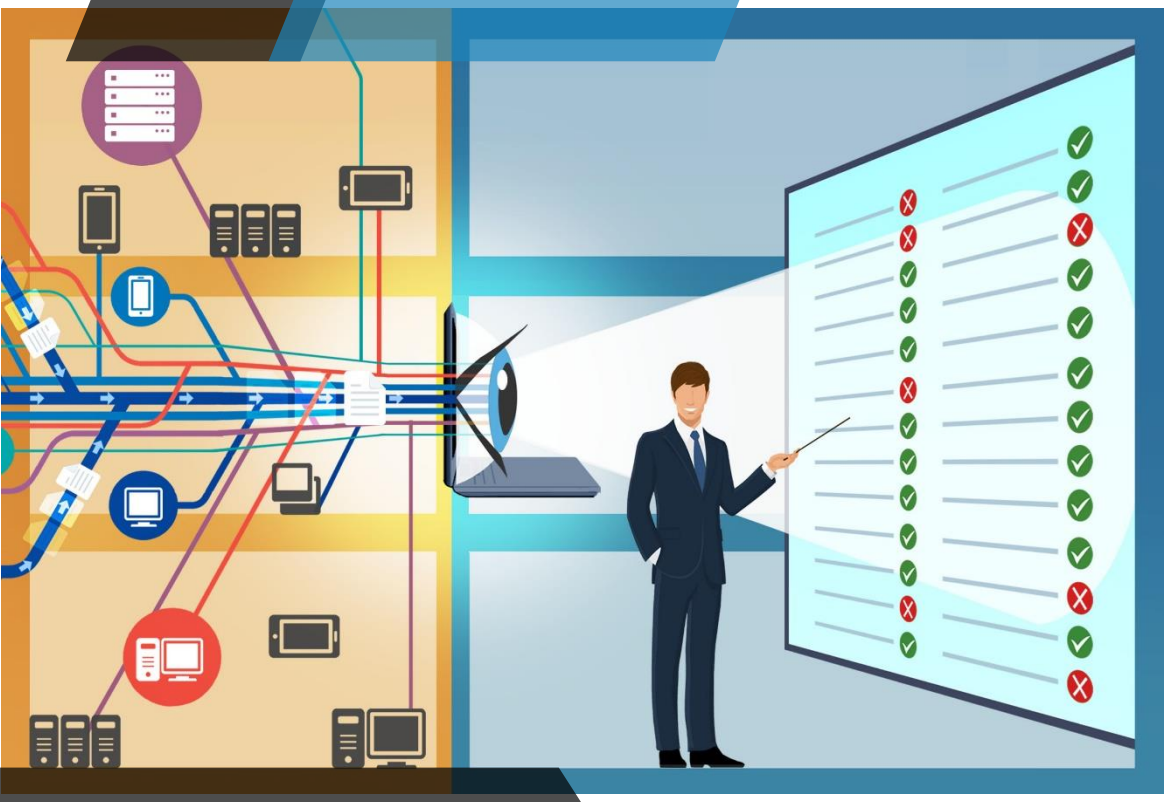
CSAT



Cybersecurity Report

Inhalt

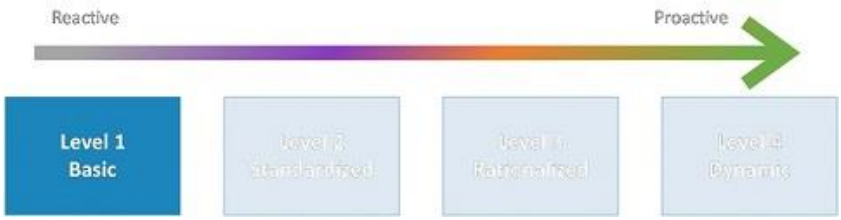
1. Zusammenfassung für das Management

Dieses Dokument ist Teil des Cybersecurity-Assessments, das im April 2021 für Contoso GmbH Contoso (in Folge) durch QS solutions durchgeführt wurde. Es bietet eine umfassende Überprüfung Ihres Programms zur IT-Sicherheit und dessen Umsetzung mit Hilfe eines Fragebogens und eines automatisierten Scans von sicherheitsrelevanten Daten und implementierten Einstellungen.

Der Bericht soll ist kein ausführlicher Kontrollbericht und auch kein Sicherheits-Audit. Gleichwohl kann er helfen, Sie darauf vorzubereiten. Darüber hinaus können die Ergebnisse als Aktionsplan verwendet werden, um die erkannten Risiken abzumildern und die Sicherheitslage Ihres Unternehmens und die Ausfallsicherheit zu verbessern.

1.1. Reifegrad des Unternehmens

Die Überprüfung des Status im Hinblick auf jedes der so genannten CIS Controls™ (v7.1 - später ausführlich erläutert) hat zu der folgenden Beurteilung des Reifegrads von Contoso geführt:



Dieser Wert basiert auf dem niedrigsten Reifegrad aller untersuchten Positionen (schwächstes Glied in der Kette).

Der Unternehmensscore berechnet sich aus dem Durchschnitt aller gegebenen Antworten des Fragebogens:

Unternehmens-Score

Er kann als Benchmark für zukünftige Bewertungen auf der Grundlage der CIS-Controls verwendet werden.

Die Größe, die Branche, das regulatorische Umfeld und andere Risikofaktoren des Unternehmens beeinflussen möglicherweise die abschließenden Empfehlungen, die mit dieser umfassenden Bewertung verbunden sind.

1.2. Strategische Betrachtungen und Empfehlungen

Eine funktionierende IT-Landschaft und deren sichere Nutzung sind essenziell für die Geschäftskontinuität. Bei Contoso werden **Sicherheitsrisiken** gesehen und bewertet und in vielen Bereichen bereits adressiert. Der Gesamteindruck ist ordentlich, was sich auch im Unternehmens-Score von 1,9 widerspiegelt, der einen Platz im Mittelfeld unter den bisher durchgeführten Assessments einnimmt. Empfohlen wird, einen Wert zwischen 2,5 und 3 anzustreben.

Allerdings sind **Richtlinien und Standards**, welche Themen von wem wie gehandhabt werden sollen, nicht ausreichend entwickelt. Solche Richtlinien sind für alle Aspekte der Cybersicherheit - organisatorische genauso wie technische - zu definieren und in der Organisation bekannt zu machen, damit das angestrebte Sicherheitslevel unabhängig von handelnden Personen gewährleistet ist.

Die operativen Aspekte der **Cybersicherheit** sollten konsequent automatisiert und ausgewertet werden. Dazu wird empfohlen, die vorhandenen Werkzeuge auszubauen und wo nötig zu ergänzen, um Einblick in Hard- und Software-Assets zu erhalten. Aus den Auswertungen sollte ein **Reporting an die Geschäftsführung** zum aktuellen Sicherheitsstatus, der Wirksamkeit der implementierten Maßnahmen und eventuellen Vorfällen abgeleitet werden. Trends aus diesen Reports sowie die Ergebnisse einer fortlaufenden **Risiko-Analyse** sollten herangezogen werden, um die **Strategie** zur IT-Sicherheit auszurichten und notwendige **Maßnahmen** identifizieren zu können. Es gilt die Balance zu finden zwischen den zu adressierenden Risiken und den eingesetzten Mitteln.

Hundertprozentige Sicherheit gibt es in der IT nicht, ist auch nicht wirtschaftlich sinnvoll und nicht einmal vom Gesetzgeber gefordert. Daher ist es wichtig, zusätzlich zu einem angemessen hohen Sicherheitsniveau, Prozeduren und **Vorgehensweisen für den Schadensfall** definiert und geübt zu haben. Kurze Reaktionszeiten, festgelegte Benachrichtigungsketten und eine saubere Dokumentation sowohl der Prozeduren als auch der einzelnen Vorfälle sind wichtig, um Ausfallzeiten, Imageschaden und - gerade in Zeiten der DSGVO - mögliche empfindliche Geldbußen abzuwenden.

Dabei ist Cybersecurity nicht nur ein IT-Thema. Die meisten Bedrohungen stehen in direktem Zusammenhang mit Endbenutzern. **Schulungen von Mitarbeitern** zu Sicherheit und Datenschutz und das damit verbundene flächendeckende Bewusstsein für IT-Sicherheit sind nicht genügend entwickelt. Setzen Sie ein für alle Mitarbeiter verpflichtendes Trainingsprogramm zur IT-Sicherheit auf, in dem Wissen vermittelt und insbesondere die richtigen Verhaltensweisen trainiert werden. Überprüfen Sie den Erfolg der Maßnahmen. Dieses Schulungsprogramm sollte vom Management-Team von Contoso sichtbar mitgetragen werden, damit es von den Mitarbeitern nicht als IT-Veranstaltung unterbewertet werden.

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 hinein zu verlagern. 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.

Die umgesetzten Sicherheitsmaßnahmen werden bei Contoso heute eher reaktiv verwaltet. Es erfolgt keine durchgängige und **regelmäßige proaktive Überprüfung** der Wirksamkeit der implementierten Sicherheitsmaßnahmen, z.B. die Überprüfung des Patch-Standes der Computer oder die Überwachung von Firewall-Protokollen. Gerade das Überwachen von Netzwerk-Protokollen verkürzt die Zeit, die vergeht vom erfolgreichen Hacker-Angriff bis zu dessen Entdeckung und Bekämpfung. Diese Überprüfungen können teilweise automatisiert werden, erfordern aber dennoch geschultes Fachwissen und entsprechende Software-Ausstattung.

Der Aktionsplan im nächsten Kapitel zeigt im Überflug die Maßnahmen, die ergriffen werden sollten. Sie basieren auf Branchen-Controls, Architekturen und Empfehlungen, wie in Kapitel 3 erläutert. Detaillierte Bewertungsergebnisse und Empfehlungen werden in den darauffolgenden Kapiteln erläutert.

2. Aktionsplan

Die Informationen, die während des Interviews mit Ihrem Sicherheitsteam gesammelt wurden, sowie die technischen Fakten, die aus dem CSAT-Scan gesammelt wurden, führen zu Maßnahmen, die sich an aktuell empfohlenen Praktiken orientieren. Die schiere Menge kann überwältigend sein. Der folgende Aktionsplan ist unser Vorschlag, sie zu priorisieren.

Der Plan besteht aus drei Phasen. Die erste Phase ist darauf ausgerichtet, das Risiko für Rapid Cyberattacks abzumildern und "niedrig hängende Früchte" zu aktivieren (Features, die relativ einfach umzusetzen sind, jedoch mit hohen Auswirkungen zur Verhinderung von Sicherheitsvorfällen). Sie beinhaltet auch eine Modernisierung Ihrer Sicherheitsstrategie.

Die zweite Phase konzentriert sich auf Features, die Ihre IT-Umgebung weiter härten, sowie auf die Implementierung von (grundlegenden) Governance- und Berichtsfunktionen, die in Ihren Cloud-Subskriptionen enthalten sind. Die dritte Phase umfasst die Erstellung/Revision von Prozessen und die Implementierung von Lösungen, die eine längere Vorbereitungszeit erfordern.

Für Ihre Umgebung schlagen wir den folgenden Aktionsplan vor:

Phase 1 | 0-30 Tage

- Machen Sie einen Workshop zur Sicherheitsstrategie, in dem sich Ihr Team über aktuelle Sicherheitsbedrohungen und die empfohlenen Vorgehensweisen zu deren Abschwächung informiert. Moderne Architektur-Prinzipien wie Zero Trust, Empfehlungen rund um Governance und Ergebnisse von CSAT sollten Bestandteil des Workshops sein. Basierend auf den Empfehlungen können Design-Entscheidungen getroffen und dokumentiert werden, die zu einer aktualisierten Cybersecurity-Strategie führen.
- Setzen Sie die Maßnahmen aus Dringende Maßnahmen und Quickwins mit der Kennzeichnung RCA-Abschwächung 0-30 Tage um. Konzentrieren Sie sich dabei auf den Schutz von Identitäten, Geräten und Daten.
- Implementieren Sie die empfohlenen Sicherheitsfunktionen, über die Sie aufgrund Ihrer aktuellen Lizenzen (EM+S E3) bereits verfügen
- Planen Sie weitere Sicherheitsprojekte auf der Grundlage der vorhandenen Roadmap. Stimmen Sie die Prioritäten von Business und IT ab. Nicht alles was aus IT-Sicht notwendig oder wünschenswert wäre, ist finanziell oder organisatorisch zu stemmen.

Phase 2 | 30-90 Tage

- Implementieren Sie weitere empfohlene Sicherheitsfunktionen, um das Schutzniveau zu erhöhen.
- Implementieren Sie Funktionen zu M365/Azure-Governance und automatisierten Berichten.
- Validieren Sie Backups und üben Sie regelmäßig die Verfahren zu Desaster & Recovery.
- Implementieren Sie Prozesse zur Kontrolle von Identitäten und Berechtigungen
- Ermitteln und beheben Sie nicht benötigte Zugriffe auf Datei-Ablagen (intern und extern).

Phase 3 | 90+ Tage

- Überarbeiten Sie Ihre Prozesse und implementieren Sie Projekte, die mehr Zeit zur Vorbereitung und Implementierung benötigen, wie z. B. Microsoft Information Protection, Azure Cloud Application Security oder Endpoint Manager – Serverhärtung
- Modernisieren Sie die aktuelle IT-Architektur, um die Umsetzung der Zero Trust Architecture zu verbessern.
- Deaktivieren Sie nicht benötigte Legacy-Netzwerkprotokolle
- Implementieren Sie ein Lifecycle-Management: halten Sie Ihre Systeme und Software - die gesamte IT-Kette - gepatcht und aktualisiert

3. Der Ansatz von CSAT

Dieser Bericht soll Ihnen ein besseres Verständnis für die aktuelle Cybersicherheitslage Ihres Unternehmens vermitteln, sowie umsetzbare Arbeitspakete, um die erkannten Risiken zu mildern, aufzeigen. Das CyberSecurity Assessment Tool (CSAT) besteht aus einem technischen Scan Ihrer Umgebung und einem Interview auf der Grundlage bekannter CIS-Steuerelemente. Der Bericht, den Sie jetzt lesen, enthält Empfehlungen zur Verbesserung Ihrer IT-Umgebung, basierend auf allgemein empfohlenen Vorgehensweisen. Um Ihnen ein besseres Verständnis unseres Ansatzes zu geben, hier zunächst eine kurze Einführung in CIS, Zero Trust Security und Rapid Cyberattacks.

3.1. Center for Internet Security

Das Center for Internet Security® (CIS) ist eine gemeinnützige Organisation, die für die CIS Controls® und CIS Benchmarks™ verantwortlich ist. Die Organisation stellt weltweit anerkannte Best Practices für die Sicherung von IT-Systemen und -Daten zur Verfügung. Die weltweite CIS-Community von IT-Experten entwickelt diese Standards kontinuierlich weiter, um proaktiv gegen aufkommende Bedrohungen zu schützen.

Der CSAT-Fragebogen basiert auf den CIS Controls und zielt darauf ab, relevante Informationen zu Ihren IT-Prozessen zu liefern. Darüber hinaus enthält der Fragebogen auch einige Fragen im Zusammenhang mit Steuerelementen der ISO27001. Weitere Informationen zum Center for Internet Security finden Sie unter https://cisecurity.org.

3.2. Zero Trust-Sicherheitsarchitektur

Die Prinzipien der Zero Trust Security-Architektur werden von der Open Group definiert, einem globalen Konsortium, das die Erreichung von Geschäftszielen durch Technologiestandards ermöglicht. Die Open Group arbeitet mit über 790 Organisationen zusammen, die Kunden, Systeme- und Lösungsanbieter, Tool-Anbieter, Integratoren, Akademiker und Berater aus verschiedenen Branchen umfassen. Organisiert in verschiedenen Arbeitsgruppen erfassen, klären und integrieren sie aktuelle und aufkommende Anforderungen, stellen Standards und Richtlinien fest und teilen Best Practices. Diese Standards gewährleisten Offenheit, Interoperabilität und Konsens.

Die Zero Trust Security Architecture ist ein Konzept, das fortlaufend neue Aspekte aufnimmt. Basierend auf dem Whitepaper "Zero Trust Core Principles" haben Unternehmen wie IBM und Microsoft diese Prinzipien bereits in ihre Referenzarchitekturen integriert. Dies hilft Organisationen dabei, die Lösungen und Produkte, die sie kennen, dem ZTA-Paradigma zuzuordnen.

