alle verfügbaren Microsoft-Sicherheitsprodukte. Die vollständige Microsoft 365 E5-Suite umfasst nicht nur Sicherheits- und Compliance-Funktionen, sondern auch Angebote zu Business Analytics mit Power BI sowie Kommunikation mit Audiokonferenzen und erweitertem Telefonsystemwert. Die folgende Liste zeigt die Sicherheitsfunktionen, die nicht in "Microsoft 365 E3", aber in "Microsoft 365 E5" verfügbar sind.

- EM+S - Azure Active Directory-Plan 2
- EM+S - Azure Information Protection Premium P2
- EM+S - Azure Advanced Threat Protection für Benutzer
- EM + S - Microsoft Cloud App Security
- Office 365 ATP - Anti-Phishing
- Office 365 ATP - Anti-Spoofing
- Office 365 ATP - Safe Attachments
- Office 365 ATP - Safe Links
- Office 365 ATP - Attack Simulator
- Office 365 ATP - Automatisierte Untersuchung und Reaktion
- Office 365 ATP - Threat Intelligence
- Windows 10 - Microsoft Defender Advanced Threat Protection
- Add-ons - Advanced Compliance
- Add-ons - Advanced Data Governance
- Add-ons - Customer Lockbox



7. Anhang B - Produkte, bei denen der Support ausläuft

Es wurden die folgenden Produkte gefunden, bei denen der Support ausgelaufen ist:

Produkte, bei denen der Support ausgelaufen ist	
WINDOWS SERVER 2003	
WINDOWS SERVER 2008 R2 SERVICE PACK 1	
WINDOWS XP	
Microsoft Office Professional Edition 2003	11.0.8173.0
Microsoft SQL Server 2008	10.52.4000.0
Microsoft SQL Server 2008	10.53.6000.34
Microsoft SQL Server 2005	9.4.5000.00

Es wurden die folgenden Produkte gefunden, bei denen der Support sehr bald ausläuft:

Produkte, bei denen der Support bald ausläuft	
WINDOWS 8.1	
Microsoft Office Standard 2010	
Microsoft Office Access 2010	



8. Anhang C - Details Secure Score

8.1. Bewertete Elemente

Die folgenden Elemente wurden von Microsoft Secure Score-Regeln erkannt und sollten gesondert überprüft werden. Das ist die Top 10 der erzielten Punkte. Überprüfen Sie den Secure Score regelmässig, um die Sicherheit zu verbessern.

Secure Score Detail Info Table (Action with text 'Scored')			
Titel	Kategorie	Score	Beschreibung
MUSTER FILIALE AG.ONMICROSOFT.COM			
Require MFA for administrative roles	Identity	7/50	Requiring multi-factor authentication (MFA) for all administrative roles makes it harder for attackers to access accounts. Administrative roles have higher permissions than typical users. If any of those accounts are compromised, critical devices and data is open to attack. You have one out of seven users with administrative roles registered and protected with MFA.
Ensure all users can complete multi-factor authentication for secure access	Identity	0/30	Multi-factor authentication (MFA) helps protect devices and data that are accessible to these users. Adding more authentication methods, such as the Microsoft Authenticator app or a phone number, increases the level of protection if one factor is compromised. You have one out of 885 users registered and protected with MFA.
Enable self-service password reset	Identity	0/5	With self-service password reset in Azure Active Directory, users no longer need to engage help desk to reset passwords. This feature works well with Azure AD dynamically banned passwords, which prevents easily guessable passwords from being used. You have 885 of 885 users who do not have self-service password reset enabled.
Designate fewer than five global admins	Identity	0/1	Reducing the number of global admins limits the number of accounts with high privileges that need to be closely monitored. If any of those accounts are compromised, critical devices and data are open to attacks. Designating fewer than five global admins reduces the attack surface area. You have 7 global admins.
Do not allow users to grant consent to unmanaged applications	Identity	0/10	Tighten the security of your services by regulating the access of third-party integrated apps. Only allow access to necessary apps that support robust security controls. Third-party applications are not created by Microsoft, so there is a possibility they could be used for malicious purposes like exfiltrating data from your tenancy. Attackers can maintain persistent access to your services through these integrated apps, without relying on compromised accounts. Policy in place: false.
Apply IRM protections to documents	Data	0/5	Using Information Rights Management protections (IRM) on email and document data prevents accidental or malicious exposure of data outside of your organization. Attackers targeting specific, high value data assets are blocked from opening them without user credentials. You have IRM on 0 out of 1317 document libraries.
Delete/block accounts not used in last 30 days	Identity	0/1	Deleting or blocking accounts that have not been used in the last 30 days, after checking with owners, helps prevent unauthorized use of inactive accounts.



			These accounts can be targets for attackers who are looking to find ways to access your data without being noticed. You have sixteen accounts that have not been used in the last 30 days.
Apply Data Loss Prevention policies	Data	0/20	Data Loss Prevention (DLP) policies can be used to comply with business standards and industry regulations that mandate the protection of sensitive information to prevent accidental or malicious disclosure. DLP sends alerts after it scans for potentially sensitive data, such as social security and credit card numbers, in Exchange Online and SharePoint Online. Setting up DLP policies will let you identify, monitor, and automatically protect sensitive information. You have 0 Data Loss Prevention (DLP) policies applied.
Turn on sign-in risk policy	Identity	0/30	Turning on the sign-in risk policy ensures that suspicious sign-ins are challenged for multi-factor authentication (MFA). You have 885 of 885 users that do not have the sign-in risky policy turned on.
Turn on user risk policy	Identity	0/30	With the user risk policy turned on, Azure Active Directory detects the probability that a user account has been compromised. As an administrator, you can configure a user risk conditional access policy to automatically respond to a specific user risk level. For example, you can block access to your resources or require a password change to get a user account back into a clean state. You have 885 users out of 885 that do not have user risk policy enabled.
Enable policy to block legacy authentication	Identity	0/20	Today, most compromising sign-in attempts come from legacy authentication. Older office clients such as Office 2010 do not support modern authentication and use legacy protocols such as IMAP, SMTP, and POP3. Legacy authentication does not support multi-factor authentication (MFA). Even if an MFA policy is configured in your environment, bad actors can bypass these enforcements through legacy protocols. You have 885 of 885 users that do not have legacy authentication blocked.
Turn on customer lockbox feature	Data	0/5	Turning on the customer lockbox feature requires that approval be obtained for datacenter operations that grants a Microsoft employee direct access to your content. Access may be needed by Microsoft support engineers if an issue arises. There is an expiration time on the request and content access is removed after the support engineer has fixed the issue. Feature in place: false.



9. Anhang D - Scope des Assessments

Das Cybersecurity Assessment wurde im folgenden Anwendungsbereich ausgeführt:

Organisation	
<i>Name des Kunden</i>	Muster AG
<i>Kerngeschäft</i>	
<i>Adresse Hauptsitz des Kunden</i>	Musterstrasse 21, CH-8000 Muster
<i>Anzahl der Mitarbeiter</i>	
<i>Bürostandort(e)</i>	

IT-Umgebung	
<i>Virtualisierungsplattform(en)</i>	VSphere
<i>Wesentliche Geschäfts-Applikationen</i>	SAP, Mail, Teams
<i>Zusätzliche Informationen</i>	Vertretungen in über 55 eigenen Geschäften mit internationalen Standorten

Schlüssel-Termine und Fristen des Assessments	
<i>Kick-off-Gespräch mit dem Kunden</i>	
<i>Komplette Interview-Serie und Bestandserfassung vor Ort</i>	
<i>Analyse / Bewertung der Daten aus der Inventarisierung</i>	
<i>Übergabe der Berichte</i>	
<i>Letztes Gespräch mit Kunden zur Überprüfung aller gelieferten Dokumente</i>	

Assessment-Teilnehmer der Sec4it		
Name	Unternehmen	Projektrolle
Beat Brunschwiler	Sec4it	