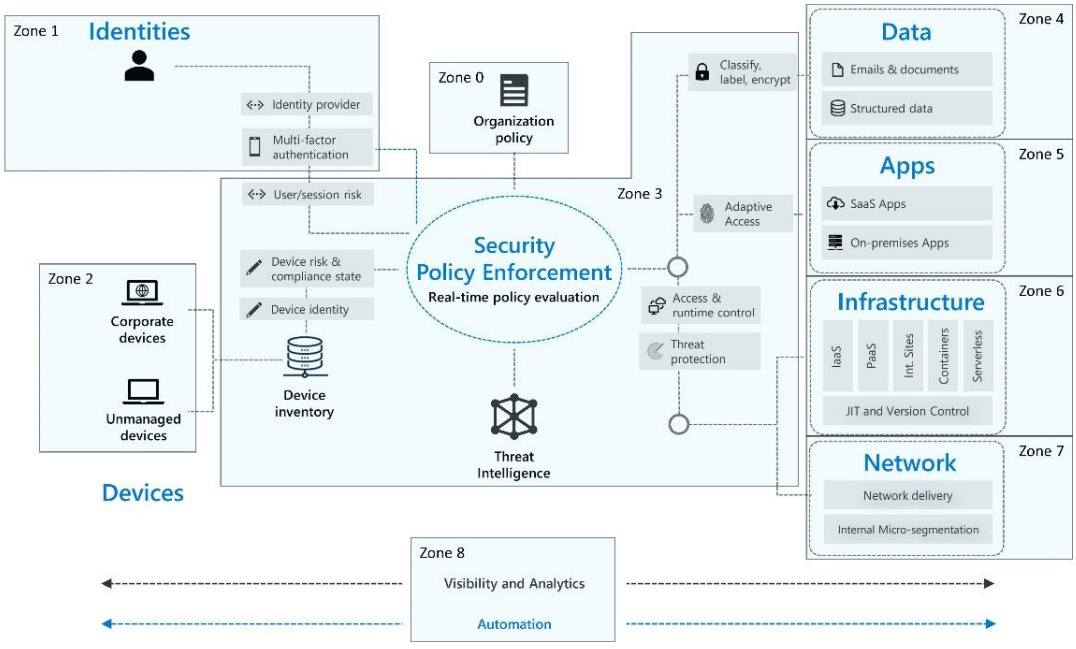
Die Architekturprinzipien sind produktunabhängig, und es liegt an der Strategie Ihres Unternehmens, mit welchen Produkten und Lösungen Sie sie letztendlich umsetzen. Da wir meist IT-Umgebungen bewerten, die aus Microsoft-basierten On-Premises und Cloud-Lösungen bestehen, basieren unsere Empfehlungen auch auf den von Microsoft empfohlenen Verfahren sowie auf der Zero Trust Reference Architecture.

Weitere Informationen finden Sie unter https://theopengroup.org und https://www.microsoft.com/en/security/business/zero-trust.

Die Prinzipien von Zero Trust sind:

1. Explizit zu prüfen
   Authentifizieren und autorisieren Sie immer basierend auf allen verfügbaren Daten, einschließlich Benutzeridentität, Standort, Geräteintegrität, Dienst oder Workload, Datenklassifizierung und Anomalien.
2. Verwenden Sie Least Privileged Access.
   Schränken Sie den Benutzerzugriff mit Just-in-time und Just-enough-access (JIT/JEA), risikobasierenden adaptiven Policies und Datenschutz ein, um sowohl Daten als auch Produktivität zu sichern.
3. Gehen Sie von einer Sicherheitsverletzung als Grundzustand aus.
   Minimieren Sie den Strahlradius von Sicherheitsverletzungen und verhindern Sie seitliche Bewegungen, indem Sie den Zugriff durch Netzwerk, Benutzer, Geräte und Apps segmentieren. Stellen Sie sicher, dass alle Sitzungen end-to-end verschlüsselt sind. Verwenden Sie Analytics, um Sichtbarkeit zu erreichen, die Erkennung von Bedrohungen zu steuern und die Abwehr zu verbessern.

Anstatt davon auszugehen, dass alles hinter der Unternehmensfirewall sicher ist, geht das Zero Trust-Modell von einer Verletzung aus und überprüft jede Anforderung, als ob sie aus einem offenen Netzwerk stammt. Unabhängig davon, wo die Anforderung ihren Ursprung hat oder auf welche Ressource sie zugreift, lehrt uns Zero Trust, "niemals zu vertrauen, immer zu überprüfen." Jede Zugriffsanforderung ist vollständig authentifiziert, autorisiert und verschlüsselt, bevor der Zugriff gewährt wird. Mikrosegmentierung und least-privileged-access Grundsätze werden angewendet, um laterale Bewegungen zu minimieren. Umfangreiche Einsicht und Analysen werden genutzt, um Anomalien in Echtzeit zu erkennen und darauf zu reagieren. Dies führt zu folgender schematischer Übersicht:



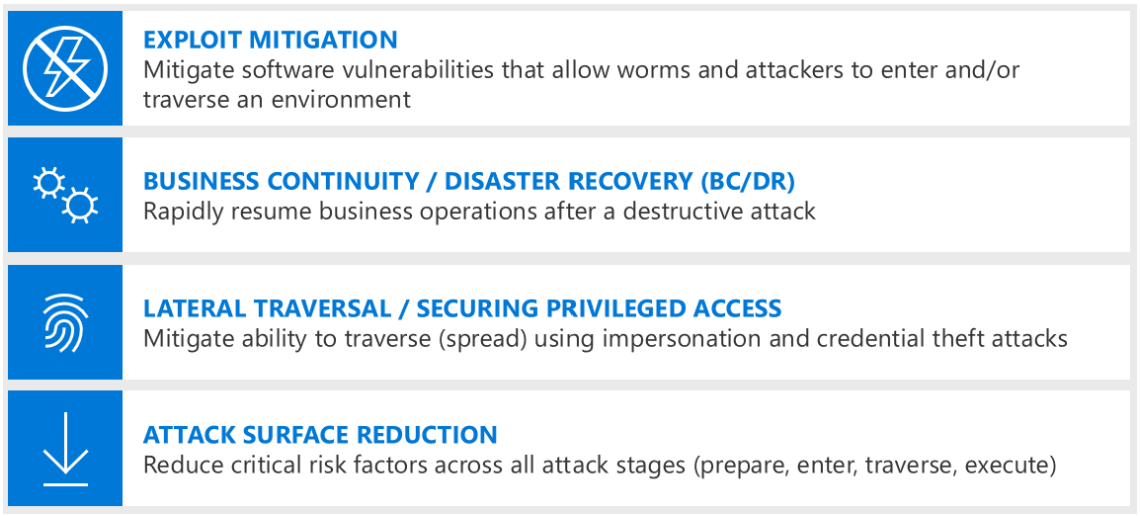
Die oben genannten Zonen korrelieren mit den jeweiligen CSAT-Empfehlungen in den Tabellen der Kapitel 4
und 5, wobei das jeweilige CIS-Control der ZTA-Zone zugeordnet wird.

3.3. Rapid Cyberattacks

Rapid Cyberattacks have become common and increasingly troublesome due to the disruptive nature of the attacks. Viele Angriffe sind erfolgreich, weil sie zum Beispiel Ihre Endnutzer ausnutzen, indem diese auf einen vertrauenswürdigen Phishing-oder Spam-Link klicken - unter Umgehung von Firewalls und Intrusion Detection Systemen. Dann, da Systeme bei Betriebssystem oder/und Software nicht auf dem neuesten oder keinem unterstützten Stand sind, Patch-Prozesse zu langsam oder gar nicht vorhanden sind oder andere Faktoren sich negativ auswirken, ist die Malware in der Lage, komplette globale Netzwerke innerhalb von Minuten zu kapern, verbunden mit der Forderung eines Lösegelds, um die Systeme wieder entriegelt zu bekommen.

Das neueste Vehikel, dass Cyber-Kriminelle vor kurzem gefunden haben, ist, System-Updates von Anwendungsanbietern zu kompromittieren, indem Trojaner in legitime Software-Updates eingeschleust werden. Diese Methode wird hauptsächlich von staatlich geförderten Organisationen verwendet, die mit ihren Angriffen bestimmte Ziele im Kopf haben. Da aber auch andere, nicht angegriffene Organisationen diese Updates erhalten, könnte die installierte Malware anderen Kriminellen einen Weg geben, diese Organisationen ebenfalls anzugreifen. Diese Entwicklungen zeigen, dass eine Strategie zur Abwehr in der Tiefe notwendiger denn je ist.

Viele Organisationen werden Opfer von Rapid Cyberattacks, wo es nur einiger einfacher Schritte bedarf, um signifkant besser dagegen gewappnet zu sein. Die wichtigsten Komponenten zur Abmilderung dieser Bedrohungen sind:



Zu den Empfehlungen in diesem Bericht gehören Meldungen, die Teil der folgenden Schlüsselaktivitäten gegen Rapid Cyberattacks sind:

Unsere Empfehlungen stammen aus den Lehren von Microsoft aus diesen Angriffen.[1]

[1] Quelle: https://aka.ms/rapidattack

4. Die wichtigsten Erkenntnisse

4.1. Dringende Maßnahmen

Um Ihnen einen kompakten Überblick über die dringendsten Erkenntnisse zu geben, haben wir diese hier zusammengefasst. Ausführliche Informationen finden Sie in den entsprechenden Controls in Kapitel 0. Wir empfehlen, die Positionen zu überprüfen und, abhängig von Ihrer Risikoaffinität und Ihren Budgetprioritäten, Ihre Auswahl dem zuvor genannten Aktionsplan oder Roadmap-/Projektplan hinzuzufügen.

Thema	Aktion	Empfohlene Softwareprodukte	ZTA-Zone	RCA-Prio
17. Security Awareness- und Trainingsprogramm	Setzen Sie ein grundlegendes Trainingsprogramm für die wichtigsten Rollen Ihrer Organisation auf. Betten Sie dieses in ein Programm zur Sensibilisierung für IT-Sicherheit und Datenschutz ein.		8	
16. Monitoring und Kontrolle von Benutzerkonten	Definieren Sie eine Standard Passwort-Policy für alle Anwendungen und Infrastruktur-Dienste. Beginnen Sie damit, MFA für alle Systeme einzurichten. Erhöhen Sie die geforderte Länge von Passwörtern, falls MFA noch nicht verfügbar ist.	Azure Multi-Factor Authentication, Conditional Access	0, 1	0-30
6. Pflege, Überwachung und Analyse von Log-Dateien	Richten Sie eine Protokollierungsplattform ein und legen Sie die Protokolle der Geräte an den Netzwerkgrenzen dort ab. Implementieren Sie einen Prozess zur Überwachung der Logs mit regelmäßiger Überprüfung auf kritische sicherheitsrelevante Einträge.	Azure Sentinel, Azure Security Center, Azure Advanced Threat Protection (ATP), Microsoft Cloud App Security	2, 3, 6, 7, 8	
4. Kontrollierte Nutzung von Administratorrechten	Implementieren Sie eine Prozedur, die Protokolle regelmäßig zu analysieren, um verdächtiges Verhalten von privilegierten Konten zu erkennen und die entsprechenden technischen Gegenmaßnahmen ergreifen.	Azure Privileged Identity Management (PIM), Azure ATP, Microsoft Cloud App Security	3, 8	30-90
3. Kontinuierliches Schwachstellen-Management	Führen Sie für die wichtigsten Systeme eine Software für Vulnerability Scans ein. Scannen Sie regelmäßig auf Lücken, speziell in Systemen mit sensiblen Informationen.	Microsoft Endpoint Manager, Microsoft Defender for Endpoints, Azure Security Center, Microsoft Cloud App Security	3, 5	0-30

3. Kontinuierliches Schwachstellen-Management	Erstellen Sie einen Prozess, um regelmäßig zu prüfen, ob die verwendeten Endpunktversionen noch unterstützt werden. Planen Sie Betriebssystem-Aktualisierungen vor dem Ende des (Mainstream-) Unterstützungsdatums.	Microsoft Endpoint Manager, Azure Security Center	2, 3	0-30
14. Zugriffskontrolle nach dem Need-to-Know-Prinzip	Trennen Sie User und Server-Systeme mittels Netzwerk-Segmentierung.		3, 6, 7	
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 Active Directory Access Reviews	1, 8	30-90
18. Sicherheit der Anwendungssoftware	Aktualisieren Sie regelmäßig alle third-party Software.	Microsoft Endpoint Manager	0, 3, 8	90+
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	0	
AD.1. IT Governance	Erstellen Sie eine Policy zu Sicherheit und Datenschutz und definieren Sie die operativen Prozesse dazu.		0, 8	
AD.1. IT Governance	Erstellen Sie eine Roadmap zur IT-Sicherheit, die alle relevanten Geschäftsziele, Compliance-Anforderungen und Pläne zur Risikominderung abdeckt.	Jährliches CSAT-Assessment, Microsoft Compliance Manager	0, 8	
AD.2. Data Governance	Definieren Sie Richtlinien zu Datenklassifizierung und -kennzeichnung und setzen Sie sie um.	Azure Information Protection Scanner, Data Loss Prevention, Azure Information Protection P2	0, 3, 4, 5	30-90

4.2. Quickwins

Die folgende Liste enthält schnell umsetzbare Maßnahmen, die für die Implementierung durch Contoso in Betracht gezogen werden sollten. Details finden Sie vielfach in Abschnitt 6.1 Technische Daten zu den CIS 20 Controls.

Thema	Aktion	Empfohlene Softwareprodukte	ZTA-Zone	RCA-Prio
Active Directory Accounts	• Überprüfen sie Konten mit riskanten UAC-Details (siehe Kapitel 6.1.16) und ändern Sie diese Einstellungen. • Bereinigen Sie alte / nicht verwendete Konten		1	
Administratoren	• Bereinigen Sie die privilegierten Gruppen des AD • Richten Sie MFA für alle Administrativen Accounts im AAD ein.	• Azure MFA	1	0-30
Sensible Assets	• Stellen Sie sicher, dass alle privilegierten Benutzer dedizierte Maschinen für ihr administrativen Aufgaben verwenden.	• Sichere, von Azure verwaltete Workstation	2	0-30
Standardkennwörter ändern	• Stellen Sie sicher, dass alle Standardkennwörter für alle Dienste und Geräte geändert werden.		1, 2, 6, 7	
Richtlinie	• Verbessern Sie die Kennwortrichtlinie (siehe Kapitel 6.1.16).		1	
Betriebssysteme	• Migrieren Sie die (fast) End-of-Life-Betriebssysteme • Isolieren Sie Endpunkten, die nicht aktualisiert oder gepatcht werden können oder legen Sie sie still.	• Windows Server 2016 oder 2019 • Windows 10	2 7	0-30
AD Computer	• Löschen Sie alte oder nicht verwendete Computerkonten aus dem AD.	•		
Sichere Konfiguration	• Stellen Sie sicher, dass SMB V1.0 deaktiviert ist • Stellen Sie sicher, dass NLA erzwungen wird, wenn RDP aktiviert ist.	•	7	90+
Schutz von E-Mail	• Überprüfen Sie SPF- und DMARC-Datensätze.	•	6	
Antivirus	• Aktualisieren Sie veraltete Virendefinitionen • Kontrollieren Sie regelmäßig den Status des Virenschutz.	• Defender for Endpoints	3, 6, 7	0-30
Firewalls	• Aktivieren Sie die Firewalls auf allen Endpunkten, auch in der Domäne.	• Windows Firewall	3, 6, 7	
Festplattenverschlüsselung	• Aktivieren Sie Festplattenverschlüsselung auf *allen* Endpunkten.	• BitLocker	2, 3, 4	

5. CIS Interview - Ergebnisse und Empfehlungen

Neben dem Unternehmens-Score geben die den CIS Controls™ (v7), sowie einer Auswahl der ISO/IEC 27001-Controls zugeordneten Ratings einen detaillierteren Einblick darüber, wie Richtlinien, Prozeduren und Management aktuell organisiert sind. Das Center for Internet Security identifiziert drei Kategorien von Kontrollgruppen: Basic, Foundational und Organizational.

In diesem Kapitel werden die jeweiligen Bewertungen auf der Grundlage des Interviews, das wir mit Ihrem Sicherheits-/IT-Personal hatten, dargestellt. Eine Bewertung stellt die aktuelle Situation dar. Abhängig von Ihrer Strategie, Richtlinien, Risikoappetit und/oder regulatorischen Anforderungen können die Ergebnisse als Orientierungshilfe dienen, welche Themen Ihr Team adressieren sollte, um Ihre Sicherheitsbewertung im nächsten Assessment zu verbessern.