Interviews wurden von der Sec4it mit den wichtigsten Beteiligten bei Muster AG durchgeführt, um - zusätzlich zur automatisierten Inventarisierung der IT-Infrastruktur - Informationen zu sammeln. Diese Ergebnisse basieren auf den Antworten auf die im Cybersecurity-Fragebogen beschriebenen Fragen. Grundlegende Interviews wurden mit den folgenden Beteiligten bei Muster AG durchgeführt:

Befragter	Titel	Interviewer
Peter Muster	Director Business Solutions / IT	Beat Brunschwiler
Fritz Musterfranz	Head of IT Systems (Chief System Architect)	Beat Brunschwiler
Hans Mustermann	System Engineer	Beat Brunschwiler



9.1. Ziele des Cybersecurity Assessments

Wie viele andere Organisationen auch, befasst sich die **Muster AG** mit den grossen Trends, denen die IT heute gegenübersteht: Verbreitung von mobilen Geräten, Auswirkungen sozialer Netzwerke auf den Arbeitsalltag, das rasante Wachstum unstrukturierter Daten, die immer verbreitetere Einführung der Cloud, Datenschutzbestimmungen, ... Alle diese Bereiche sind von einer sich wandelnden Bedrohungslandschaft betroffen, was enorme Auswirkungen auf Sicherheitsprogramme und deren Umsetzung hat.

Das Cybersecurity Assessment liefert eine highlevel Bewertung des Reifegrads des Sicherheitsprogramms der **Muster AG** basierend auf den Sicherheits-Controls aus den drei Domänen (Basic, Foundational und Organisation) des vom Center for Internet Security® veröffentlichten Frameworks CIS Controls™ Version 7.

Die Ziele des Cybersecurity Assessments sind:

- Auf eine ganzheitliche, integrierte Weise eine Grundlage für den Schutz von IT-Assets und zur Förderung moderner Cybersecurity Praktiken zu schaffen.
- Die Ausrichtung auf Empfehlungen eines bekannten und hoch angesehenen Sicherheits-Frameworks als Grundlage für ein Cybersecurity-Programm.
- Entwicklung eines Sicherheits-Pfads für den Gang in die Cloud, wo Kontrolle rund um Authentifizierung, Autorisierung und Datenschutz noch wichtiger ist.
- Entwicklung von Empfehlungen auf Basis von Interviews und den während des Scans der IT-Umgebung erhobenen Fakten.
- Aufdecken kritischer Punkte zur Cybersicherheit.
- Erstellen einer priorisierten Aktionsliste, die als unmittelbare Roadmap für das Cybersecurity-Programm der Organisation dienen kann.

9.2. Inventory Tools

Für eine technische Bestandsaufnahme der IT-Infrastruktur bei der **Muster AG** wurde das Cyber Security Assessment Tool (CSAT) verwendet. Die so gewonnenen Daten zu IT-Assets und deren aktuellem Status dienten als Input für Bewertungen, Analysen und Berichte.

9.3. Cyber Security Assessment Tool

Das Cyber Security Assessment Tool (CSAT) wurde von erfahrenen Sicherheitsexperten entwickelt, um schnell den aktuellen Stand der Sicherheit eines Unternehmens bewerten und Verbesserungen basierend auf Tatsachen empfehlen zu können.

Das Tool sammelt relevante Daten aus der IT-Umgebung durch Scannen von z.B. Endpunkten, Active Directory und SharePoint Online. Darüber hinaus verwendet es einen Fragebogen, um Informationen über Richtlinien und andere wichtige Indikatoren zu sammeln.



Organisationen sind auf der Suche nach einem Weg, ihren Sicherheits-Status einfach und schnell zu überprüfen. Sie wollen Einblick in ihre Schwachstellen, basierend auf Daten aus der IT-Infrastruktur der Organisation und Office 365. Das Cyber Security Assessment Tool von QS solutions leistet dies durch automatische Scans und Analysen. Diese bilden die Grundlage, auf der CSAT-Empfehlungen und einen unmittelbaren Aktionsplan zur Verbesserung Ihrer IT-Sicherheit erstellt. CSAT ist die perfekte Lösung die Sicherheit zu optimieren und zu zeigen, dass Ihre Organisation Sicherheit sehr ernst nimmt. Dies ist auch angesichts der EU-DSGVO und anderer datenschutzrechtlichen Bestimmungen wichtig.



10. Anhang E - Hintergrund des Assessments

10.1. Einführung

Hybride IT-Strategien - die Integration zwischen traditionellen, lokalen IT-Infrastrukturen und Cloud-Plattformen - sind zum Standard für nahezu jede Organisation geworden. Dies hat das Aufgabenfeld der Cybersecurity erheblich erweitert. Die traditionell eher minimalistische und von Natur aus statische Denkweise in der IT-Sicherheit ist mit der Cloud nicht mehr ausreichend, da sich die IT-Landschaft ständig erweitert und in einem immer schnelleren Tempo verändert. Die Verantwortung der Geschäftsbereiche für die Sicherheit und klare Anweisungen zum benötigten Sicherheitsniveau sind grundlegend für Schutz der Assets des Unternehmens.

Diese veränderten Rahmenbedingungen erfordern ein umfassendes Cybersecurity-Programm. Die tägliche Praxis muss in Einklang stehen mit den heutigen Bedrohungen und Risiken, die sich gegenüber früher erheblich verändert haben:

Traditionelle IT-Umgebungen	Moderne IT-Umgebungen
„Skript-Kiddies“ und Cyber-Verbrechen	Cyber-Spionage; Cyber-Krieg
Einzelne Cyber-Kriminelle	(Fremd) gesponserte Aktionen durch grosse Hacker-Gruppen mit fast unbegrenzten Ressourcen
Angriffe auf die <i>Fortune 500</i> und multinationale Unternehmen	Alle Sektoren sind betroffen, selbst kleine und mittlere Organisationen
Unternehmenseigene, streng verwaltete Geräte	(Nicht) verwaltete Bring Your Own Device (BYOD) und/oder Choose Your Own Device (CYOD) Richtlinien
Auf das Geschäft/Gewerbe ausgerichtete Strategie-Anforderungen	Datenschutz zentrierte Strategie ist Pflicht
Sicherheitspraxis zum Schutz von IT-Assets	Datenschutz zum Schutz der Privatsphäre

Die Anforderungen der Endanwender haben sich schnell geändert, und die Art und Weise, wie sie arbeiten, wird nicht mehr von der Organisation bestimmt. Die Denkweise wird vielmehr von den eigenen täglichen Erfahrungen mit Cloud-Diensten und deren schier unendlichen Möglichkeiten geprägt. Daten werden an vielen unterschiedlichen Orten abgelegt. Die Anwender erwarten, zu jeder Zeit von überall und von allen Geräten auf alle Daten und Anwendungen der Organisation zugreifen zu können. Das führt zu neuen Sicherheitsrisiken, weil damit grössere Teile einer Unternehmens-IT für Angreifer sichtbar werden.

Es gibt keine absolute Sicherheit, sie ist vielmehr stets von den spezifischen Bedrohungen und Risiken eines Unternehmens abhängig. Was für die eine Organisation passt, kann für die andere viel zu viel sein. Was in der einen Situation als vernünftig erachtet wird, kann für eine andere Organisation völlig unpassend sein. Es gibt nicht das Sicherheits-Konzept für alle. Ein auf einem Reifegrad basierender Ansatz kann helfen, diese Unterschiede im Umgang mit Risiken und Bedrohungen in der IT zu berücksichtigen.

Um ein messbares Sicherheits-Framework umsetzen zu können wird ein Bündel von empfohlenen Massnahmen benötigt. Aus diesem Grund verwendet das Cybersecurity Assessment das **CIS Controls™**



(v8) Sicherheits-Framework, das vom **Center for Internet Security®** (CIS) (<http://www.cisecurity.org>) veröffentlicht wurde. Siehe: Anhang E - Hintergrund des Assessments

Im Rahmen des Cybersecurity Assessments wurde das Cybersecurity Practice Level der **Muster AG** über die Beantwortung eines Fragebogens gemessen. Der Fragebogen basiert auf den Praktiken der Domänen Basic, Foundational und organizational des CIS-Control™ (v8) Sicherheits-Frameworks.