5.1. Basic CIS Controls

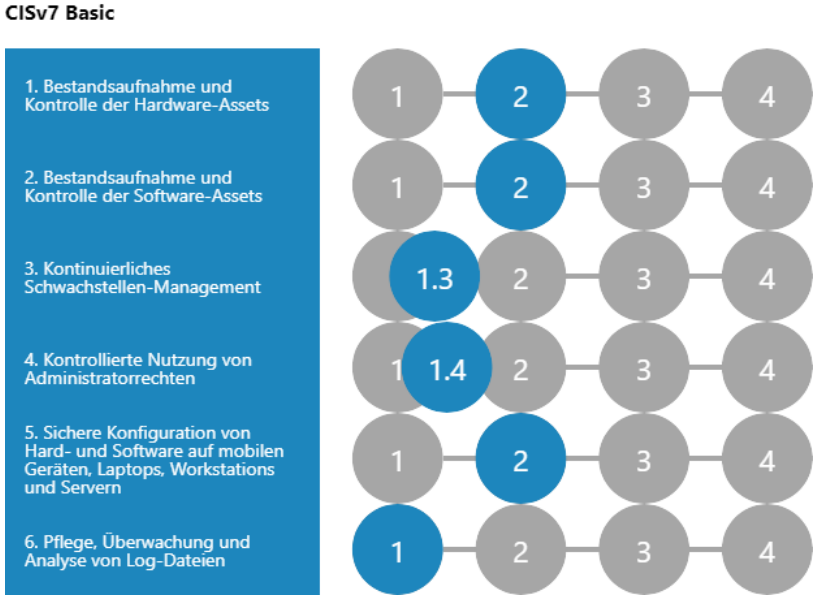
Die Basic CIS Controls beziehen sich auf Inventarisierung, Abgrenzung und Kontrolle Ihrer IT-Umgebung. Die Controls und ihre Ziele werden im Folgenden beschrieben. Die ZTA-Spalte ordnet die Controls wie in Kapitel 3 erwähnt der Zero Trust Architecture-Zone zu.

Thema	Ziel	ZTA-Zone
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.	3
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
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.	3, 8
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.	1
5. Sichere Konfiguration von Hard- und Software	Rigorose Prozesse für das Konfigurations- und Änderungsmanagement von mobilen Geräten, Laptops, Workstations und Servern, zusammen mit einer aktiven Verwaltung	3

für mobile Geräte, Laptops, Workstations und Server	(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.	8

5.1.1. Basic CIS Controls - Sicherheitsbewertung

Basierend auf den Antworten zu den Basic Controls zeigt die unten stehende Grafik Ihre aktuelle Sicherheitsbewertung.



5.1.2. Basic CIS Controls - Ergebnisse und Empfehlungen

Die folgenden Maßnahmen können helfen, Ihre Position bei den Basic CIS Controls zu verbessern. Die in der Themenspalte angegebene Zahl korreliert mit dem jeweiligen Control.

Dringend						
Thema	**Frage**	**Antwort**	**Empfehlung**	**Empfohlene Produkte**	**ZTA-Zone**	**RCA-Prio**
3. Kontinuierliches Schwachstellen-Management	Sind Discovery-Tools implementiert, die Schwachstellen in Software und Konfigurationen auf den Systemen innerhalb der Infrastruktur der Organisation identifizieren?	Basic (1) Nicht implementiert	Führen Sie für die wichtigsten Systeme eine Software für Vulnerability Scans ein. Scannen Sie regelmäßig auf Lücken, speziell in Systemen mit sensiblen Informationen.	Microsoft Endpoint Manager, Microsoft Defender for Endpoints, Azure Security Center, Microsoft Cloud App Security	3, 5	0-30
3. Kontinuierliches Schwachstellen-Management	Verwenden Sie Betriebssystemversionen, die nicht mehr aktualisiert werden können? (End of Service/Out of Support)	Basic (1) Nicht unterstützte Betriebssysteme sind vorhanden, kein Plan zur Abhilfe vorhanden Begründung u.a.: Es gibt veraltete Betriebssysteme, die auf Geräten genutzt werden, welche an Produktionsmaschinen angeschlossen sind. Dadurch sind Updates unmöglich, da die	Erstellen Sie einen Prozess, um regelmäßig zu prüfen, ob die verwendeten Endpunktversionen noch unterstützt werden. Planen Sie Betriebssystemaktualisierungen vor dem Ende des (Mainstream-) Unterstützungsdatums.	Microsoft Endpoint Manager, Azure Security Center	2, 3	0-30

		Produktionsmaschine kein Update zulässt.				
4. Kontrollierte Nutzung von Administratorrechten	Hat jeder Administrator einen persönlichen Admin-Account zusätzlich zu seinem normalen Benutzer-Account, abgesichert mit MFA und Just-in-Time-Berechtigungen, und eine dedizierte Workstation für die administrativen Aufgaben?	Basic (1) Nicht implementiert Persönlichen Admin-Account gibt es mit möglichst genau definierten Rechten. MFA, dedizierte Workstation, etc gibt es nicht.	Führen Sie persönliche Admin-Accounts und dedizierte administrative Workstations ein, zusammen mit MFA für administrative Zugriffe von außen.	Azure AD Privileged Identity Management (PIM), Privileged Access Management (PAM), Azure Multi-Factor Authentication, Privileged Access Workstations	1, 3	0-30
4. Kontrollierte Nutzung von Administratorrechten	Gibt es einen laufenden Prozess zur Überprüfung der Berechtigungen, um sicherzustellen, dass jede Person mit Administratorrechten von einem leitenden Angestellten autorisiert ist?	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	8	
4. Kontrollierte Nutzung von Administratorrechten	Werden privilegierte Konten auf verdächtiges Verhalten überwacht, z.B. erfolglose Anmeldungen und Änderungen in Gruppen mit administrativen Rechten?	Basic (1) Nicht implementiert Gruppe der Domänenadmins (de.ig.sys) wird aktiv überwacht. AD-Audit Tool existiert, kann auch Daten liefern,	Implementieren Sie eine Prozedur, die Protokolle regelmäßig zu analysieren, um verdächtiges Verhalten von privilegierten Konten zu erkennen und die entsprechenden technischen Gegenmaßnahmen ergreifen.	Azure Privileged Identity Management (PIM), Azure ATP, Microsoft Cloud App Security	3, 8	30-90

		wird jedoch nur auf Anfrage geprüft.				
6. Pflege, Überwachung und Analyse von Log-Dateien	Wurden alle Geräte und Server, einschließlich Domänencontrollern, Firewalls und eingehenden und ausgehenden Proxys, so konfiguriert, dass der gesamte Datenverkehr (sowohl zulässig als auch blockiert) und fehlgeschlagene Anmeldeversuche ausführlich protokolliert werden? Werden die Protokolle zentral gesammelt, gegen Manipulation geschützt und für die ständige Erkennung und Meldung verdächtiger Aktivitäten verwendet?	Basic (1) Nicht implementiert	Richten Sie eine Protokollierungsplattform ein und legen Sie die Protokolle der Geräte an den Netzwerkgrenzen dort ab. Setzen Sie eine Security Information and Event Management (SIEM)-Lösung auf und aggregieren Sie die 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	2, 3, 6, 7, 8	
6. Pflege, Überwachung und Analyse von Log-Dateien	Kontrolliert und analysiert der Sicherheitsbeauftragte oder 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.		8	

Hoch						
Thema	**Frage**	**Antwort**	**Empfehlung**	**Empfohlene Produkte**	**ZTA-Zone**	**RCA-Prio**
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?	Standardized (2) In begrenztem Umfang implementiert	Erweitern Sie den Umfang des/der Discovery-Tools auf die gesamte IT-Infrastruktur.	Microsoft Endpoint Manager, Network Discovery-Lösung	3, 6, 7, 8	
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 Unternehmensnetzwerk verbinden können?	Standardized (2) In begrenztem Umfang implementiert Für WLAN umgesetzt.	Übernehmen Sie den 802.1x-Standard, um Geräte zu authentifizieren, bevor sie sich mit dem Netzwerk verbinden.	Microsoft Endpoint Manager, 802.1.x	3, 6, 7, 8	
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 iOS + Windows ja (95%), Mac OS + Linux nein (5%)	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 for Endpoints	3, 5	
2. Bestandsaufnahme und Kontrolle der Software-Assets	Ist Software Whitelisting implementiert, um auf allen Systemen der Organisation nur autorisierte Softwareprogramme zur Ausführung zuzulassen?	Standardized (2) Für einige Systeme implementiert Mac OS + Linux: Nicht	Weiten Sie das Software Whitelisting auf alle Systeme aus.	Microsoft Endpoint Manager, AppLocker, Windows Defender Application Control, Azure Security	3, 4	90+

		iOS: Whitelisting mit Quarantänemodus bei Missachtung Windows: Windows Store geblockt / durch Private Store ersetzt, Applocker		Center, Microsoft Cloud App Security		
3. Kontinuierliches Schwachstellen-Management	Ist eine automatisierte Lösung für das Patch Management implementiert, die die fortlaufende Aktualisierung aller System der Organisation sicherstellt?	Standardized (2) Für einige Systeme implementiert Windows Client + Server hat Automatismen, aber nicht für 100% aller Endpoints (Validierung, Uralt-OS, etc). Windows Server (aktuelle OS) befinden sich jedoch in einem sehr hohen Grad der Aktualität. iOS, Mac OS, Linux hat keine automatisierte Lösung	Erweitern Sie den Scope Ihres Patch Management Tools auf die gesamte IT Infrastruktur. Untersuchen Sie alle nicht gepatchten Systeme.	Microsoft Endpoint Manager, Windows Server Update Services (WSUS), Azure Security Center	3	0-30
4. Kontrollierte Nutzung von Administratorrechten	Sind alle Standard-Admin-Passwörter für Anwendungen, Betriebssysteme, Drucker, Firewalls, Wireless Access Points und andere (IOT) Geräte in einmalige Passwörter geändert? Entsprechen die	Standardized (2) Für einige Systeme implementiert 80-90% geändert, gibt Einzelanwendungen und Geräte (Drucker) wo Standard-PWs	Stellen Sie sicher, dass alle von außen zugänglichen / sichtbare Geräte berücksichtigt sind. Fahren Sie fort, die Passwörter der Systeme mit dem	Azure Security Center	2, 3, 6, 7	

	verwendeten Kennwörter der Richtlinie für privilegierte Konten?	nicht geändert wurden.	höchsten Risiko zu ändern.			
4. Kontrollierte Nutzung von Administratorrechten	Haben Sie eindeutige Kennwörter für lokale Administratorkonten für jedes System implementiert? Haben Sie ein zentrales Management für lokale Admin-Konten implementiert?	Standardisierte (2) Lokale Administratorkonten haben das gleiche Passwort auf mehreren Systemen. LAPS für Windows Clients wird aktiv genutzt, konzernweit. LAPS für Windows Server ist geplant, aber nicht umgesetzt.	Implementieren Sie eine Lösung, um die lokalen Adminkonten zentral zu verwalten; implementieren Sie eindeutige Kennwörter pro System, und deaktivieren Sie die Accounts, wenn Sie sie nicht benötigen.	Local Administrator Password Solution (LAPS), Microsoft Endpoint Manager	1, 3	0-30
5. Sichere Konfiguration von Hard- und Software auf mobilen Geräten, Laptops, Workstations und Servern	Sind Discovery-Tools implementiert, die auf sämtlichen Systemen in der Infrastruktur 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 for Endpoints, Azure Security Center, Microsoft Cloud App Security	2, 3, 6, 7	
5. Sichere Konfiguration von Hard- und Software auf mobilen Geräten, Laptops, Workstations und Servern	Haben Sie auf allen Systemen auf Ihrer Sicherheitsrichtlinie basierende, sichere Hardening Baselines implementiert? Zum Beispiel Deaktivieren alter Protokolle wie SMB v1, und TLS 1.0/1.1.	Standardized (2) Für einige Schlüssel-Systeme implementiert (z.B. Web-Server, DMZ Server) Rudimentär (Windows Firewall, UAC, Windows-Apps)	Definieren Sie Hardening-Vorgaben für alle Systeme, wobei diese standardmäßig so weit wie möglich abgeschlossen sein sollten.	Azure VMs, Azure CIS Hardened Images, Microsoft Endpoint Manager	2, 3, 6, 7	30-90 (Protokolle)

5.2. Foundational CIS Controls

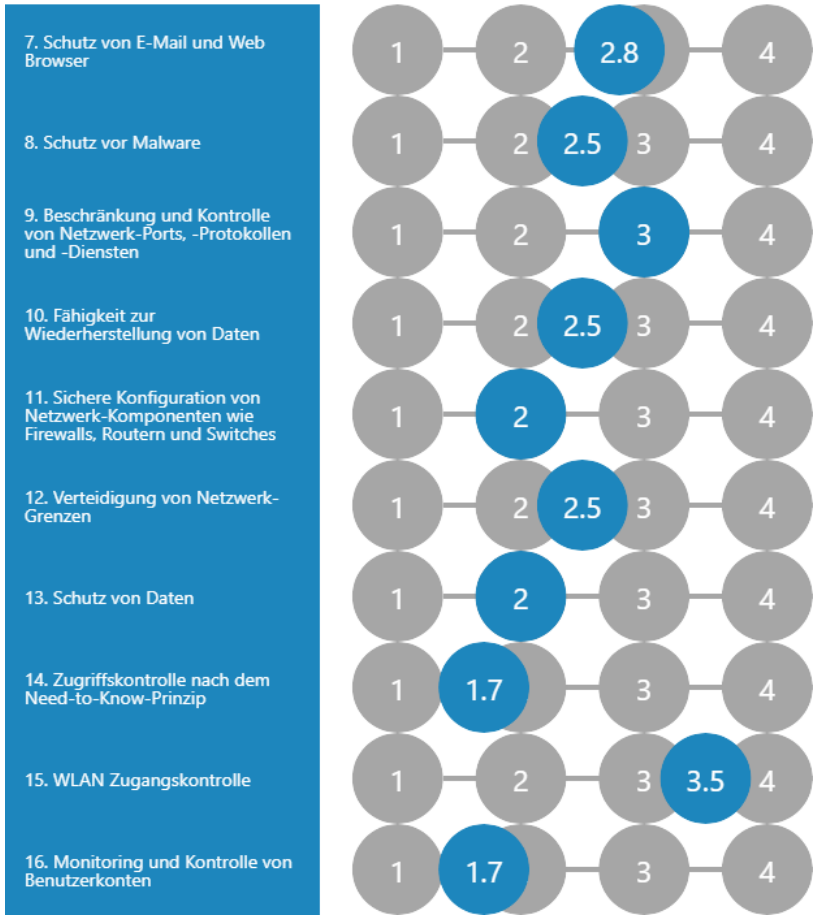
Die Foundational CIS Controls konzentrieren sich hauptsächlich auf die Sicherung von Assets mit Hilfe von Technologie in der gesamten IT-Umgebung und auf die Erkennung von Bedrohungen. Die Controls und ihre Ziele werden im Folgenden beschrieben.
Die ZTA-Spalte ordnet die Controls wie in Kapitel 3 erwähnt der Zero Trust Architecture-Zone zu.

Thema	Ziel	ZTA-Zone
7. Schutz von Email und Web Browser	Minimieren der Angriffsfläche und der Möglichkeiten für Angreifer, menschliches Verhalten mittels Web-Browser und E-Mail-Systemen zu manipulieren.	3, 4, 7
8. Schutz vor Malware	Kontrolle der Installation, Verbreitung und Ausführung von bösartigem Code an mehreren Stellen im Unternehmen. Nutzung und Optimierung von Automatismen, die eine schnelle Aktualisierung der Schutzmaßnahmen, Sammeln von Informationen und korrigierende Aktionen ermöglichen.	3
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.	6, 7
10. Fähigkeit zur Wiederherstellung von Daten	Prozesse und Werkzeuge, um kritische Informationen zu sichern und mit einer geprüften Vorgehensweise zeitnah wiederherstellen zu können.	4, 7
11. Sichere Konfiguration von Netzwerkgeräten wie Firewalls, Router und Switches	Rigorose 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.	2, 3, 6, 7, 8
12. Verteidigung von Netzwerk-Grenzen	Erkennen / Verhindern / Korrigieren des Datenflusses in informationsübertragenden Netzwerken unterschiedlicher Vertrauensstufen mit einem Schwerpunkt auf sicherheitsschädlichen Daten.	6, 7
13. Datenschutz	Prozesse und Werkzeuge zur Verhinderung von Datenverlust verringern die Auswirkungen verlorener Daten und stellen Schutz und Integrität von sensiblen Informationen sicher.	3, 4
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. WLAN Zugangskontrolle	Prozesse und Werkzeuge, um die sichere Verwendung von drahtlosen lokalen Netzwerken (WLANs), Accesspoints und WLAN-Client-Systemen zu verfolgen / kontrollieren / verhindern / korrigieren.	