Zusätzlich zum Fragebogen wurden relevante, sicherheitsbezogene Daten zur IT-Umgebung von Muster AG gesammelt. Aus den Ergebnissen des Fragebogens und den gesammelten Daten wurden Empfehlungen, Aktionspunkte und eine kurzfristige Roadmap zur Verbesserung von Richtlinien und Praktiken in der IT-Sicherheit bei Muster AG abgeleitet.

10.2. Hintergrund des Control Frameworks (CIS)

Das CIS Controls™ (v8) Sicherheits-Framework umfasst **drei** Domänen. Die Controls sind in diese Domänen gruppiert, um die Fokussierung in der Umsetzung und im anschliessenden Betrieb zu erleichtern. Die **Basic** Controls definieren eine Baseline für die Cybersecurity, während die **Foundational** Domäne grundlegende, wichtige Massnahmen zum Schutz der IT-Assets umfasst. Die **Organizational** Domäne bietet prozess- und verfahrenstechnische Anleitungen mit proaktiven und mitigativen Steuerelementen zum Schutz der Organisation vor Bedrohungen aus dem Internet.

Die CIS Controls™ (v8) verwenden eine verallgemeinerte Annäherung an den Begriff einer Risikobewertung. Statt aus der Sicht eines bestimmten Unternehmens (z. B. einer Agentur oder einer Einrichtung), wurden die CIS Controls™ (v8) auf der Basis eines Konsens-Prozesses zur Risikobewertung erstellt. Diese Konsens-Risikobewertung konsolidiert das Urteil einer grossen Gruppe von Experten aus Behörden, Industrie und Wissenschaft über die Bedrohungen und Schwachstellen, wie sie in der Regel in grösseren Unternehmen gefunden werden.

Die CIS Controls™ (v8) wurden aus den am häufigsten gefundenen Angriffsmustern abgeleitet und durch die Experten überprüft. Dadurch liefern sie eine optimale Grundlage für hochgradig wirksame Massnahmen. Das Framework versucht nicht, umfassende IT- und Sicherheitsrisiko-Management-Frameworks zu ersetzen. Die CIS Controls™ (v8) konzentrieren sich stattdessen auf eine kleinere Zahl einfach umsetzbarer Steuerelemente mit hoher Hebelwirkung und grossem Nutzen.

Für das Cybersecurity Assessment werden die technischen CIS Controls™ (v8) bei den Organizational Controls um eine Auswahl von highlevel Steuerelementen aus dem ISO/IEC 27001:2013 Framework erweitert. Die Fragen hierzu beziehen sich auf IT- und Data Governance und umfassen die Bereiche Richtlinien, Compliance, Risikomanagement und Datenschutz.

10.3. SOM-Modell

Sind im Fall a) z. B. die meisten Prozesse auf Level 3, aber ein Prozess ist auf Level 1, so wird die gesamte Organisation mit Level 1 bewertet. Die Bewertung nach a) weist somit auf das höchste Bedrohungsrisiko hin, während die Bewertung nach b) mehr den grundsätzlichen Vorbereitungsgrad der Organisation im Hinblick auf die Abwehr von Cyberangriffen reflektiert. Die folgende Abbildung zeigt die Ebenen des Modells:



Die Gesamt-Beurteilung einer Organisation bestimmt sich a) aus der niedrigsten Punktzahl in einer der untersuchten Komponenten als schwächstem Glied der Kette sowie b) aus dem Durchschnitt der erreichten Punktzahlen aller untersuchten Komponenten.