5.2.1. Foundational CIS Controls - Übersicht Score

Basierend auf den Antworten zu den Foundational Controls zeigt die unten stehende Grafik Ihre aktuelle Sicherheitsbewertung.

CISv7 Foundational



5.2.2. Foundational CIS Controls - Ergebnisse und Empfehlungen

Die folgenden Maßnahmen können helfen, Ihre Position bei den Foundational Controls zu verbessern. Die in der Themenspalte angegebene Zahl korreliert mit dem jeweiligen Control.

Dringend						
Thema	**Frage**	**Antwort**	**Empfehlung**	**Empfohlene Produkte**	**ZTA-Zone**	**RCA-Prio**
7. Schutz von E-Mail und Web Browser	Werden Benutzer daran gehindert, nicht autorisierte Browser- und E-Mail-Client-Plugins und Add-On-Anwendungen zu installieren?	Basic (1) Nicht implementiert	Definieren Sie eine Richtlinie für die Verwendung von Browser- und E-Mail-Client-Plugins und Add-On-Anwendungen. Gewinnen Sie Einblick in die Nutzung.	Microsoft Endpoint manager, Microsoft Defender for Endpoints	2, 5	0-30
11. Sichere Konfiguration von Netzwerk-Komponenten wie Firewalls, Routern und Switches	Sind automatische Tools implementiert, die genehmigte Sicherheits-Standards auf Netzwerk-Geräten verifizieren und Abweichungen aufspüren?	Basic (1) Nicht implementiert	Implementieren Sie eine Network Device Management Solution.	Network Device Management Solution	3, 6, 7, 8	
14. Zugriffskontrolle nach dem Need-to-Know-Prinzip	Erfolgt die Netzwerk-Segmentierung aufgrund der Klassifizierung oder der Kennzeichnung der auf den Systemen gespeicherten Informationen?	Basic (1) Nicht implementiert	Trennen Sie User und Server-Systeme mittels Netzwerk-Segmentierung.		3, 6, 7	
16. Monitoring und Kontrolle von Benutzerkonten	Wird für alle Benutzer auf allen Systemen Multifaktorauthentifizierung (MFA) bei der Anmeldung über Richtlinien erzwungen?	Basic (1) Nicht definiert / nicht implementiert	Definieren Sie eine standard Passwort-Policy für alle Anwendungen und Infrastruktur-Dienste. Beginnen Sie damit,	Azure Multi-Factor Authentication, Conditional Access	0, 1	0-30

			MFA für alle Systeme einzurichten. Erhöhen Sie die geforderte Länge von Passwörtern, falls MFA noc nicht verfügbar ist.			
16. Monitoring und Kontrolle von Benutzerkonten	Wird die Account/Identity-Verwaltung von den jeweiligen Abteilungen betrieben mit einem verantwortlichen Besitzer für jeden Account? Werden ungenutzte Accounts nach einer bestimmten Zeit gesperrt und/oder 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 Active Directory Access Reviews	1, 8	30-90

Hoch						
Thema	**Frage**	**Antwort**	**Empfehlung**	**Empfohlene Produkte**	**ZTA-Zone**	**RCA-Prio**
8. Schutz vor Malware	Werden Anti-Malware-Ereignisse und Protokolle weitergeleitet und an einem zentralen Ort gespeichert? Wird die IT / das Sicherheitsteam automatisch alarmiert, um Maßnahmen zu ergreifen? Gibt es Berichte, um Trends zu erkennen?	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 for Endpoints, Azure Security Center, Microsoft Cloud App Security	3, 8	

9. Beschränkung und Kontrolle von Netzwerk-Ports, -Protokollen und -Diensten	Sind hostbasierte Firewalls auf allen Systemen implementiert und so konfiguriert, dass eingehender und ausgehender Datenverkehr nur für genehmigte Programme, Protokolle und Netzwerk-Ports zulässig ist?	Standardized (2) Für einige Systeme implementiert Windows Server: Windows Firewall aus Windows Client: Windows Firewall aktiv, inkl. Domänenprofil (Eingehender Verkehr unterliegt GPO, ausgehend immer frei)	Installieren oder aktivieren Sie für alle Systeme die standardmäßigen Soft-Firewalls mit den zugehörigen Standard-Konfigurationen.	Microsoft Defender for Endpoints, Microsoft Endpoint Manager	2, 7	
10. Fähigkeit zur Wiederherstellung von Daten	Hat Ihre Organisation einen Backup-Prozess, bei dem jedes System automatisch gesichert wird? Wird die Wiederherstellung vierteljährlich getestet und verifiziert?	Standardized (2) Alle Systeme (egal ob VM, Hardware oder Netzwerk) werden automatisiert gesichert. Regelmäßige Tests finden nicht statt - durch wiederkehrende Restores ist die Funktionalität jedoch gesichert. Existenz des Backups wird durch Monitoring aktiv geprüft.	Weiten Sie den Backup-Prozess auf alle Systeme aus. Testen Sie regelmäßig die Wiederherstellung.	Azure Back-up	5, 6, 8	0-30 90+ (test)
12. Verteidigung von Netzwerk-Grenzen	Erfordert jede Zugriffsverbindung von außen die Verschlüsselung des	Standardized (2) Verschlüsselung ist für alle Anmeldungen	Erzwingen Sie Verschlüsselung und MFA für Anmeldungen von außerhalb.	Azure Multi-Factor Authentication	1, 3, 6, 7	0-30

	Datenverkehrs und Multi-Faktor-Authentifizierung?	von außerhalb implementiert.				
13. Schutz von Daten	Bewerten Sie regelmäßig Daten, um sensible Informationen zu identifizieren, für die Verschlüsselung und Integritätskontrollen erforderlich sind?	Standardized (2) Auf einigen Systemen implementiert	Identifizieren Sie die sensiblen Informationen in allen Datenquellen der Organisation.	Azure Information Protection Scanner, Data Loss Prevention, Office 365 Advanced Data Governance, Azure Information Protection P2, Azure SQL Data Discovery & Classification	3, 4	
13. Schutz von Daten	Haben Sie Geräte- und Festplattenverschlüsselung auf mobilen Geräten und allen anderen Systemen, auf denen vertrauliche Daten gespeichert werden, implementiert?	Standardized (2) Auf den meisten Systemen mit sensiblen Daten implementiert (keine Server)	Aktivieren Sie Verschlüsselung auf allen Datenquellen der Organisation.	BitLocker, Microsoft Endpoint Manager, Azure Key Vault	2, 3	
14. Zugriffskontrolle nach dem Need-to-Know-Prinzip	Ist für die Kommunikation über nicht vertrauenswürdige Netzwerke die Verschlüsselung sensibler Informationen im Transit (z. B. TLS) 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.		2, 4, 6, 7	

5.3. Organizational CIS Controls

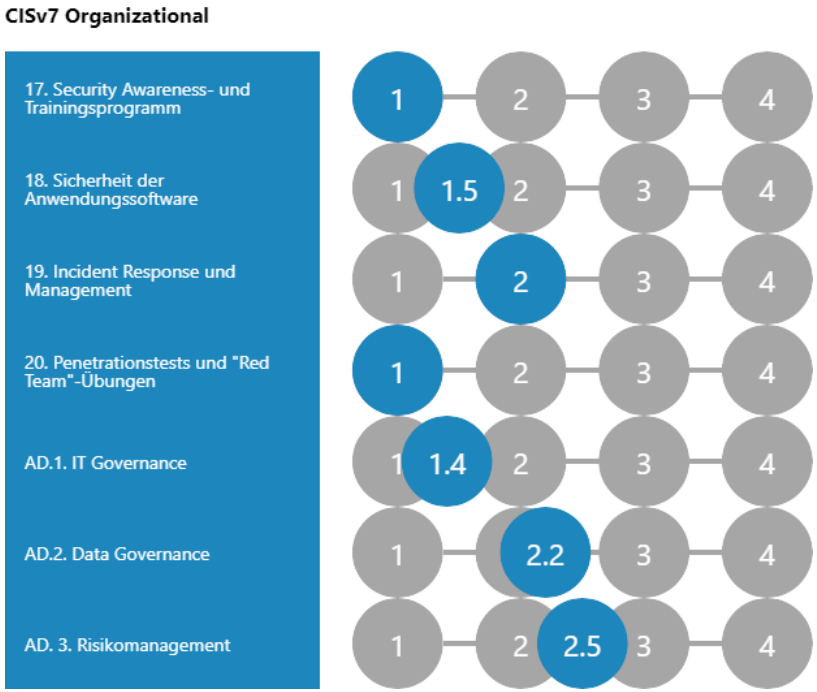
Die Organizational CIS Controls beziehen sich auf Prozesse und Abläufe der Organisation. Die Controls werden mit einer Auswahl von high-level Elementen AD.1 - 3 erweitert, die aus dem ISO/IEC 27001:2013-Framework entnommen wurden. Die zusätzlichen Fragen beziehen sich auf IT- und Data-Governance und umfassen die Bereiche Richtlinien, Compliance, Risikomanagement und Datenschutz. Die Controls und ihre Ziele werden im Folgenden beschrieben.
Die ZTA-Spalte ordnet die Controls wie in Kapitel 3 erwähnt der Zero Trust Architecture-Zone zu.

Thema	Ziel	ZTA-Zone
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.	0, 8
18. Sicherheit der Anwendungssoftware	Verwaltung des Sicherheits-Lebenszyklus für alle in-house entwickelte oder erworbene Software, um Schwachstellen zu verhindern oder zu erkennen und zu korrigieren.	0, 5, 8
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	0, 8
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	8
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.	0, 8
AD.2. Data Governance	Umsetzung gesetzlicher Datenschutzanforderungen über einen risikobasierten Ansatz, mit Fokus auf dem Schutz personenbezogener Daten (PII).	0, 8

AD.3. Risikomanagement	Risikomanagement bekommt in heutigen IT-Organisationen immer mehr Gewicht, besonders wenn regulatorische Anforderungen wie DSGVO, HiPAA, PCI-DSS und dergleichen verpflichtend sind. Ein effektives Risikomanagement hilft Ihrer Organisation, diese Risiken zu kontrollieren.	0, 8

5.3.1. Organizational CIS Controls - Übersicht Score

Basierend auf den Antworten zu den Organizational und ISO27001 Controls zeigt die unten stehende Grafik Ihre aktuelle Sicherheitsbewertung.



5.3.2. Organizational CIS Controls - Ergebnisse und Empfehlungen

Die folgenden Maßnahmen können helfen, Ihre Position bei den Organizational und ISO27001 Controls zu verbessern. Die in der Themenspalte angegebene Zahl korreliert mit dem jeweiligen Control.

Dringend						
Thema	**Frage**	**Antwort**	**Empfehlung**	**Empfohlene Produkte**	**ZTA-Zone**	**RCA-Prio**
17. Security Awareness- und Trainingsprogramm	Verfügt Ihr Unternehmen über ein Programm zur Sensibilisierung für IT-Sicherheit und Datenschutz?	Basic (1) Kein Programm zur Sensibilisierung für IT-Sicherheit und Datenschutz	Setzen Sie ein Programm zur Sensibilisierung für IT-Sicherheit und Datenschutz auf.		8	90+
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 Benachrichtigung bei Sicherheits-Vorfällen?	Basic (1) Kein Trainingsprogramm	Setzen Sie ein grundlegendes Trainingsprogramm für die wichtigsten Rollen Ihrer Organisation auf.		8	
18. Sicherheit der Anwendungssoftware	Wird sichergestellt, dass alle third-party Software immer noch supportet wird und aktuell (gepatcht) oder gemäß den Sicherheitsempfehlungen der Entwickler hinreichend gehärtet ist?	Basic (1) Nicht implementiert	Aktualisieren Sie regelmäßig alle third-party Software.	Microsoft Endpoint Manager	0, 3, 8	90+
19. Incident Response und Management	Ist eine Prozedur zur Reaktion auf Sicherheits-Vorfälle (Incident Response Procedure) definiert mit den	Basic (1) Keine Prozedur definiert	Setzen Sie eine grundlegende Incident Response Procedure auf, die die häufigsten	Office 365 Advanced Compliance:	0	

	passenden Benachrichtigungen, Zusammenstellung von Daten, Verantwortlichkeiten, gesetzeskonformen Protokollierungen und Kommunikations-Stragie?		Szenarien abdeckt. Trainieren und leben Sie diesen Prozess	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 Infrastruktu der Organisation und verwenden diesen als Input für Penetration Tests.	Microsoft Endpoint Manager, Microsoft Defender for Endpoints, Azure Security Center, Pen testing tools	3, 8	
AD.1. IT Governance	Haben Sie eine von der Geschäftsleitung des Unternehmens definierte und bestätigte Sicherheits- und Datenschutzrichtlinie?	Basic (1) Datenschutzpolicy existiert, aber keine Sicherheitsrichtlinie	Erstellen Sie eine Policy zur IT-Sicherheit und definieren Sie die operativen Prozesse dazu.		0, 8	
AD.1. IT Governance	Wie ist die Trennung von funktionalen 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.	Azure AD Identity Governance	0	
AD.1. IT Governance	Haben Sie einen Plan / eine Roadmap zur Verbesserung der IT-Sicherheit, der von der Geschäftsleitung unterstützt wird? Passt diese Roadmap zur Geschäftsstrategie?	Basic (1) Kein Plan oder Roadmap zur IT-Sicherheit definiert.	Erstellen Sie eine Roadmap zur IT-Sicherheit, die alle relevanten Geschäftsziele, Compliance-	Jährliches CSAT-Assessment, Microsoft Compliance Manager	0, 8	

			Anforderungen und Pläne zur Risikominderung abdeckt.			
AD.2. Data Governance	Sind Datenklassifizierung und -kennzeichnung in der gesamten Organisation implementiert?	Basic (1) Keine Datenklassifizierung und/oder keine Datenkennzeichnung	Definieren Sie Richtlinien zu Datenklassifizierung und -kennzeichnung und setzen Sie sie um.	Azure Information Protection Scanner, Data Loss Prevention, Azure Information Protection P2	0, 3, 4, 5	30-90

Hoch						
Thema	**Frage**	**Antwort**	**Empfehlung**	**Empfohlene Produkte**	**ZTA-Zone**	**RCA-Prio**
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.		0, 1, 3, 5	90+
20. Penetrationstests und "Red Team"-Übungen	Werden regelmäßig Penetrations-Tests auf allen Systemen und Anwendungen des Unternehmens 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.		8	
AD.1. IT Governance	Wird die regulatorische und gesetzliche Compliance fortlaufend überprüft und sichergestellt?	Standardized (2) Lokale legislative und regulatorische Anforderungen sind	Setzen Sie branchenspezifische Best Practice Ansätze um.	Microsoft Compliance Manager	0, 3, 8	

		umgesetzt und werden regelmäßig überprüft.				
AD.1. IT Governance	Erhält die Geschäftsleitung Berichte zur IT-Sicherheit? Werden Risiken an die kommuniziert?	Standardized (2) Das IT-Management erhält bei Bedarf Berichte zur IT-Sicherheit und wird ad-hoc über Risiken informiert.	Implementieren Sie eine Prozedur, um dem Vorstand den Status und die Risiken der IT-Sicherheit regelmäßig zu melden.	Microsoft Compliance Manager	8	
AD.2. Data Governance	Wie ist das Datenrisikomanagement in Ihrer Organisation organisiert?	Standardized (2) Risikobewertungen werden durchgeführt. Risiken werden dokumentiert und Maßnahmen zu deren Reduzierung ergriffen.	Setzen Sie einen erweiterten Risk Management Prozess um.		8	
AD. 3. Risikomanagement	Wie ist das Risikomanagement für Lieferanten und Drittanbieter, die (privilegierten) Zugriff auf Ihre Systeme und Daten haben, organisiert?	Standardized (2) Es wurde ein Prozess definiert, aber nur teilweise umgesetzt.	Erweitern sie den Prozess zur Risikobewertung auf alle Anbieter.		0, 8	

6. Gescannte Daten und deren Analyse

Neben dem Interview in Bezug auf CIS und zusätzliche Controls haben wir einen automatisierten Scan (einer Auswahl) Ihrer IT-Umgebung durchgeführt. Wir haben Informationen gesammelt, die unter anderem den aktuellen Stand der Konfiguration Ihrer IT-Landschaft, die Entdeckung personenbezogener Daten, das Identitätsmanagement, die Software-Versionierung und vieles mehr betreffen.

In diesem Kapitel werden die Fakten zusammengefasst, die wir zusammen mit dem jeweiligen Sicherheitsrisiko/der Sicherheitsbedrohung gefunden haben, sowie Empfehlungen, um diese Schwachstellen zu beheben.

6.1. Technische Daten zu den CIS 20 Controls

Die folgenden Tools wurden für die Erhebung der Informationen verwendet:

- Cyber Security Assessment Tool (CSAT).

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

CSAT stellt keine Bestandsaufnahme der Hardwareressourcen bereit. Dieses Control wird in Kapitel 5 behandelt. Die Zahlen unten wurden vom IT-Team zur Verfügung gestellt.

Inventarisierung	Typ	Anzahl	Gesamt
Physische Server	Windows	17	85
	Linux oder andere	68	
Virtuelle Server	Windows	520	
	Linux oder andere	135	
Endanwender-Geräte	Desktops Windows	1000	4580
	Desktops Mac OSx	5	
	Laptops Windows	1800	
	Laptops Mac OSx	25	
	Mobiles, Tablets	1750	

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

Ausgabe CSAT – Status Versionierung

OS ERMITTELTE ENDPUNKTE

Microsoft Windows 10 Enterprise	1267
Microsoft Windows 10 Enterprise 2016 LTSB	6
Microsoft Windows 10 Enterprise LTSC	8
Microsoft Windows 10 Entreprise	118
Microsoft Windows 10 Pro	70
Microsoft Windows 10 企业版	7
Microsoft Windows 7 Enterprise	193
Microsoft Windows 7 Professional	10
Microsoft Windows 7 Professionnel	1
Microsoft Windows 7 企业版	7
Microsoft Windows Server 2008 R2 Datacenter	19
Microsoft Windows Server 2008 R2 Enterprise	19
Microsoft Windows Server 2008 R2 Standard	22
Microsoft Windows Server 2012 R2 Datacenter	28
Microsoft Windows Server 2012 R2 Standard	91
Microsoft Windows Server 2012 Standard	2
Microsoft Windows Server 2016 Datacenter	3
Microsoft Windows Server 2016 Standard	186
Microsoft Windows Server 2019 Standard	67
Microsoft Windows XP Professional	7
Microsoft Windows 7 Entreprise	5
Microsoft(R) Windows(R) Server 2003 Standard x64 Edition	1
Microsoft(R) Windows(R) Server 2003, Standard Edition	7

Ausgabe CSAT - AD Computerkonten

AD COMPUTER ACCOUNT (ENABLED COMPUTER ACCOUNT) - AT

Aktivierte Accounts	744
Deaktivierte Accounts	289
Client OS aktiv in den letzten 30 Tagen	527
Server OS aktiv in den letzten 30 Tagen	20
Client OS mehr als 30 Tage inaktiv	158
Server OS mehr als 30 Tage inaktiv	3

AD COMPUTER ACCOUNT (ENABLED COMPUTER ACCOUNT) - DE

Aktivierte Accounts	3233
Deaktivierte Accounts	9
Client OS aktiv in den letzten 30 Tagen	2060
Server OS aktiv in den letzten 30 Tagen	423
Client OS mehr als 30 Tage inaktiv	708
Server OS mehr als 30 Tage inaktiv	38

AD COMPUTER ACCOUNT (ENABLED COMPUTER ACCOUNT) - FR

Aktivierte Accounts	366
Deaktivierte Accounts	12
Client OS aktiv in den letzten 30 Tagen	267
Server OS aktiv in den letzten 30 Tagen	26
Client OS mehr als 30 Tage inaktiv	69
Server OS mehr als 30 Tage inaktiv	4

AD COMPUTER ACCOUNT (ENABLED COMPUTER ACCOUNT) - UK

Aktivierte Accounts	111
Deaktivierte Accounts	3
Client OS aktiv in den letzten 30 Tagen	97
Server OS aktiv in den letzten 30 Tagen	11
Client OS mehr als 30 Tage inaktiv	3
Server OS mehr als 30 Tage inaktiv	0

BETRIEBSSYSTEME, DIE SICH NIE AM AD ANGEMELDET HABEN

Keine Daten	14
Windows XP Professional	22

BETRIEBSSYSTEME, DIE SICH NIE AM AD ANGEMELDET HABEN

Keine Daten	2
Windows Server 2003	1
Windows XP Professional	1

OS BEI AD ANGEMELDET (LETZTE 30 TAGE)

Keine Daten	2
Mac OS X	4
Windows 10 Enterprise	407
Windows 10 Pro	2
Windows 7 Enterprise	106
Windows 7 Professional	2
Windows Server 2008 R2 Datacenter	1
Windows Server 2008 R2 Standard	4
Windows Server 2012 R2 Standard	4
Windows Server 2016 Standard	10
Windows Server 2019 Standard	1
Windows XP Professional	4

OS BEI AD ANGEMELDET (LETZTE 30 TAGE)

Keine Daten	2
CentOS	1
Data Domain OS	3
Mac OS X	21
unknown	1
Windows 10 Enterprise	1626
Windows 10 Enterprise 2016 LTSB	12
Windows 10 Enterprise LTSC	8
Windows 10 Pro	105
Windows 10 企业版	11
Windows 7 Enterprise	233
Windows 7 Professional	17
Windows 7 企业版	9
Windows Server 2003	8
Windows Server 2008 R2 Datacenter	18
Windows Server 2008 R2 Enterprise	19
Windows Server 2008 R2 Standard	13
Windows Server 2012 R2 Datacenter	23
Windows Server 2012 R2 Standard	81
Windows Server 2012 Standard	3
Windows Server 2016 Datacenter	1
Windows Server 2016 Standard	193
Windows Server 2019 Standard	64
Windows XP Professional	11

OS BEI AD ANGEMELDET (LETZTE 30 TAGE)

Windows 10 Entreprise	248
Windows 7 Professionnel	2
Windows Server 2008 R2 Standard	3
Windows Server 2012 R2 Datacenter	3
Windows Server 2012 R2 Standard	6
Windows Server 2016 Datacenter	1
Windows Server 2016 Standard	13
Windows 7 Entreprise	17

OS BEI AD ANGEMELDET (LETZTE 30 TAGE)

Keine Daten	6
Cisco Identity Services Engine	4
Windows Server 2012 R2 Standard	1
Windows Server 2016 Standard	13
Windows Server 2019 Standard	2

OS BEI AD ANGEMELDET (LETZTE 30 TAGE)

Windows 10 Enterprise	96
Windows 10 Enterprise LTSC	1
Windows Server 2008 R2 Standard	2
Windows Server 2012 R2 Datacenter	2
Windows Server 2016 Datacenter	1
Windows Server 2016 Standard	4
Windows Server 2019 Standard	2

Schlussfolgerungen und Empfehlungen

- **Die (fast) end-of-life OS** Windows XP und 7, Windows Server 2003, 2008 und 2012 wurden gefunden. Erstellen Sie einen Plan, um diese Betriebssysteme abzulösen. Für **Windows 7 und Windows Server 2008** erhalten Sie erweiterten Sicherheitssupport, wenn Sie diese Betriebssysteme nach Azure verschieben.
- Die auf mehreren Endpunkten gefundenen **Versionen** von **Windows 10** sind nicht der neueste Stand. Die aktuelle Version von Windows 10 ist 20H2. Bringen Sie alle Endpunkte auf die jeweils aktuelle Version.
- Der Support für die Builds von Windows 10 ist zeitlich begrenzt. Es wird empfohlen, eine langfristige Strategie bezüglich der Builds von Windows 10 zu haben. Unterstützen Sie diese mit einem Tool wie Microsoft Endpoint Manager.
- Bereinigen Sie regelmäßig die Computer-Konten des AD.

Ausgabe CSAT – Installierte Anwendungen

Flag	Name Anwendung	Version	Datum erste Installation	Herausgeber	#Endpunk...
	2007 Microsoft Office Suite Service Pack 2 (SP2)			Microsoft	30
	Microsoft SQL Server 2008			Microsoft Corporation	10
	Adobe Flash Player 11 ActiveX	11.7.700.202	12.02.2021	Adobe Systems Incorporated	1
	Java 2 SDK, SE v1.4.2_15	1.4.2_15	14.03.2013	Sun Microsystems, Inc.	5
	PDFCreator	1.6.2	24.04.2014	pdfforge	34
	TeamViewer 6	6.0.10194		TeamViewer GmbH	1
	UltraVnc	1.1.9.6	23.07.2014	uvnc bvba	1
	7-Zip 9.20	9.20.00.0	04.03.2013	Igor Pavlov	8
	Adobe Reader X (10.1.4)	10.1.4	17.07.2014	Adobe Systems Incorporated	19

Schlussfolgerungen und Empfehlungen

- Die (fast) end-of-life Softwareprodukte SQL Server 2005, 2008, 2012, 2014 und Office 2007 wurden gefunden. Lösen Sie diese Produkte so schnell wie möglich ab.
- Es wurden verschiedene (alte) Versionen von Anwendungen wie Flash Player, Java, TeamViewer oder 7-Zip gefunden. Bringen Sie diese Anwendungen auf die aktuellste Version.

Alt- und (fast) end-of-life Produkte stellen ein hohes operationelles Risiko dar und erhöhen die Anfälligkeit für Bedrohungen. Produkte, die das Ende ihres Lebenszyklus erreicht haben, werden nicht mehr unterstützt, und Updates und/oder Hotfixes für Bedrohungen und Sicherheitsanfälligkeiten werden nicht mehr bereitgestellt.
Der Wechsel zu Azure verbessert die Sicherheit und erhöht die Flexibilität, Zuverlässigkeit und Skalierbarkeit im Vergleich zu einer herkömmlichen IT-Umgebung. Beginnen Sie mit der Aktualisierung aller Software-Produkte, die ihr Ende des Supports (fast) erreicht haben. Siehe Anhang B - Produkte, bei denen der Support ausläuft.

Hinweis: Microsoft bietet derzeit ein Sicherheitsupdate-Feature für Windows Server 2008-Instanzen an, wenn diese von on-premises auf virtuelle Azure-Maschinen verschoben werden. Es gelten die allgemeinen Geschäftsbedingungen.

Stellen Sie sicher, dass die Clients immer auf der stabilsten unterstützten Version der Software ausgeführt werden. Softwaretools wie **Defender for Endpoints** oder **Azure Security Center** können Ihnen helfen, Einblicke in die installierten Anwendungen auf den Endpunkten zu erhalten. Werkzeuge wie **Cloud-App-Sicherheit** können Ihnen helfen, die Verwendung von Schatten-IT-Anwendungen in der Cloud zu netdecken.

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 – Status Lizenzen

Schlussfolgerungen und Empfehlungen

- **EM+S** E3 ist in der Fläche zugewiesen, aber nicht implementiert. Prüfen Sie, welche so schon lizensierten Features die Sicherheit sinnvoll verbessern helfen können.

6.1.3. CIS Control 3: Kontinuierliches Schwachstellen-Management

Ausgabe CSAT – Status Updates

Endpunkte mit fehlenden kritischen Updates	0

Schlussfolgerungen und Empfehlungen

- Keine Endpunkte mit fehlenden kritischen Sicherheitspatches gefunden.

6.1.4. CIS Control 4: Kontrollierte Nutzung von Administratorrechten

Ausgabe CSAT – Administrative Gruppen im Active Directory

AD ADMINISTRATOREN - AT

Eingebaute Domänen-Gruppe für Administratoren	7
Domänen-Administratoren	6
Enterprise-Administratoren	0
Schema-Administratoren	0
Benutzer mit Administrator-Rechten	14

AD ADMINISTRATOREN - DE

Eingebaute Domänen-Gruppe für Administratoren	20
Domänen-Administratoren	14
Enterprise-Administratoren	0
Schema-Administratoren	0
Benutzer mit Administrator-Rechten	27

AD ADMINISTRATOREN - FR

Eingebaute Domänen-Gruppe für Administratoren	4
Domänen-Administratoren	3
Enterprise-Administratoren	0
Schema-Administratoren	0
Benutzer mit Administrator-Rechten	5

AD ADMINISTRATOREN - UK

Eingebaute Domänen-Gruppe für Administratoren	4
Domänen-Administratoren	3
Enterprise-Administratoren	0
Schema-Administratoren	0
Benutzer mit Administrator-Rechten	5

Schlussfolgerungen und Empfehlungen

- **In den integrierten Administratoren-Gruppen im Forest** wurde eine hohe Anzahl von Administratoren gefunden. Die Mitglieder dieser Gruppen haben die volle Kontrolle über die Domänencontroller, daher sollte die Mitgliedschaft so weit wie möglich begrenzt werden. Überprüfen Sie diese Gruppe und bereinigen Sie alte / nicht verwendete Benutzerkonten.
- **Es wurde eine hohe Anzahl von Domänenadministratoren gefunden**. Die Mitglieder dieser Gruppe haben die volle Kontrolle über die Domäne, daher ist die Mitgliedschaft so weit wie möglich zu begrenzen. Überprüfen Sie diese Gruppe und bereinigen Sie alte / nicht verwendete Benutzerkonten.
- **Es wurde eine hohe Anzahl von Enterprise-Administratoren gefunden**. Die Mitglieder dieser Gruppe haben die volle Kontrolle über alle Domänen in einem Forest. Diese Gruppe enthält idealerweise höchstens ein Mitglied. Überprüfen Sie diese Gruppe und bereinigen Sie alte / nicht verwendete Benutzerkonten.
- **Es wurde eine hohe Anzahl von Schema-Administratoren gefunden.** Mitglieder dieser Gruppe können das Active Directory-Schema ändern. Diese Gruppe enthält idealerweise höchstens ein Mitglied. Überprüfen Sie diese Gruppe und bereinigen Sie alte / nicht verwendete Benutzerkonten.
- **Trotz persönlicher Administratorkonten werden zum Teil weiterhin Sammelaccounts genutzt.** Es wird empfohlen, ausschließlich persönliche Admin- oder dedizierte Dienst-Konten zu verwenden.
- **Bei einigen Administratorkonten läuft das Passwort nie ab.** Aktivieren Sie auch bei Administratoren die regelmäßige Änderung des Passworts. Alternativ können Sie MFA einrichten und / oder die Anmeldungen der privilegierten Konten proaktiv monitoren.

Ausgabe CSAT – Rollen im Azure Active Directory

Es werden nur Rollen angezeigt, die auch Mitglieder enthalten.

Ausgabe CSAT – Status MFA für privilegierte Konten im Azure Active Directory

Schlussfolgerungen und Empfehlungen

- Es wurde **eine große Anzahl von Globalen Administratoren** gefunden. Idealerweise haben weniger als 5 Benutzer diese Rolle. Überprüfen Sie diese Accounts und bereinigen Sie alte / nicht verwendete Benutzerkonten.

- Multi-Faktor-Authentifizierung war zum Zeitpunkt des Scans nicht für alle Administratoren aktiviert. Das wurde mittlerweile verbessert.

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 und für alle privilegierten Konten **Multi Faktor Authentifizierung (MFA)** zu aktivieren. Ebenfalls empfohlen wird ein Prozess, in dem die Berechtigungen für privilegierte Konten regelmäßig überprüft werden.

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. Mit **Azure MFA** können Sie Multi-Faktor-Authentifizierung für alle (privilegierten) Accounts erzwingen.

Darüber hinaus ist es eine empfohlene Sicherheitspraxis, nicht nur normale Benutzerkonten von privilegierten Benutzerkonten zu trennen (d. h. normale von privilegierten Aufgaben zu trennen), sondern zusätzlich separate Privileged Access Workstations zu verwenden, die den einzelnen privilegierten Benutzern zugeordnet sind. So wird z.B. das Risiko von Pass the Hash-Angriffen oder anderen Angriffen auf Anmeldeinformationen verringert. Wir empfehlen dringend, solche Arbeitsplätze in der Cloud zu implementieren. Durch den Einsatz von **Windows Virtual Desktops** können Sie solche sicheren Workstations - vollständig verwaltet und überwacht - bereitstellen. Die Benutzer müssen so keine separaten Geräte mit sich herumtragen mit all den Risiken, die damit verbunden sind.

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

Ausgabe CSAT – AD-Domänen- und Gesamtstrukturfunktionsebenen

DOMÄNEN-LEVEL - AT

Name der Domäne	at
Domänen-Level	WINDOWS SERVER 2008 R2
Forest-Level	WINDOWS SERVER 2008 R2

DOMÄNEN-LEVEL - DE

Name der Domäne	de
Domänen-Level	WINDOWS SERVER 2008 R2
Forest-Level	WINDOWS SERVER 2008 R2

DOMÄNEN-LEVEL - FR

Name der Domäne	fr
Domänen-Level	WINDOWS SERVER 2008 R2
Forest-Level	WINDOWS SERVER 2008 R2

DOMÄNEN-LEVEL - UK

Name der Domäne	uk
Domänen-Level	WINDOWS SERVER 2008 R2
Forest-Level	WINDOWS SERVER 2008 R2

Schlussfolgerungen 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.

Ausgabe CSAT – Sichere Konfiguration von Endpunkten

SICHERE KONFIGURATION

Powershell x32 Bypass	1
Powershell x32 uneingeschränkt	58
Powershell x64 Bypass	1
Eingehendes RDP ohne NLA aktiviert	125
Endpunkte mit RDP-Sicherheitsstufe niedriger als 2	243
Endpunkte mit LM-Kompatibilität niedriger als 5	756
SMBv1 Client aktiviert	98
SMBv1 Server aktiviert	414
SMB V2 aktiviert	689
SMB V3 aktiviert	593

Schlussfolgerungen und Empfehlungen

Systeme werden aktuell nicht durchgängig gehärtet, weshalb alte, unsichere Sicherheitsprotokolle weiterhin zulässig sind. Implementieren Sie **CIS-gehärtete Images** aus dem **Azure VM-Store** um neue VMs sicher und schnell zu implementieren. CIS verfügt über verschiedene freie Benchmarks auf https://www.cisecurity.org/cis-benchmarks/.

Darüber hinaus stellt Microsoft für verschiedene Server, Clients und Middleware kostenlose Group Policies für die Sicherheitskonfiguration bereit, die auf aktuellen Empfehlungen basieren, um so die Sicherheit Ihrer Assets zu erhöhen. Beachten Sie bei der Umsetzung die Überprüfung auf Aktualisierungen - speziell alle 6 Monate nach der halbjährlichen Veröffentlichung ihrer Produkte. Wenn Sie andere Betriebssysteme verwenden, suchen Sie nach ähnlichen Baselines und erstellen Sie einen Prozess um diese herum.

- **512** 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 Microsoft Endpoint Manager deaktiviert werden.
- Es wurden **125** Endpunkte gefunden, die **RDP ohne NLA** aktiviert haben, stellen Sie sicher, dass verwaltete RDP-Endpunkte NLA auf Remote-Maschinen NLA aktiviert haben. Deaktivieren Sie RDP auf Maschinen, auf denen es nicht benötigt wird.
- **243** Endpunkte mit niedriger **RDP-Sicherheitsstufe** (nicht gesetzt / Level 0 oder 1) gefunden. Erhöhen Sie die Sicherheitsstufe auf 2, um Transport Layer Security (TLS) für die Vorauthentifizierung zu verwenden.

Ausgabe CSAT – Registry Machine

Registry Key	Wert(e)	Daten	Bewertung ↑
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters	RestrictNullSessAccess	0	Schlecht
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa	EveryoneIncludesAnonymous	1	Schlecht
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa	lmcompatibilitylevel		Schlecht
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManWorkstation\Parameters	RequireSecuritySignature	0	Schlecht
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell	ExecutionPolicy	Bypass	Schlecht
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell	ExecutionPolicy	Unrestricted	Schlecht
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell	ExecutionPolicy	Bypass	Schlecht
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	AutoAdminLogon	1	Suspekt
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters	RequireSecuritySignature	0	Suspekt
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa	LimitBlankPasswordUse	0	Suspekt
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp	SecurityLayer	1	Suspekt

Ausgabe CSAT – Registry Users

Registry Key	Wert(e)	Daten	Bewertung ↑
HKEY_CURRENT_USER\Control Panel\Desktop	ScreenSaverActive		Suspekt
HKEY_CURRENT_USER\Control Panel\Desktop	ScreenSaverIsSecure		Suspekt

Schlussfolgerungen und Empfehlungen

CSAT überprüft 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 das 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

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

Ausgabe CSAT – Ungültige Anmeldeversuche im Active Directory

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

S-1-5-21-808331520-826681909-1660491571-7163	3
S-1-5-21-808331520-826681909-1660491571-6437	2
S-1-5-21-808331520-826681909-1660491571-1278	1
S-1-5-21-808331520-826681909-1660491571-7124	1
S-1-5-21-808331520-826681909-1660491571-8875	0

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

S-1-5-21-2131559260-169161015-1982612992-23140	100
S-1-5-21-2131559260-169161015-1982612992-19814	31
S-1-5-21-2131559260-169161015-1982612992-9969	8
S-1-5-21-2131559260-169161015-1982612992-7473	7
S-1-5-21-2131559260-169161015-1982612992-29054	6

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

S-1-5-21-3061677275-3141726960-3819589214-1642	5
S-1-5-21-3061677275-3141726960-3819589214-3635	5
S-1-5-21-3061677275-3141726960-3819589214-1198	2
S-1-5-21-3061677275-3141726960-3819589214-1204	1
S-1-5-21-3061677275-3141726960-3819589214-3774	1

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

S-1-5-21-3328545213-268796786-2658145146-2120	11
S-1-5-21-3328545213-268796786-2658145146-1102	2
S-1-5-21-3328545213-268796786-2658145146-1340	1
S-1-5-21-3328545213-268796786-2658145146-1509	1
S-1-5-21-3328545213-268796786-2658145146-1675	1

*Benutzernamen wurden in die Benutzer-SID geändert; alle Details finden Sie in CSAT.

Schlussfolgerungen und Empfehlungen

- Es wurde Accounts mit einer großen Anzahl von fehlerhaften Anmeldeversuchen ermittelt. Dies ist ein Zeichen dafür, dass Konten angegriffen werden. Wir empfehlen, die Konten zu

überprüfen, das Passwort zurückzusetzen, MFA zu aktivieren und den Benutzer darüber zu informieren, wie es weitergeht.

Um das Risiko zu verringern, durch gestohlene Identitäten kompromittiert zu werden, sollten verdächtige Anmeldungen überwacht werden. Es wird empfohlen, **Azure Active Directory Defender for Identity** zu implementieren, um frühzeitig Warnungen vor Angriffen auf lokale Domänencontroller zu erhalten. Diese Sicherheitslösungen ermöglichen die Überwachung gegen verschiedene (AD) Angriffe und Anomalien. Kombinieren Sie dies mit **Azure Active Directory Identity Protection** für Benutzerkonten in der Cloud. Legen Sie außerdem Benachrichtungen für die Personen fest, die über verdächtige Aktivitäten Bescheid wissen müssen.

Wenn Benutzer aufgrund von Passwort-Attacken oder vergessenem Passwort ausgesperrt werden, kann das Zurücksetzen des Passworts im Self-Service helfen, dass sie schnell wieder handlungsfähig sind. Aktivieren Sie den SSPR-Prozess in Azure Active Directory in Kombination mit MFA. Legen Sie mindestens zwei Mittel zur Authentifizierung des Benutzers fest, bevor er berechtigt wird, sein Kennwort zurückzusetzen. Das Tool wird von den Benutzern sehr geschätzt und senkt die Anzahl der Helpdesk-Anrufe erheblich.

Die Überwachung auf Azure SQL-Servern sollte aktiviert sein. Aktivieren Sie die Überwachung auf Ihrem SQL Server, um Datenbankaktivitäten in allen Datenbanken auf dem Server nachzuverfolgen und in einem Überwachungsprotokoll zu speichern.

Azure Defender für SQL sollte auf Ihren SQL-Servern aktiviert sein. Azure Defender für SQL ist ein einheitliches Paket, das erweiterte SQL-Sicherheitsfunktionen bietet. Es erkennt und mindert mögliche Datenbankschwachstellen und erkennt anomale Aktivitäten, die auf eine Bedrohung für Ihre Datenbank hinweisen könnten. Azure Defender für SQL erfordert einige zusätzliche Lizenzen.

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 Raktion auf Bedrohungen.

Stellen Sie sicher, dass die Microsoft 365-Überwachungsprotokollsuche aktiviert ist. Aktivieren Sie die Mailbox-Überwachung für alle Benutzer. Konfigurieren Sie in Azure mindestens ein Protokollprofil, um Protokolle vom Tenant zu empfangen. Legen Sie die Aufbewahrungsdauer auf mindestens 365 Tage fest, und stellen Sie sicher, dass das Überwachungsprofil alle Aktivitäten erfasst. Konfigurieren Sie Aktivitätsprotokollwarnungen für vertrauliche Aktivitäten.

Alle Organisationen können die kostenlose Version von Azure Security Center verwenden. Während es grundlegende Funktionen bereitstellt, gibt es Ihnen Einblick in die Sicherheitsposition Ihrer Azure-Umgebung. Außerdem werden Azure-Sicherheitsempfehlungen aktiviert, die Ihnen helfen, Ihre Sicherheitslage zu verbessern. Es wird dringend empfohlen, ein Upgrade von Azure Security Center auf ein kostenpflichtiges Abonnement durchzuführen, um weitere Features zu aktivieren und den Zeitraum, für den die Protokolldateien gespeichert werden, zu verlängern.

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

Ausgabe CSAT - Spoofing-Schutz für E-Mail

Schlussfolgerungen und Empfehlungen

- **Der SPF-Datensatz ist mit einem Soft Fail konfiguriert**. Bei einem Soft Fail dürfen die Absender, die nicht im SPF-Datensatz enthalten sind, weiterhin E-Mails aus der E-Mail-Domäne senden. Wenn die SPF-Datensätze auf einen Hard Fail geändert werden, werden die E-Mails, die von nicht zulässigen Absendern gesendet werden, gelöscht. Prüfen Sie, ob alle autorisierten E-Mail-Server/Domänen in den SPF-Records enthalten sind. Ändern Sie anschließend den Parameter ~all des SPF-Records in -all, um die Einstellung für einen Hard Fail zu aktivieren.
- **DMARC-Datensätze sind ohne Richtlinie konfiguriert**. Die DMARC-Richtlinie bestimmt, was mit Nachrichten passiert, wenn die SPF- und/oder DKIM-Prüfung fehlschlägt. Es wird empfohlen, die Richtlinie auf 'Zurückweisen' ('Reject') zu setzen. Mit der Policy 'Reject' werden nicht autorisierte Mails gelöscht. Das ist wesentlich für den Kampf gegen Spoofing. Wenn die Richtlinie auf p=none festgelegt ist, wird DMARC zwar überprüft, der empfangende Server wird die Nachricht aber trotzdem an die Mailbox übergeben, wodurch die SPF- und DKIM-Funktionen unbrauchbar werden.

Wir empfehlen, die Datensätze für **SPF** und **DMARC** anzupassen, um eine unautorisierte Nutzung Ihrer E-Mail-Domäne(en) zu verhindern und den Schutz vor Spam, Betrug und Phishing zu verbessern. Es wird nicht nur Ihre eigenen Mitarbeiter schützen, sondern auch die Empfänger außerhalb Ihres Unternehmens.

> **Hinweis**: Beachten Sie, dass Spoofer, die denselben Domänennamen zum Senden gefälschter Nachrichten verwenden (wie die häufig verwendeten Clouddienstanbieter), zu einem "Pass" führen, wenn Ihr SPF-Eintrag überprüft wird, wie es in Ihrem SPF-Eintrag erwähnt wird. Kombinieren Sie daher den SPF-Datensatz mit DKIM-Signaturen und DMARC-Richtlinien, um Ihren Schutz vor Spooferen zu verbessern.

Optional, aber empfohlen: Überprüfen Sie die korrekte Implementierung von SPF, DKIM und DMARC, indem Sie ein kostenloses Tool verwenden, das von Microsoft MISA-Partner Valimail.com bereitgestellt wird. Informationen: https://www.microsoft.com/security/blog/2019/06/03/secure-cloud-free-dmarc-monitoring-office-365/.

Es wird empfohlen, Office 365 Advanced Threat Protection (Microsoft Defender for Office 365) zu implementieren. Diese Lösung - mit den richtigen Richtlinien - schützt Ihre Organisation vor Bedrohungen die von E-Mails, Web-Links (URLs) und Collaboration-Tools asugehen können.

6.1.8. CIS Control 8: Schutz vor Malware

Ausgabe CSAT – Übersicht Antivirus

Serverendpunkte ohne Windows Defender	217
Clientendpunkte ohne Antivirus	14
Endpunkte mit veralteter Viren-Definition	6

Ausgabe CSAT - Abgelaufener Virenschutz

Endpunktname	Name Virenschutz	Definition
NB0432	Windows Defender	OUT_OF_DATE
NB35-135	Windows Defender	OUT_OF_DATE
NB45-032	Windows Defender	OUT_OF_DATE
NB61-013	Windows Defender	OUT_OF_DATE
NB86-020	Windows Defender	OUT_OF_DATE

Schlussfolgerungen und Empfehlungen

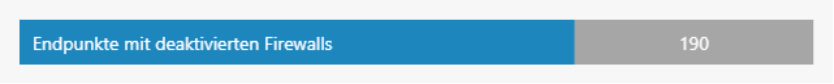
- Es wurden **14** Endpunkte ohne oder mit deaktiviertem Virenschutz gefunden. Mildern Sie dieses Risiko, indem Sie eine Antivirensoftware auf diesen Maschinen aktivieren.
- Es wurden **6** Endpunkte mit veralteten Virendefinitionen gefunden. Diese Endpunkte sind anfällig für Angriffe. Ein veraltetes Antivirenprogramm ist nicht in der Lage, die neuesten Bedrohungen zu erkennen und darauf zu reagieren. Wir empfehlen, so schnell wie möglich zu aktualisieren und einen automatisierten Aktualisierungsmechanismus zu implementieren.

CSAT ist nicht in der Lage, Informationen zum Antivirenstatus auf Servern zu erfassen, die nicht Windows Defender verwenden. Es wird empfohlen, den Status des Virenschutzes regelmäßig mit Hilfe einer zentralen Verwaltungslösung zu überprüfen und sicherzustellen, dass auf allen Computern ein aktiviertes und aktuelles Antivirenprogramm ausgeführt wird.

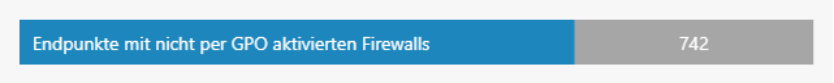
Eine Antivirensoftware ist ein grundlegendes Mittel, Angriffe und Viren abzuwehren. Es wird empfohlen, **Defender for Endpoints** zu implementieren und auf allen Endpunkten zu erzwingen. Es handelt sich um eine vollständige EDR-Lösung (Endpoint Detection and Response), die proaktiven Endpunktschutz, Erkennung von Sicherheitsverletzungen, automatisierte Untersuchung und Incident Response bietet. Dieses Tool gibt Ihnen auch Einblicke in Sicherheitslücken und Fehlkonfigurationen auf Endpunkten.

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

Ausgabe CSAT – Status lokale Firewalls



Ausgabe CSAT – Status lokale Firewalls über GPO



Schlussfolgerungen und Empfehlungen

- Es wurden **190** Endpunkte mit einer oder mehreren deaktivierten Windows Firewall-Profilen gefunden. Es wird empfohlen, die Firewalls auf allen 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, **Defender for Endpoints** 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.

Wenn Azure-Ressourcen verwendet werden, wird empfohlen, die Best Practice Vorschläge von Microsoft zu befolgen, um sicherzustellen, dass Verbindungen von und zu den Azure-Ressourcen gesichert werden. Mit einer korrekt eingerichteten Netzwerksicherheitsgruppe können Sie den Datenverkehr von und zu den Ressourcen in Azure filtern.

6.1.10. CIS Control 10: Fähigkeit zur Wiederherstellung von Daten

CSAT bewertet die Bestandsaufnahme der Funktionen zur Datenwiederherstellung nicht. Dieses Control wird in Kapitel 5, Foundational CIS Controls, abgedeckt.

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

CSAT bewertet die sichere Konfiguration von Netzwerkgeräten nicht. Dieses Control wird in Kapitel 5, Foundational CIS Controls, abgedeckt.

6.1.12. CIS Control 12: Verteidigung von Netzwerk-Grenzen

CSAT bewertet die Verteidigung der Netzwerkgrenzen nicht. Dieses Control wird in Kapitel 5, Foundational CIS Controls, abgedeckt.

6.1.13. CIS Control 13: Schutz von Daten

Ausgabe CSAT – Status Verschlüsselung mit BitLocker

ENDPUNKTE

Client-Endpunkte ohne BitLocker-Verschlüsselung	53
Server-Endpunkte ohne BitLocker-Verschlüsselung	436

Schlussfolgerungen und Empfehlungen.

- Für **53** Client-Endpunkte ist die BitLocker-Verschlüsselung nicht aktiviert.
- Für **436** Server-Endpunkte ist die BitLocker-Verschlüsselung nicht aktiviert.

Ein unverschlüsselter Speicher in den falschen Händen stellt ein hohes Risiko für Datenverlust dar. Das gilt speziell für mobile Geräte wie Laptops, Tablets und Smartphones. Desktop-Computer, die sich an (halb-)öffentlichen Stellen befinden, könnten jedoch in die gleiche Risikokategorie fallen, ebenso wie Serverspeicher, wenn dieser ersetzt wird.

Die Implementierung von Plattenverschlüsselung wie Windows BitLocker oder Android/IOS-Geräteverschlüsselung ist eine kosteneffiziente Methode, um Datenverlust bei gestohlenen oder verlorenen Geräten zu verhindern, indem ein unbefugter Zugriff auf den Speicher verhindert wird.

Viele Vorschriften wie PCI-DSS, HiPAA und die DSGVO erfordern die Verwendung von Datenverschlüsselung. Wir empfehlen, die Geräteverschlüsselung für alle Endpunkte über ein zentrales Managementtool wie Endpoint Manager oder andere Mobile Device Management-Lösungen zu aktivieren, wo Sie diese Geräte auch mit anderen Sicherheitsrichtlinien verwalten und sogar Geschäftsdaten von den Geräten löschen können.

Ausgabe CSAT – Potenziell personenbezogene Daten

<keine auffälligen Daten>

Schlussfolgerungen und Empfehlungen.

Geleakte Unternehmensinformationen sind und werden eine Quelle für Reputationsverlust für Unternehmen sein. Dies ist jedoch relativ einfach zu verhindern. Darüber hinaus verlangen viele Regelungen wie die bereits erwähnten, dass Sie personenbezogene Daten im Rahmen Ihrer organisatorischen und technischen Möglichkeiten schützen. Es hilft auch der Kontinuität des Unternehmens, sein geistiges Eigentum, Finanzdaten, Strategien und Ähnliches zu schützen.

Mindern Sie das Risiko von Datenverlust, Markenschäden, schlechter Presse, Bußgeldern und andere negativen Folgen. Etablieren Sie Prozesse und Features, um alle Dokumente und Datenquellen, die sensible Daten enthalten, (automatisch) zu klassifizieren, zu kennzeichnen und zu schützen, indem Sie **Microsoft Information Protection (MIP)** implementieren. Diese Lösung klassifiziert, kennzeichnet und schützt Dokumente und E-Mails innerhalb einer Organisation. Es schützt vor unangemessenen Freigaben und Datenlecks und verhindert, dass nicht autorisierte Benutzer auf freigegebene Daten zugreifen. Darüber hinaus bietet MIP Ihnen die Möglichkeit, den Zugang zu den Dokumenten zu widerrufen und zu verfolgen, an wen sie weitergegeben wurden und wer Zugriff auf die Informationen hatte. Mit diesen Funktionen kann AIP helfen, regulatorische Anforderungen wie die DSGVO / GDPR, PCI DSS und andere Finanz-, Industrie- oder behördliche Reglementierungen zu erfüllen.

Eine andere Option, um Datenverlust / Datenlecks zu verhindern, ist die Implementierung einer Cloud Application Security-Lösung, die in Azure verfügbar ist. CAS ist in der Lage, die Verwendung von Schatten-IT-Anwendungen zu überwachen. Mit geeigneten Richtlinien kann es entweder verhindern, dass sensible Daten an nicht genehmigte Anwendungen weitergegeben werden, oder es kann AIP aufrufen, um die Daten automatisch zu kennzeichnen und zu verschlüsseln, bevor sie an eine solche Shadow-IT-Anwendung weitergegeben werden.

Durch die Implementierung des sogenannten Conditional Access kann der Zugriff auf sensible Informationen für Benutzer mit Geräten, die verwaltet oder nicht verwaltet sein können, eingeschränkt oder gewährt werden, während eine Risikoanalyse für eine Reihe von Parametern durchgeführt wird, um zu prüfen, ob der Benutzer Zugriff auf die betreffenden Daten, Anwendungen oder Ressourcen erhalten soll.

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

Im Allgemeinen wird empfohlen, eine Architektur zu implementieren, die eine Verschlüsselung bei der Übertragung (auch lokal), der Ablage und - in sehr sensiblen Umgebungen - auch im Speicher erfordert. Letzteres kann z.B. durch **Azure Confidential Computing** erreicht werden.

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

Ausgabe CSAT - Berechtigungen auf SharePoint-Sites

Schlussfolgerungen und Empfehlungen

- Das Teilen mit externen Usern ist auf bestehende externe User eingeschränkt. Das ist gut, da so eine gewisse Kontrolle besteht, wohin Daten fließen können.

Dateifreigaben, SharePoint- und Teams-Sites enthalten höchstwahrscheinlich vertrauliche Daten. Es ist zwingend erforderlich, dass nur die richtigen Benutzer Zugriff auf diese Informationen haben. Unter Berücksichtigung der vorgenannten Vorschriften empfehlen wir Geschäftsprozeduren zum Erstellen vierteljährlicher Berichte an den Datenbesitzer, um zu überprüfen, ob die aktuellen Benutzerberechtigungen so noch erforderlich sind.

Ausgabe CSAT – Extern geteilte Daten aus SharePoint

Schlussfolgerungen und Empfehlungen

Zusätzliche Risiken entstehen durch Daten, die mit externen Benutzern wie Geschäftspartnern, Kunden/Konsumenten, über SharePoint, OneDrive und Teams gemeinsam genutzt werden. Externe Nutzer werden meist nicht zentral verwaltet. Während interne Benutzerkonten wahrscheinlich deaktiviert werden, wenn jemand das Unternehmen verlässt oder wenn er aus der Zugriffsgruppe entfernt wird, wenn er in eine andere Rolle wechselt, werden externe Benutzer nicht auf dieselbe Weise verwaltet. Das Anwendungsmanagement sollte Berichte erstellen für die fachlichen Besitzer von Daten, damit diese entscheiden können, ob die externen Benutzer noch Zugriff auf die Daten benötigen. Wenn externe Benutzer entfernt werden können, sollten sie das Anwendungsmanagement informieren. Diesen Prozess im Laufe der Zeit synchron zu halten, ist eine organisatorische Herausforderung.

<u>Rollen in MS Teams</u>

Die Zusammenarbeit in MS Teams basiert auf einem flachen Berechtigungsmodell. Alle Mitglieder, interne und externe Mitglieder, haben dieselben Berechtigungen, um Zugriff auf Daten in einem Team zu erhalten. Berechtigungsrollen sind nur für die Rollen Besitzer und Mitglied vorhanden, wobei der Besitzer nur mehr Berechtigung zum Verwalten des Teams hat.

Eine Funktion, die einem Teammitglied, egal ob intern oder extern, nur lesenden Zugriff geben würde, ist nicht verfügbar.

<u>Gemeinsame Nutzung von Dokumenten und Zugriffsrechten</u>

Die gemeinsame Nutzung eines Dokuments ist eine leistungsfähige Funktion zur Zusammenarbeit mit mehreren Benutzern sowohl innerhalb als auch außerhalb der Organisation. Dies aus Sicht exzellenter Usability und Informationsmanagement, um nur ein einziges Dokument im gesamten Kollaborationsprozess zu halten.

Wenn ein Dokument gemeinsam genutzt wird, werden die ursprünglichen Berechtigungen geändert. Die eingeladenen internen und externen Benutzer werden dem Dokument hinzugefügt. Dies macht es nicht mehr konform zu den Berechtigungen, die auf die Website oder das Team gesetzt sind, wo es gespeichert ist. Die einzige Möglichkeit, die Berechtigungen wieder auf Original zurückzuspeichern, besteht darin, den Endbenutzer die gemeinsame Nutzung des Dokuments in der richtigen Weise deaktivieren zu lassen. Die Vorgang hierfür ist zu kompliziert, als dass ein normaler

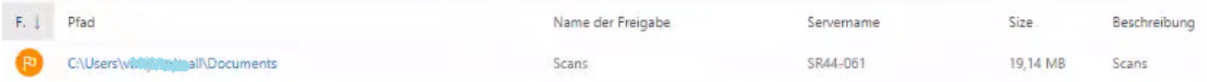
Endanwender das umsetzen könnte. Das führt zu einer Umgebung für die Onlinezusammenarbeit, die nicht mehr compliant ist.

Automatisieren Sie Governance und garantieren Sie eine konforme Kollaborationsumgebung.

Um die Umgebung für die Zusammenarbeit zu steuern und sie in einen konformen Status zu bekommen und zu erhalten, kann Automatisierung helfen. Geben Sie kontrollierten Zugriff auf Sites und Teams, indem Sie den Eigner nur definierte funktionale Rollen verwenden lassen. Der Eigentümer ist nicht der Eigentümer der Website oder des Teams und kann die Berechtigungen nicht selbst ändern. Es können nur die voreingestellten Rollen verwendet werden.

Eine periodische Aktivität erinnert den Inhaber des Teams / der Site daran, die Zugangsberechtigung sowohl für interne als auch für externe Benutzer zu überprüfen. Um die Erstellung von Sites oder Teams mit den richtigen Rollen und Zugriffsrechten zu vereinfachen, empfehlen wir, ein Tool wie PortalTalk zu implementieren. Das ist ein cloudbasiertes Produkt, das Ihnen hilft, Kontrolle und Governance der Zugriffsrechte in SharePoint, MS Teams und Microsoft 365 Gruppen zu erlangen und zu bewahren.

Ausgabe CSAT – Freigaben auf Endpunkten



Server-Name	Pfad	Name des Shares	Größe	Beschreibung
AB12EASY-HSM	C:\Archiv	Archiv	31,68 TB	
AB12EASY-HSM	C:\Archiv	Easy$	31,68 TB	Standortfreigabe
NT-SRV1	F:\Benutzer-Daten	Daten	11,79 TB	
IJ12FILE2A	D:\File\Group	File	2,6 TB	Group Share
KH12FILE1A	D:\File\User	File	2,35 TB	Users Share
JH12FSL2	D:\FSLogixODFC	FSLogixODFC$	2,13 TB	
DF12FSL1	D:\FSLogixODFC	FSLogixODFC$	2,13 TB	
HUINSTALL	D:\Install	Install	2,03 TB	
UH12FileArc1	E:\PST-Dateien	PST	1,8 TB	
Wienfile01	G:\Benutzer-Daten	Daten	1,51 TB	

Schlussfolgerungen 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.

6.1.15. CIS Control 15: WLAN Zugangskontrolle

CSAT bewertet die Zugriffsskontrolle im WLAN nicht. Dieses Control wird in Kapitel 5, Foundational CIS Controls, abgedeckt.

6.1.16. CIS Control 16: Monitoring und Kontrolle von Benutzerkonten

Ausgabe CSAT – Übersicht Konten im Active Directory

AD ACCOUNTS - AT

Aktivierte Accounts	584
Deaktivierte Accounts	185
Aktive Accounts ohne Anmeldung für mehr als 30 Tage	97
Aktive Accounts ohne Anmeldung für mehr als 90 Tage	81
Aktive Accounts ganz ohne Anmeldung	42
Als 'kritisch' geflaggte Accounts	0

AD ACCOUNTS - DE

Aktivierte Accounts	3316
Deaktivierte Accounts	565
Aktive Accounts ohne Anmeldung für mehr als 30 Tage	681
Aktive Accounts ohne Anmeldung für mehr als 90 Tage	582
Aktive Accounts ganz ohne Anmeldung	395
Als 'kritisch' geflaggte Accounts	4

AD ACCOUNTS - FR

Aktivierte Accounts	300
Deaktivierte Accounts	5
Aktive Accounts ohne Anmeldung für mehr als 30 Tage	68
Aktive Accounts ohne Anmeldung für mehr als 90 Tage	59
Aktive Accounts ganz ohne Anmeldung	15
Als 'kritisch' geflaggte Accounts	0

AD ACCOUNTS - UK

Aktivierte Accounts	151
Deaktivierte Accounts	17
Aktive Accounts ohne Anmeldung für mehr als 30 Tage	32
Aktive Accounts ohne Anmeldung für mehr als 90 Tage	27
Aktive Accounts ganz ohne Anmeldung	19
Als 'kritisch' geflaggte Accounts	0

Ausgabe CSAT – User Account Control Flags im Active Directory (nur aktive Accounts)

UAC DETAILS AKTIVE AD ACCOUNTS - AT

Kein Kennwort erforderlich	3
Kann Passwort nicht ändern	0
PreAuth nicht erforderlich	0
Umkehrbares Textpasswort	0
Kennwort läuft nie ab	530
Smartcard erforderlich	0
Nur DES Schlüssel verwenden	0
Trusted To Auth For Delegation (Konto wird für Delegierungszwecke aktiviert)	0
Partial Secrets Account (Konto ist ein schreibgeschützter Domänencontroller - RODC)	0

UAC DETAILS AKTIVE AD ACCOUNTS - DE

Kein Kennwort erforderlich	4
Kann Passwort nicht ändern	0
PreAuth nicht erforderlich	0
Umkehrbares Textpasswort	0
Kennwort läuft nie ab	2303
Smartcard erforderlich	0
Nur DES Schlüssel verwenden	0
Trusted To Auth For Delegation (Konto wird für Delegierungszwecke aktiviert)	0
Partial Secrets Account (Konto ist ein schreibgeschützter Domänencontroller - RODC)	0

UAC DETAILS AKTIVE AD ACCOUNTS - FR

Kein Kennwort erforderlich	3
Kann Passwort nicht ändern	0
PreAuth nicht erforderlich	0
Umkehrbares Textpasswort	0
Kennwort läuft nie ab	148
Smartcard erforderlich	0
Nur DES Schlüssel verwenden	0
Trusted To Auth For Delegation (Konto wird für Delegierungszwecke aktiviert)	0
Partial Secrets Account (Konto ist ein schreibgeschützter Domänencontroller - RODC)	0

UAC DETAILS AKTIVE AD ACCOUNTS - UK

Kein Kennwort erforderlich	2
Kann Passwort nicht ändern	0
PreAuth nicht erforderlich	0
Umkehrbares Textpasswort	0
Kennwort läuft nie ab	138
Smartcard erforderlich	0
Nur DES Schlüssel verwenden	0
Trusted To Auth For Delegation (Konto wird für Delegierungszwecke aktiviert)	0
Partial Secrets Account (Konto ist ein schreibgeschützter Domänencontroller - RODC)	0

Schlussfolgerungen und Empfehlungen

- **753** Konten haben **sich 90 Tage lang nicht angemeldet** und **478** Konten haben **sich noch nie angemeldet**. Überprüfen Sie diese Accounts und bereinigen Sie die, die nicht verwendet werden.
- **789** Konten sind **deaktiviert**. Bereinigen Sie diese Konten.
- Für **[X]** 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. Um diese Einstellung zu ändern, sollte ein IT-Administrator PowerShell verwenden.
- **3334** 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 – Passwort-Policy des Active Directory

PASSWORT-RICHTLINIE - AT

Dauer der Sperre in Minuten	15372286728
Komplexes Passwort erforderlich	false
Maximale Gültigkeit von Passwörtern	10675199
Minimale Gültigkeit von Passwörtern	0
Minimale Passwort-Länge	5
Passwort-Historie	0
Schwellwert Sperre	0

PASSWORT-RICHTLINIE - DE

Dauer der Sperre in Minuten	60
Komplexes Passwort erforderlich	false
Maximale Gültigkeit von Passwörtern	10675199
Minimale Gültigkeit von Passwörtern	0
Minimale Passwort-Länge	6
Passwort-Historie	0
Schwellwert Sperre	100

PASSWORT-RICHTLINIE - FR

Dauer der Sperre in Minuten	30
Komplexes Passwort erforderlich	false
Maximale Gültigkeit von Passwörtern	10675199
Minimale Gültigkeit von Passwörtern	0
Minimale Passwort-Länge	6
Passwort-Historie	0
Schwellwert Sperre	10

PASSWORT-RICHTLINIE - UK

Dauer der Sperre in Minuten	30
Komplexes Passwort erforderlich	true
Maximale Gültigkeit von Passwörtern	42
Minimale Gültigkeit von Passwörtern	1
Minimale Passwort-Länge	7
Passwort-Historie	24
Schwellwert Sperre	0

Schlussfolgerungen und Empfehlungen

Es wird empfohlen, die Kennwortrichtlinie einheitlich(!) gemäß anerkannten Vorgaben zu konfigurieren, z. B.:

- Dauer der Kontosperre: **30** Minuten
- Kennwort muss Komplexitätsvoraussetzungen entsprechen: **Aktiviert** (**true**)
- Maximale Gültigkeit von Passwörtern: **90** Tage
- Minimale Gültigkeit von Passwörtern: **1** Tag
- Minimale Passwort-Länge: **12** Zeichen
- Passwort-Historie: **24** Passwörter
- Schwellwert Kontosperre: **5** ungültige Anmeldeversuche
-

Ausgabe CSAT – Übersicht Konten im Azure Active Directory

Tenant	Externe Benutzer	Aktivierte Benutzer	Deaktivierte Benutzer	Aktivierte Benutzer ohne MFA	O365 Durchsuchen des Überwachungsprotokolls
contoso.onmicrosoft.com	59	2903	59	2931	Yes

Schlussfolgerungen und Empfehlungen

Ein starkes, komplexes Kennwort ist die erste Verteidigungslinie beim Schutz Ihrer Konten. MFA ist eine Funktion, die den Benutzernamen und das Kennwort sowie eine weitere Überprüfungsmethode erfordert, um sich bei einem Konto anzumelden. Dies kann z. B. ein zufällig generierter SMS-Code, ein Telefonanruf, eine Smartcard (virtuell oder physisch) oder ein biometrisches Gerät sein.Falls Konten (mit aktiviertem MFA) vorhanden sind, bei denen Benutzernamen und Kennwörter kompromittiert wurden, z. B. durch Phishing-E-Mails oder Brute-Force-Angriffe, können die Angreifer keinen Zugriff auf die Konten erhalten, da sie nicht in der Lage sind, die zweite Form der Authentifizierung abzuschließen. Es wird empfohlen, MFA zusammen mit Conditional Access zu implementieren, um Ihre Benutzer zu schützen, da dies höchst effektiv ist, um Angriffe zu stoppen. Erzwingen Sie dies mit **Azure MFA** und **Azure Active Directory Conditional Access**. Durch eine Richtlinie für den bedingten Zugriff (Conditional Access) können Sie den Zugriff auf Ressourcen für Geräte blockieren, die die in Ihrer Konformitätsrichtlinie festgelegte Bedrohungsstufe überschreiten.

Ausgabe CSAT – Externe Benutzer im Azure Active Directory

Schlussfolgerungen und Empfehlungen

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

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

Inventarisierung	Anzahl
Lokales Administratorkonto auf gescannten Endpunkten aktiviert	**394**
Gastkonten auf gescannten Endpunkten aktiviert	**2**

Schlussfolgerungen und Empfehlungen

- LAPS ist bereits für Clients im Einsatz und soll demnächst auch für die Server verwendet werden.
- Auf den gescannten Endpunkten wurden aktive Gastkonten gefunden. Diese Konten erfordern keine Authentifizierung und auch kein Kennwort für die Anmeldung. Zur Erhöhung der Sicherheit empfehlen wir die Deaktivierung aller Gastkonten.

6.1.17. CIS Control 17: Security Awareness- und Trainingsprogramm

CSAT bewertet dieses Thema nicht. Dieses Control wird in Kapitel 5, Foundational CIS Controls, abgedeckt.

6.1.18. CIS Control 18: Sicherheit der Anwendungssoftware

CSAT bewertet dieses Thema nicht. Dieses Control wird in Kapitel 5, Foundational CIS Controls, abgedeckt.

6.1.19. CIS Control 19: Incident Response und Management

CSAT bewertet dieses Thema nicht. Dieses Control wird in Kapitel 5, Foundational CIS Controls, abgedeckt.

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

CSAT bewertet dieses Thema nicht. Dieses Control wird in Kapitel 5, Foundational CIS Controls, abgedeckt.

6.2. Microsoft und Azure 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. Die zugrunde liegende Baseline wird fortlaufend weiterentwickelt und den Entwicklungen angepasst. Daher eignen sich diese Scores nicht für eine Messung des Fortschritts.

Unter diesem Link finden Sie weitere Infos zum Microsoft Secure Score. Oder überprüfen Sie den Score direkt unter https://security.microsoft.com/securescore/

Microsoft Secure Score

Die folgenden Empfehlungen wurden aus dem Microsoft Secure Score übernommen und sollten überprüft werden. Dies sind die Top 10 der Gesamtübersicht. Wir empfehlen, den Secure Score regelmäßig zu überprüfen. um die Sicherheitslage zu verbessern.

	Kategorie	Score	Beschreibung
Contoso.onmicrosoft.com			
Require MFA for administrative roles	Identity	0/10	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.
Enable Password Hash Sync if hybrid	Identity	5/5	Password hash synchronization is one of the sign-in methods used to accomplish hybrid identity. Azure AD Connect synchronizes a hash, of the hash, of a user's password from an on-premises Active Directory instance to a cloud-based Azure AD instance. Password hash synchronization helps by reducing the number of passwords your users need to maintain to just one. Enabling password hash synchronization also allows for leaked credential reporting.
Ensure all users can complete multi-factor authentication for secure access	Identity	0/9	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.
Enable self-service password reset	Identity	0/1	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.
Designate more than one global admin	Identity	1/1	Having more than one global administrator helps if you are unable to fulfill the needs or obligations of your organization. It's important to have a delegate or an emergency account someone from your team can access if necessary. It also allows admins the ability to monitor each other for signs of a breach.

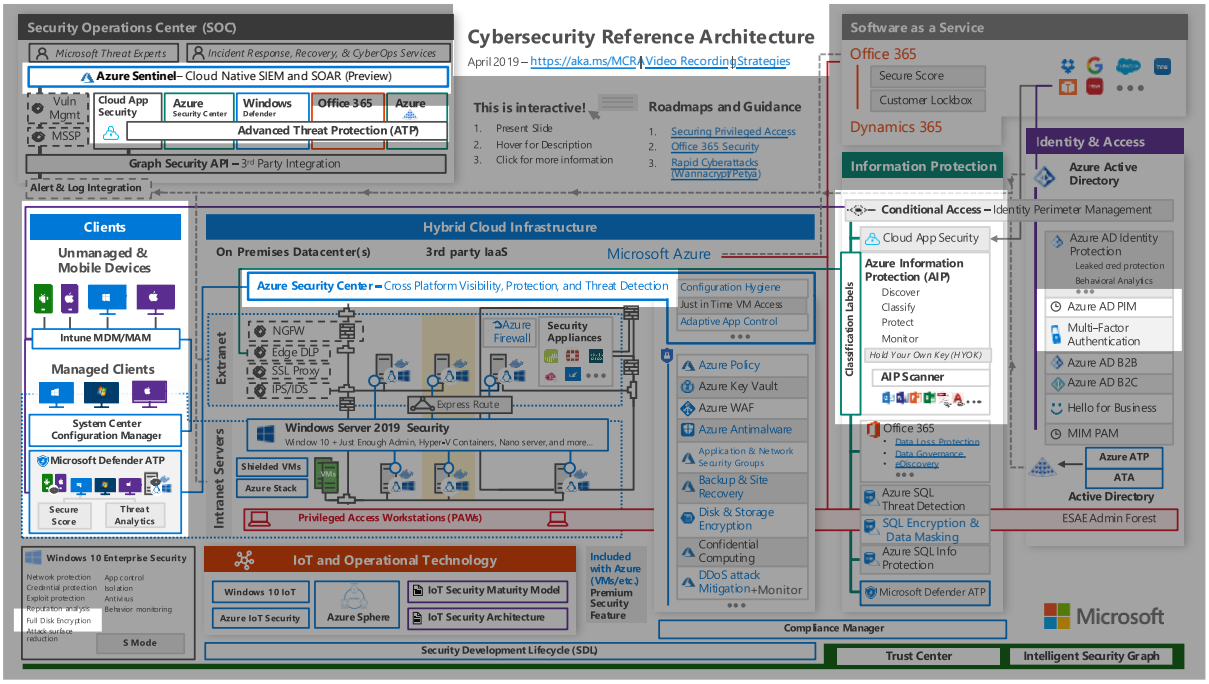
Do not expire passwords	Identity	0/8	Research has found that when periodic password resets are enforced, passwords become less secure. Users tend to pick a weaker password and vary it slightly for each reset. If a user creates a strong password (long, complex and without any pragmatic words present) it should remain just as strong in the future as it is today. It is Microsoft's official security position to not expire passwords periodically without a specific reason, and recommends that cloud-only tenants set the password policy to never expire.
Do not allow users to grant consent to unmanaged applications	Identity	4/4	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.
Remove TLS 1.0/1.1 and 3DES dependencies	Apps	1/1	Review all your clients to check which ones use TLS 1.0/1.1 and 3DES to communicate with Office 365. The goal is to upgrade your clients to move away from using weaker protocols and cipher. You can access a report showing all the TLS 1.0/1.1 and 3DES connections in your tenants grouped by user and agent information. After all your clients are migrated and the usage below is zero, you will be awarded full points.
Use limited administrative roles	Identity	1/1	Limited administrators are users who have more privileges than standard users, but not as many privileges as global admins. Leveraging limited administrator roles to perform required administrative work reduces the number of high value, high impact global admin role holders you have. Assigning users roles like Password Administrator or Exchange Online Administrator, instead of Global Administrator, reduces the likelihood of a global administrative privileged account being breached.
Turn on sign-in risk policy	Identity	0/7	Turning on the sign-in risk policy ensures that suspicious sign-ins are challenged for multi-factor authentication (MFA).

Azure Security Center Secure Score

<keine Daten>

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. Diese Referenzarchitektur berücksichtigt auch die bereits früher in diesem Bericht erläuterten Zero Trust Architecture-Prinzipien.



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.

Microsoft 365 Business und Microsoft 365 E3

Microsoft 365 Business und Microsoft 365 E3 enthalten die Basissicherheitssuite Enterprise Mobility + Security E3.

Die folgenden Sicherheitsprodukte sind in Microsoft 365 Business verfügbar. Bitte beachten Sie, dass Microsoft 365 Business nur bis maximal 300 Seats reicht. Bei mehr Seats ist Microsoft 365 E3 erforderlich.

Die mit (E3) gekennzeichneten Elemente sind nur in Microsoft 365 E3 enthalten.

- EMS - Azure Active Directory P1
    - Enthält Self Service Passwort-Reset für Azure AD
- EMS - Microsoft Information Protection Plan 1
- EMS - Conditional Access
    - bietet differenzierte Zugriffssteuerung, um Ihre Unternehmensdaten sicher zu halten. Dabei ermöglicht es Benutzern ihre Arbeite bestmöglich von jedem Gerät und von jedem Ort aus zu erledigen.
- EMS - Azure AD Conditional Access und Multi-Factor Authentication (E3)
- EMS - Microsoft Endpoint Manager

    - fokussiert auf Mobile Device Management (MDM) und Mobile Application Management (MAM) für Windows, Android und iPhone
- Microsoft Defender for Office 365 - Malware Detection
- Windows 10 - BitLocker
- Windows 10 - Hello for Business
- Windows 10 - Windows Defender Application Control Guard
- Windows 10 - Windows Defender Credential Guard
- Data Loss Prevention (DLP)

Anhang B - Produkte, bei denen der Support ausläuft

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

End-of-Life-Produkte	
WINDOWS XP	
WINDOWS 7 SERVICEPACK1	
WINDOWS 10 1511	
WINDOWS 10 1607	
WINDOWS 10 1703	
WINDOWS 10 1709	
WINDOWS 10 1903	
WINDOWS 10 PRO 1809	
WINDOWS SERVER 2008 R2 SP1	
WINDOWS SERVER 2012	
WINDOWS SERVER 2012 R2	
Microsoft Office Professional Plus 2007	
SQL Server 2005	
SQL Server 2008	
SQL Server 2008 R2	
SQL Server 2012	
SQL Server 2014	
SQL Server 2016	

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

Produkte, bei denen das End-of-Life bevorsteht	
WINDOWS SERVER 2016 1067	
WINDOWS 10 ENTERPRISE 1809	
WINDOWS 10 1909	
WINDOWS 10 2004	

Die folgenden unterstützten Builds von Windows 10 wurden gefunden:

Windows 10 - Unterstützte Builds	
Microsoft Windows 10 Enterprise LTSC version 1809	1
Microsoft Windows 10 Enterprise version 1809	137
Microsoft Windows 10 Enterprise version 1909	68
Microsoft Windows 10 Entreprise version 1809	5
Microsoft Windows 10 Entreprise version 1909	1
Microsoft Windows 10 企业版 version 1809	2

Die folgenden nicht unterstützten Builds von Windows 10 wurden gefunden:

Windows 10 - Nicht unterstützte Builds	
Microsoft Windows 10 Enterprise version 1703	3
Microsoft Windows 10 Enterprise version 1709	56
Microsoft Windows 10 Entreprise version 1709	2
Microsoft Windows 10 Pro version 1809	4
Microsoft Windows 10 企业版 version 1709	4

Anhang C – Umfang des Assessments

Das Cybersecurity Assessment wurde unter Berücksichtigung der folgenden Scoping-Informationen durchgeführt:

Organisation	
Name des Kunden	Contoso GmbH
Kerngeschäft	IT
Adresse Hauptsitz des Kunden	Am Berg 1 • 50226 Frechen • Germany
Anzahl der Mitarbeiter	3000
Standort(e)	weltweit

IT-Umgebung	
Plattform-Architektur	Hybrid
Virtualisierungsplattform(en)	VM Ware
Schutz vor Malware	Windows Defender
Software-/Patch-Management	SCCM
(Mobile) Device Management	MobileIron

Schlüssel-Termine und Fristen des Assessments	
Aktivität	**Datum**
Kick-off-Gespräch mit dem Kunden	29.3.2021
Komplette Interview-Serie und Bestandserfassung vor Ort	19. + 26.4.2021
Analyse / Bewertung der Daten aus der Inventarisierung	30.4.2021
Übergabe der Berichte	3.5.2021
Letztes Gespräch mit Kunden zur Überprüfung aller gelieferten Dokumente	

Assessment-Teilnehmer von Partnern		
Name	**Unternehmen**	**Projektrolle**
Dieter Klein	QS solutions	Berater

Interviews wurden von QS solutions mit den wichtigsten Beteiligten durchgeführt, um - zusätzlich zur automatisierten Inventarisierung der IT-Infrastruktur - Informationen zu sammeln. Die Ergebnisse basieren auf den Antworten der im Cybersecurity-Fragebogen enthaltenen Fragen. Interviews wurden mit den folgenden Beteiligten bei durchgeführt:

Befragter	Position	Interviewer
Thomas Scharf	Group Head of Network Technology	
Hans Erbacher	System Administrator	
Max Fuchs		
Uwe Groß		

Ziele des Cybersecurity Assessments

Wie viele andere Organisationen auch, befasst sich Contoso 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 von Contoso 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.

Inventory Tools

Zur Bewertung der IT-Infrastruktur (Technical Topics) von Contoso wurde das Cyber Security Assessment Tool verwendet, um die erforderlichen Informationen zu ihrem aktuellen Konfigurationsstatus zu erfassen.

Cyber Security Assessment Tool

CSAT wird von erfahrenen Sicherheitsexperten entwickelt, um schnell den Reifegrad 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. Endpunkte, Active Directory oder SharePoint. Darüber hinaus verwendet CSAT 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.

Anhang D - Hintergrund des Assessments

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 *Fortune 500* 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™ (v7)** Sicherheits-Framework, das vom **Center for Internet Security®** (CIS) (http://www.cisecurity.org) veröffentlicht wurde. Siehe: Anhang D - Hintergrund des Assessments

Im Rahmen des Cybersecurity Assessments wurde das Niveau der Cybersecurity Practice von Contoso über die Beantwortung eines Fragebogens gemessen. Der Fragebogen basiert auf den Praktiken der Domänen Basic, Foundational und Organizational des CIS Control™ (v7) Sicherheits-Frameworks.

Zusätzlich zum Fragebogen wurden relevante, sicherheitsbezogene Daten zur IT-Umgebung von Contoso 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 Contoso abgeleitet.

Hintergrund des Control Frameworks (CIS)

Das CIS Controls™ (v7) 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™ (v7) 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™ (v7) 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™ (v7) 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™ (v7) konzentrieren sich stattdessen auf eine kleinere Zahl vergleichsweise einfach umsetzbarer Steuerelemente mit hoher Hebelwirkung und großem Nutzen.

Für das Cybersecurity Assessment werden die technischen CIS Controls™ (v7) 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.

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.