Ausgabe CSAT – Status SMB

Endpoint Name	SMBv1	SMBv2	SMBv3
	Yes	Yes	No
	Yes	Yes	No

Ausgabe CSAT - Fortschritt des Reifegrads im Companyscore

Unternehmens-Score



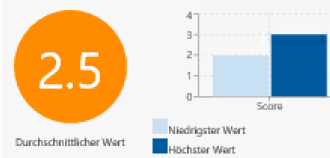


Reifegrad nach CISv8 Basic

1. BESTANDSAUFNAHME UND KONTROLLE DER HARDWARE-ASSETS



2. BESTANDSAUFNAHME UND KONTROLLE DER SOFTWARE-ASSETS



3. KONTINUIERLICHES SCHWACHSTELLEN-MANAGEMENT



4. KONTROLLIERTE NUTZUNG VON ADMINISTRATORRECHTEN



5. SICHERE KONFIGURATION VON HARD- UND SOFTWARE AUF MOBILEN GERÄTEN, LAPTOPS, WORKSTATIONS UND SERVERN



6. PFLEGE, ÜBERWACHUNG UND ANALYSE VON LOG-DATTEIN



Reifegrad nach CISv8 Foundation

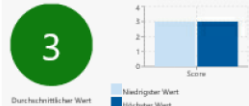
7. SCHUTZ VON E-MAIL UND WEB BROWSER



8. SCHUTZ VOR MALWARE



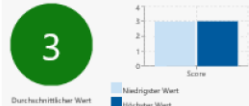
9. BESCHRÄNKUNG UND KONTROLLE VON NETZWERK-PORTS, -PROTOKOLLEN UND -DIENSTEN



10. FÄHIGKEIT ZUR WIEDERHERSTELLUNG VON DATEN



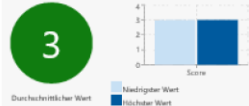
11. SICHERE KONFIGURATION VON NETZWERK-KOMPONENTEN WIE FIREWALLS, ROUTERN UND SWITCHES



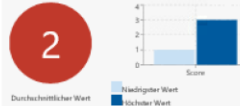
12. VERTEIDIGUNG VON NETZWERK-GRENZEN



13. SCHUTZ VON DATEN



14. ZUGRIFFSKONTROLLE NACH DEM NEED-TO-KNOW-PRINZIP



15. WLAN ZUGANGSKONTROLLE

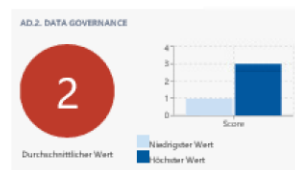
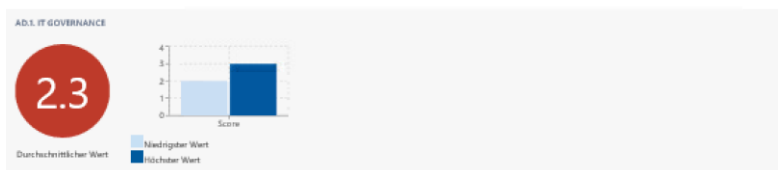
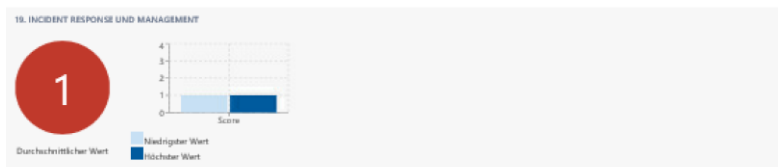
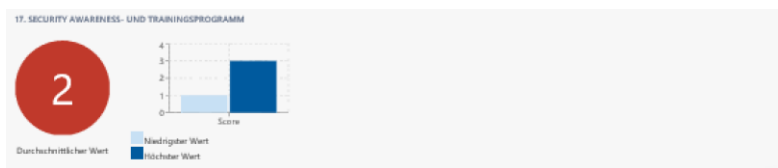


16. MONITORING UND KONTROLLE VON BENUTZERKONTEN





Reifegrad CISv8 Organizational



10.4. Abnahme und Empfehlung

Mit der Unterzeichnung dieses Dokumentes sind die Empfehlungen/Massnahmen und das Cybersecurity Assessment abgeschlossen.

Muster AG

sec4it

Peter Muster

Head of IT Systems

(Chief System Architect

Unterschrift:

Unterschrift:

Ort und Datum:

8000 Muster, XX.YY.2026

Ort und Datum: