M365 Security Assessment

Report, 19.04.2024

VERTRAULICH

CUSTOMER

INHALTSVERZEICHNIS

1 MANAGEMENT SUMMARY

1.1 Ausgangslage und Auftrag

Die **CUSTOMER** (nachfolgend auch als XXX referenziert) hat die InfoGuard beauftragt die Microsoft 365 Umgebung in der Cloud einem Security- und Konfigurationsreview zu unterziehen. Damit will die XXX sicherstellen, dass die aktuellen Einstellungen auf Seiten des Microsoft Tenants und der Microsoft 365 Plattform ihren Zweck erfüllen und den Security Best Practices entsprechen.

1.2 Assessment Scope

Als Bestandteile der M365 Infrastruktur wurden die folgenden Kernkomponenten genannt (Siehe Kapitel 2.2):

- Microsoft Entra ID (ehem. Azure Active Directory)
- Exchange Online
- SharePoint/OneDrive
- Teams

1.3 Gesamtbeurteilung Microsoft 365 Security

1.3.1 Technische Risiko Bewertung M365

Insgesamt ist der Tenant auf Basis der Assessment Beobachtungen bereits sehr gut aufgestellt und viele Einstellungen wurden unter Berücksichtigung der Sicherheit vorgenommen. In den verschiedenen Teilbereichen gibt es weiterhin Verbesserungspotenzial. Insgesamt stellt sich das Sicherheitsdispositiv unter Berücksichtigung der Schwachstellenklassifikation (siehe Kapitel 3.2) und dem hinzugezogenen Prüfkatalog in 72% (Information/Geringe Schwachstellen) und 28% (Mittlere- und hohe Schwachstellen) dar. Das aktuelle Microsoft 365 Sicherheitsdispositiv entspricht im Durchschnitt einer hohen Maturität.

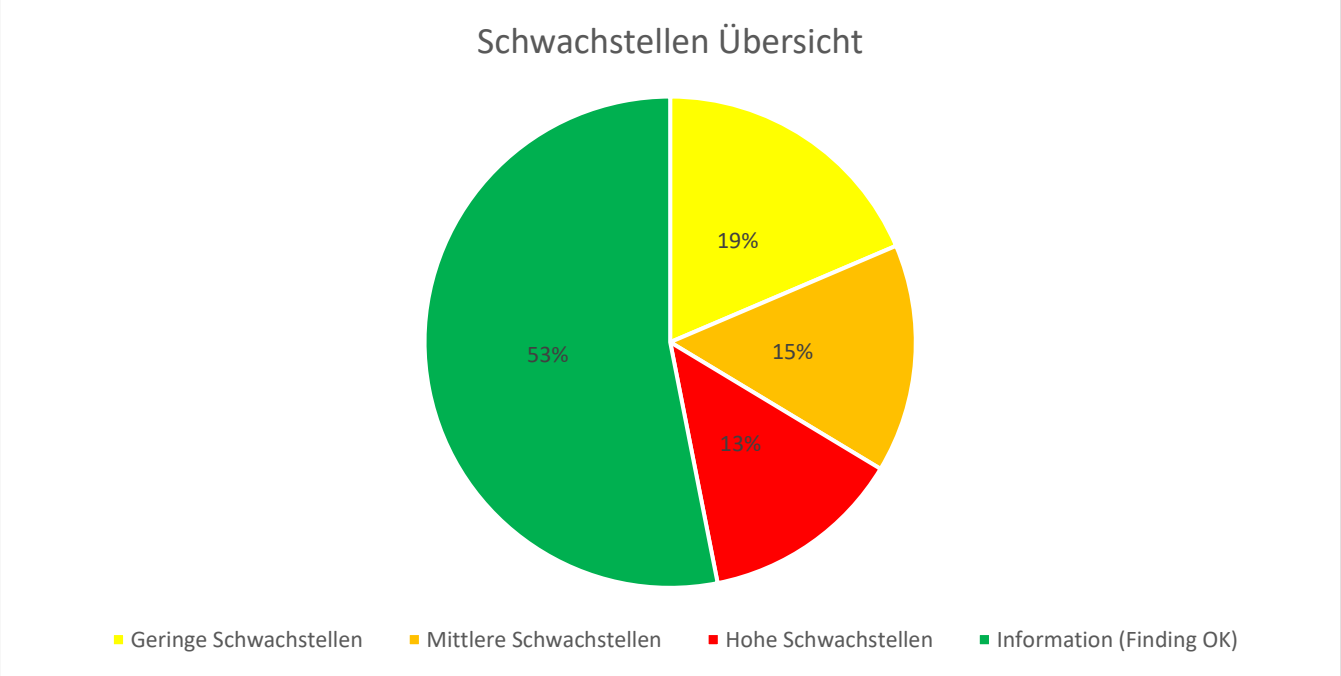

Abbildung 1 Übersicht der Schwachstellen und Verteilung (Schwachstellenklassifikation: siehe Kapitel 3.2)

Das technische Sicherheitsdispositiv in konkreten Zahlen, basierend auf dem Prüfkatalog mit 113 individuellen Prüfpunkten.

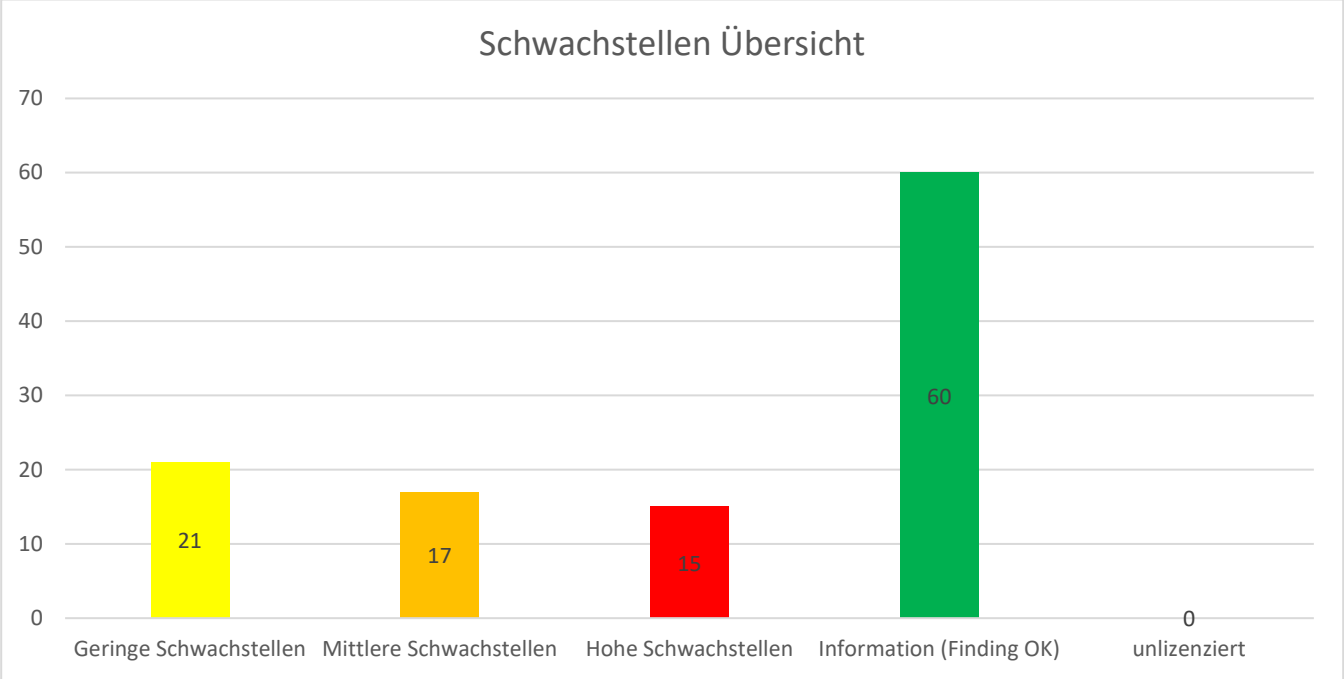

Abbildung 2 Übersicht Anzahl der Schwachstellen und Verteilung

Die Teilbereiche in welchen noch Verbesserungspotenzial liegt, verteilen sich auf die verschiedenen Komponenten von Microsoft 365. Dabei gibt es die folgenden primären Handlungsfelder:

- **Authentifizierung und Autorisierung:** Die Authentifizierungsmethoden sollen anhand der Beobachtungen gehärtet werden. Ebenfalls sollte der Zugriff für Administratoren mit zusätzlichen Conditional Access Richtlinien ergänzt werden. Weiter gibt es diverse Tenant Einstellungen, welche das Sicherheitsdispositiv zusätzlich erhöhen würden.
- **Mail-Kommunikation:** Die identifizierten Exchange Online Schwachstellen sollten evaluiert und implementiert werden. Unter der Berücksichtigung der derzeitigen Architektur soll entschieden werden, welche Massnahmen umgesetzt werden sollen.
- **Kollaborationssicherheit:** Die bereits bestehenden Richtlinien und Sicherheitsmechanismen sollten weiter an die Best-Practice-Ansätze angenähert werden. Dies beinhaltet den Schutz der Kollaboration über SharePoint Online, OneDrive for Business und Teams.

1.4 Bereinigung von Artefakten

Während des durchgeführten Microsoft 365 Security Assessments wurden verschiedene Artefakte auf Systemen hinterlassen. Diese können jedoch nur durch den Kunden entfernt werden. Alle Artefakte können nachfolgender Tabelle entnommen werden. Um den ursprünglichen Zustand der Systeme wiederherzustellen, wird empfohlen, diese Artefakte zu bereinigen.

AUFGABE	BESCHREIBUNG
Benutzeraccount löschen	Der zur Verfügung gestellte Benutzeraccount sollte gelöscht werden: • XXXXX@XXXcloud.onmicrosoft.com

Tabelle 1 Bereinigung von Artefakten

2 M365 SECURITY ASSESSMENT

2.1 Vorgehen

Die Erfassung des IST-Zustandes erfolgt mittels unterschiedlicher Methoden. Es wird eine einmalige Prüfung des Tenants durchgeführt, wobei die typischen Security und Best-Practice-Ansätze geprüft und dokumentiert werden. Diese Prüfung erfolgt teils automatisiert und teils manuell, wobei die Ergebnisse durch einen Cloud Security Engineer evaluiert werden.

Während des Assessment vom XXXX bis XXXX wurden die folgenden Punke berücksichtigt:

- Aufnahme der IST-Situation der derzeitigen Microsoft 365 Umgebung
- Eine individuelle **technische** Risikobewertung und Priorisierung der 113 Prüfpunkte.

Die identifizierten technischen Schwachstellen und Optimierungspotenziale werden anhand des Prüfkatalogs bewertet. Dabei wird jeder Prüfpunkt für alle Organisationen identisch auditiert, egal ob die Services effektiv eingesetzt werden oder nicht. Einzig anhand der Lizenzierung werden gewisse Prüfpunkte bei fehlenden Lizenzen exkludiert und mit der Klassifikation «Unlizenziert» deklariert.

Nach dem Assessment liegen die folgenden Ergebnisse vor:

- Eine Übersicht über das derzeitige Sicherheitsdispositiv der Microsoft 365 Lösung.
- Eine Bewertung basierend auf den Komponenten von Microsoft 365 und der Identitätsplattform.

Die effektive Risikobewertung der einzelnen Schwachstellen muss durch den Kunden selbst durchgeführt werden. Dies kann in der Excel-Taskliste mit der Spalte «Status» dokumentiert werden. Danach kann im Sheet «Helper» die aktualisierte Schwachstellen Übersicht anhand des Mapping aus Kapitel 3.3 gesichtet werden.

2.2 Detaillierte Scope Beschreibung

Die InfoGuard hat im Auftrag des Kunden ein Microsoft 365 Security Assessment durchgeführt, welches typische sicherheitskritische Einstellungen überprüft. Diese Checks sind aus den Erfahrungswerten der InfoGuard im Rahmen von Incident Response Vorfällen, aus dem Penetration Testing sowie von Microsoft Best Practice und CIS/CISA Vorgaben zusammengestellt.

Das Assessment betrachtet dabei die folgenden Aspekte eines typischen Microsoft Tenants:

- Microsoft Entra ID (ehem. Azure Active Directory)
- Exchange Online
- SharePoint/OneDrive
- Teams
- Defender for Office 365

2.3 Ergebnisse aus dem Assessment

2.3.1 Entra ID und Microsoft Tenant

Unter dem Begriff «Entra ID und Microsoft Tenant» wird das Identitiy Setup, die umgesetzten Microsoft Zero Trust Prinzipien wie auch die generelle Tenant Sicherheit evaluiert. Für die XXX wurde Microsoft Entra ID Premium mit Plan 2 identifiziert. Somit sind Funktionen wie Identitiy Protection, Identitiy Governance wie auch Conditional Access verfügbar.

Die Synchronisierung der lokalen Identitäten mit den Cloud Identitäten erfolgt mittels Entra Connect, wobei der Password-Hash-Sync nicht aktiviert wurde. Single-Sign-On via Entra Connect und die Self-Service-Password-Reset Funktionalität wurden ebenfalls nicht aktiviert.

Die Microsoft Zero Trust Prinzipien für die XXX wurden konfiguriert und weisen eine hohe Maturität auf. Dabei wurde ein durchdachtes und voll ausgearbeitetes Conditional Access Regelwerk identifiziert. Das Conditional Access Regelwerk sollte lediglich eine dedizierte MFA Policy für Administratoren (IGM365_197, IGM365_200) und einer «Microsoft Azure Management» (IGM365_204) Policy ergänzt werden.

Die Allgemeinen Tenant Einstellungen weisen bereits eine hohe Maturität auf. Die «Consent» Einstellungen für die Enterprise Applikationen sind restriktiv, und erlauben normalen Benutzern keine Integration von Drittanbieter Applikationen. Dies entspricht der Best-Practices. Ebenfalls wurde der Gastzugriff auf andere Entra Objekte wie auch das Einladen von Gastbenutzern eingeschränkt.

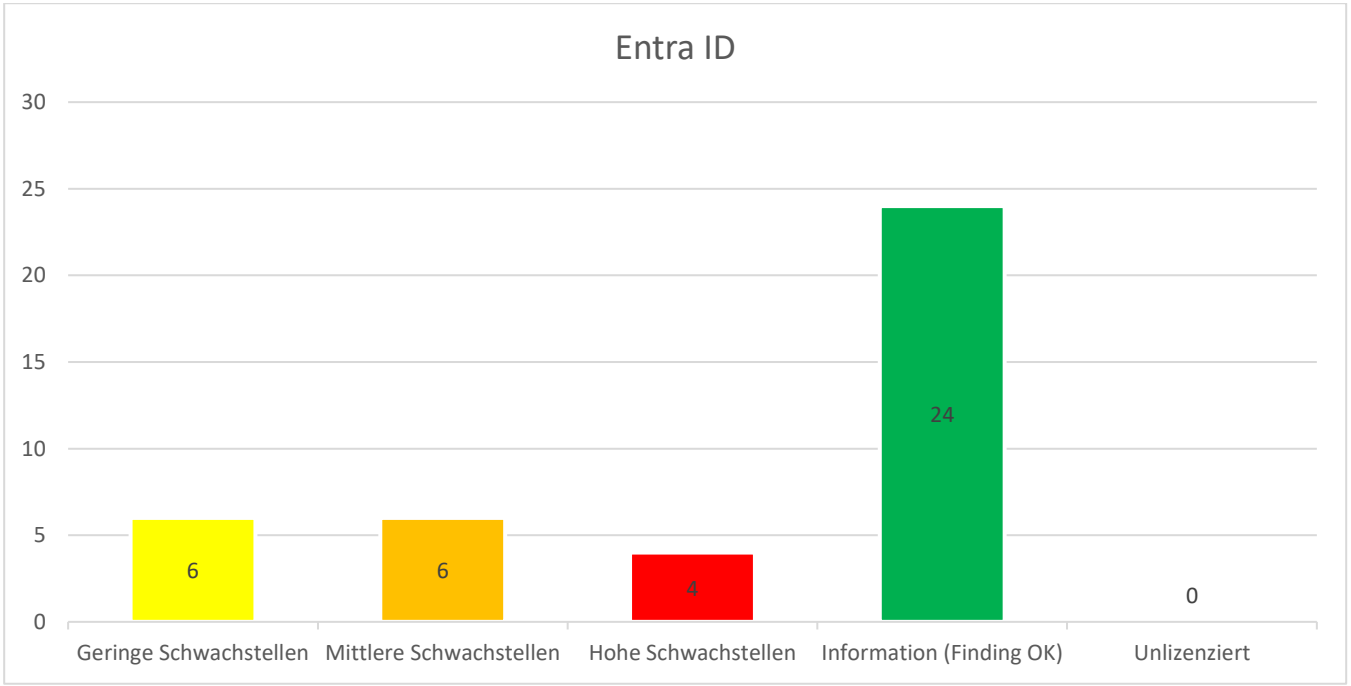

Abbildung 3 Übersicht Schwachstellen zu Entra ID

2.3.2 Privileged Access

Unter Privileged Access versteht sich der privilegierte Zugriff zum XXX Microsoft Tenant, genauer um die Entra ID Rollen Berechtigungen. Die Betrachtung des privilegierten Zugriffs auf den Tenant ist ein wichtiger Bestandteil des Assessments. Hier gilt es insbesondere das Prinzip des Least-Privilege Ansatzes konsequent umzusetzen. Dabei sollte darauf geachtet werden, dass Benutzern lediglich die Rechte eingeräumt werden, die sie für die Erledigung ihrer Arbeiten benötigen. Auch ein Augenmerk sollte auf die Anzahl der Benutzer mit der Rolle «Global Administrator» gelegt werden.

Die XXX hat bereits diverse Massnahmen für den Schutz des privilegierten Zugriffes getroffen, jedoch gibt es noch Verbesserungspotenzial. Es wurden drei «Global Administrator»-Gruppen identifiziert, dies sollte auf maximal eine beschränkt werden. Ebenfalls kann das Alerting mittels PIM noch weiter ausgebaut werden. Für die beiden Break-Glass-Administratoren sollten ebenfalls dringend ein Alerting aktiviert werden. Anhand der fehlenden Berechtigung zum Monitoring konnte ein allenfalls vorhandenes Alerting nicht gesichtet werden.

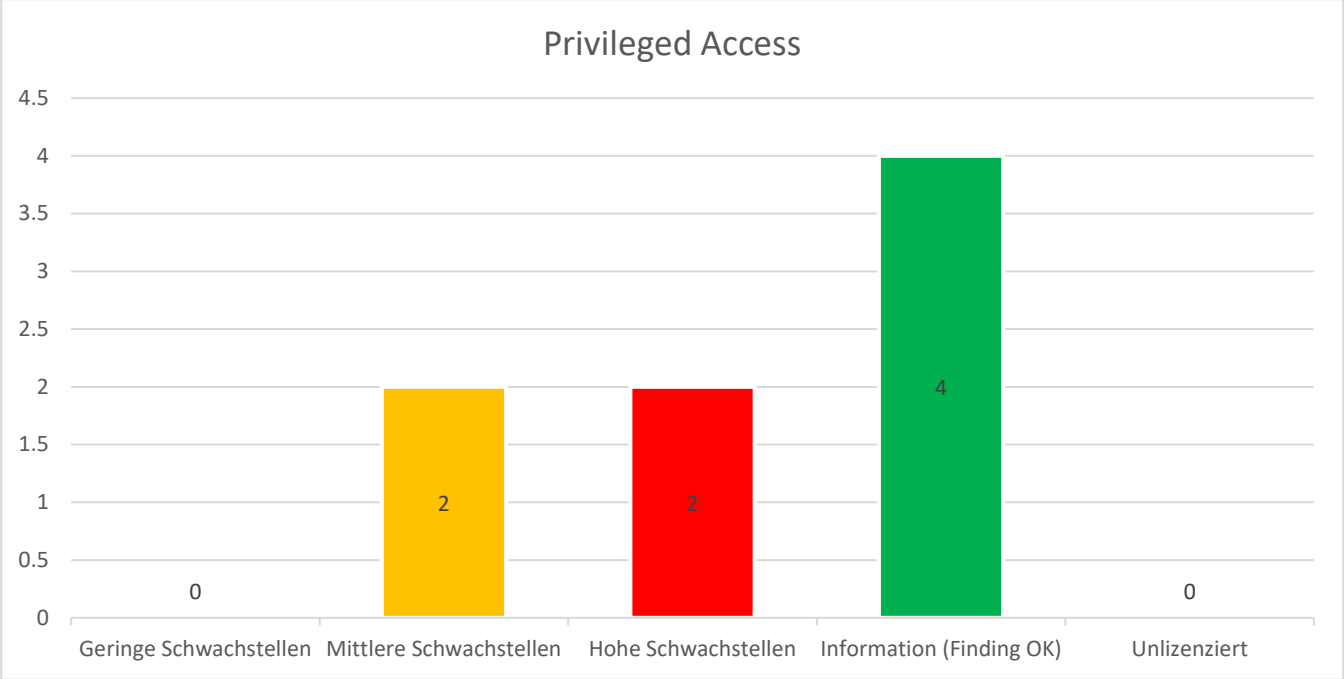

Abbildung 4 Übersicht Schwachstellen zu Privileged Access

2.3.3 Exchange Online und Microsoft Defender for Office 365

Exchange Online wird derzeit noch nicht aktiv verwendet. Die Sicherheitsfunktionen aus dem Microsoft Defender for Office 365 (MDO) sind im Einsatz. Die MDO wie auch Exchange Online Protection Policies sollten mit den Empfohlenen Massnahmen aus dem Report ergänzt werden. Dazu gehört insbesondere die Härtung der Anti-Phishing, Safe Links und Safe Attachments Funktionen.

Insgesamt sollten noch mehr Supportfunktionen für die Benutzer eingerichtet werden. Dies beinhaltet die Phishing Tips, Exchange Mail Tips wie auch die External Sender Warnung. Durch die Implementation der Supportfunktionen erhält der Benutzer mehr Kontext über die laufende Kommunikation, welcher bestenfalls mittels interner Weisung noch genauer erläutert wird.

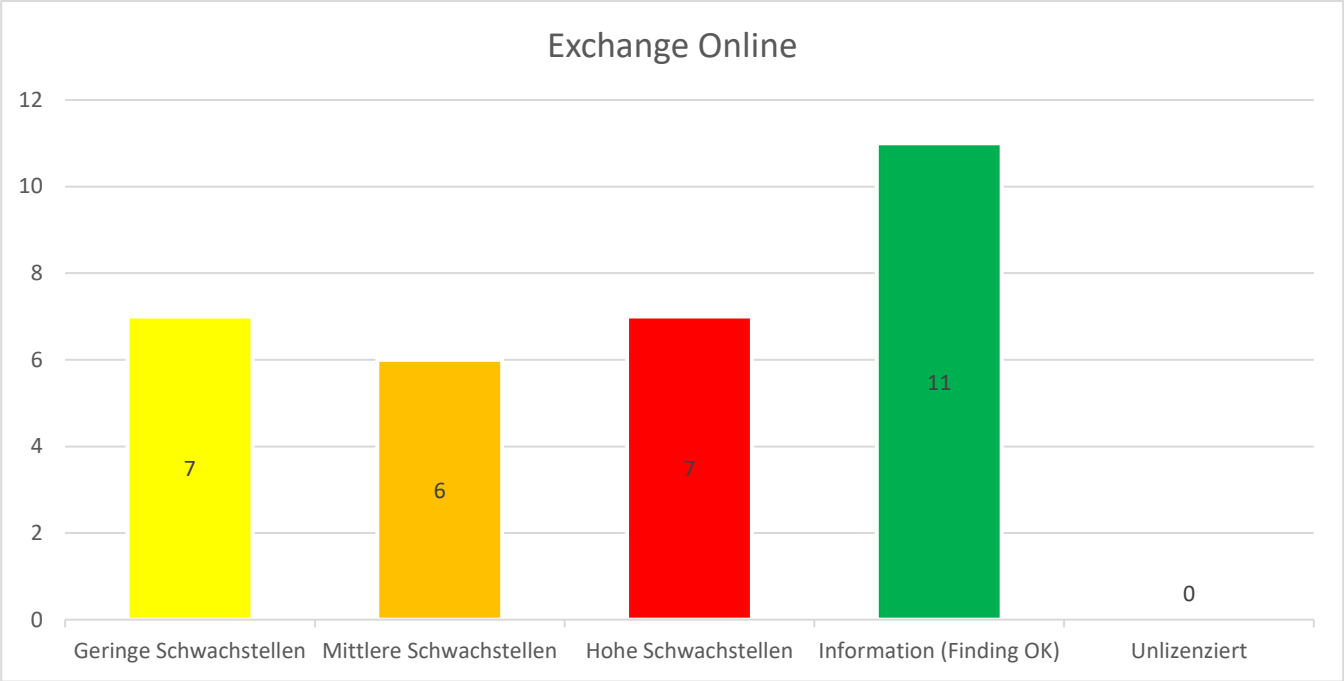

Abbildung 5 Übersicht Schwachstellen zu Exchange Online

2.3.4 SharePoint Online und OneDrive

SharePoint Online und OneDrive for Business werden momentan lediglich von einem kleinen Teil der XXX verwendet. Die MDO-Funktionalitäten sind aktiviert und im Einsatz. Das Whitelisting externer Domänen sollte evaluiert werden, generell sollte die Entra ID B2B Integration (IGM365_241) aktiviert werden, anhand dieser Einstellung wird der Umgang mit Gästen und dessen Restriktionen von Entra ID selbst übernommen.

SharePoint Online bzw. OneDrive for Business sind Kollaborationstools – die Idee dahinter ist oft das Teilen von Daten mit Dritten und nicht nur das Nutzen einer gemeinsamen Dateiablage ausschliesslich für das eigene Unternehmen. Daher sind die gefundenen Schwächen etwas zu relativieren, da diese primär das Teilen der Daten mit Dritten adressieren.

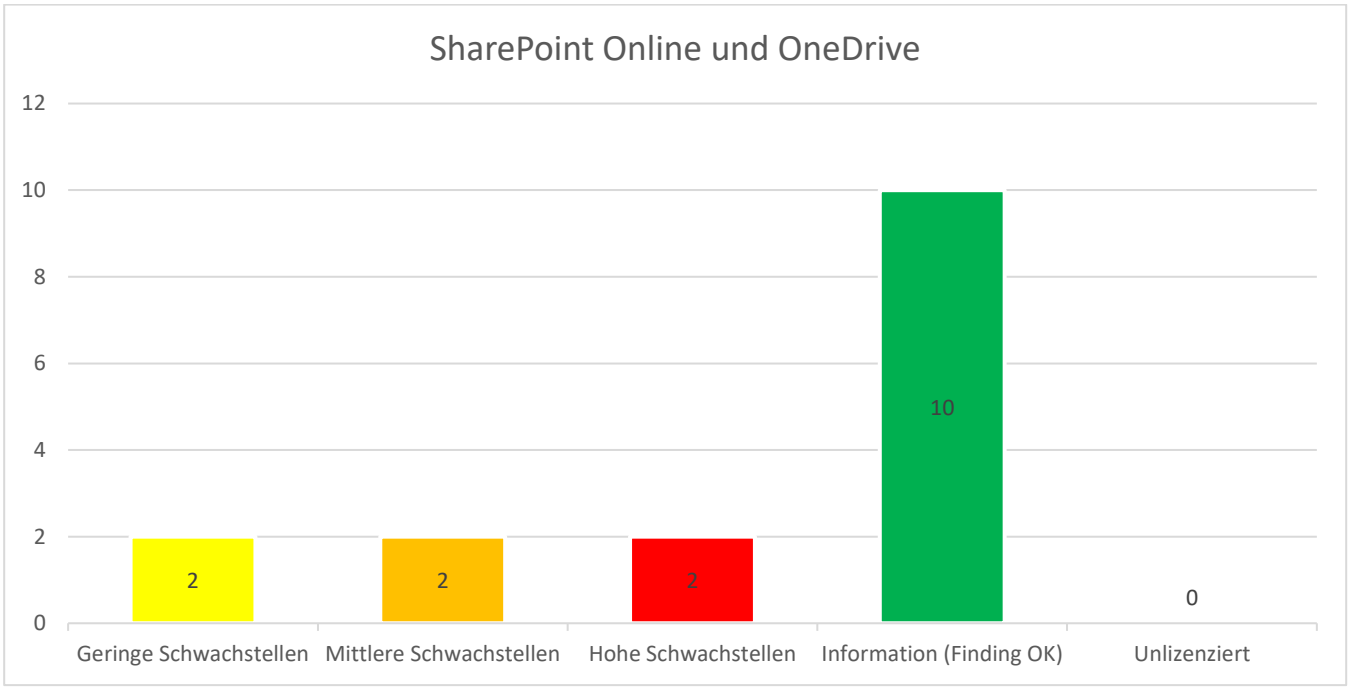

Abbildung 6 Übersicht Schwachstellen zu SharePoint Online und OneDrive for Business

2.3.5 Teams

Teams ist für die XXX aktiv im Einsatz und umfasst bereits diverse Sicherheitsmassnahem. Die MDO-Funktionalitäten sind für Teams aktiviert und im Einsatz. Einzig die Meeting Policy sollte anhand der identifizierten Schwachstellen evaluiert und weiter eingeschränkt werden. Hier gilt es jedoch zu beachten, dass die Sicherheit an den Kollaborations-Use-Case der XXX angeglichen wird. Ebenfalls sollte die erlaubte Kommunikation mit Skype Benutzern deaktiviert werden.

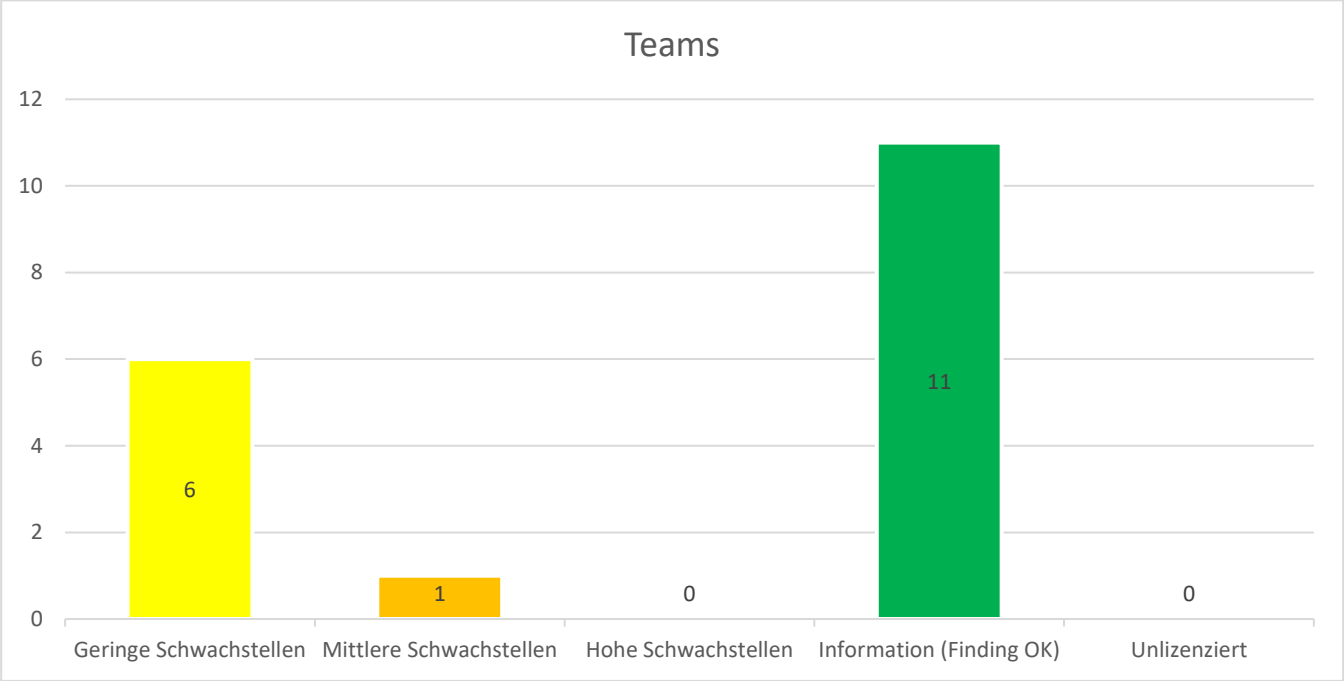

Abbildung 7 Übersicht Schwachstellen zu Teams

2.4 Nächste Schritte

Das Excel «XXX_Microsoft-365-Security-Assessment_Tasklist.xlsx» enthält die detaillierten Ergebnisse aus dem Microsoft 365 Security Assessment. Dabei basiert die Tabelle «Findings» auf dem Prüfkatalog und umfasst 113 einzelne Prüfpunkte. Es wird empfohlen die einzelnen Mitigationen anhand der jeweiligen Anleitung der Unternehmung angepasst durchzuführen.

2.4.1 Empfohlenes weiteres Vorgehen

Wie bereits im Vorgehen erwähnt, handelt es sich bei der Excel-Taskliste um eine Sammlung von technischen Schwachstellen und Optimierungspotenzialen. Die eigentliche Risikobewertung soll durch die Unternehmung erfolgen. Dabei sollen in der Excel-Taskliste die Spalten «Priorität», «Zuständig», «Status», «Erledigt per» und «Bemerkung» zur Dokumentation verwendet werden. Das Ergebnis aus der Dokumentation mit den genannten Spalten ist eine aktualisierte Risiko Übersicht im «Helper» Sheet, basierend auf der «Status» Spalte und dem Mapping aus Kapitel 3.3. Ebenfalls wird direkt ein erster Implementationsplan der Schwachstellen mit dem Status «Offen» und «in Bearbeitung» erstellt.

Weiter empfehlen wir anhand des ersten Implementierungsplans die festgestellten Schwachstellen und Optimierungspotenziale anhand der definierten Umsetzungspriorität und individuellen Risikobewertung innerhalb der folgenden Fristen umzusetzen:

- **Umsetzungspriorität 1**: kurzfristig [sofortige Umsetzung – 1 Monat]
- **Umsetzungspriorität 2**: mittelfristig [innert 1 – 6 Monate]
- **Umsetzungspriorität 3**: Individualentscheidung [Entscheidung von Fall zu Fall]

2.4.2 Excel-Taskliste

Die folgende Tabelle beschreibt die einzelnen Spalten der Excel-Taskliste.

SPALTE	BESCHREIBUNG
ID	Identifikation der Findings der InfoGuard (Informativ)
Lvl (Baisc/Advanced)	Stufe des Microsoft 365 Security Assessments. (B für Basic, A für Advanced)
OK/NOK	Ergebnis der Prüfung
Check	Prüfpunkt, was wurde geprüft?
Beobachtung	IST-Zustand, welcher aus der produktiven Umgebung der Unternehmung extrahiert wurde.
Risiko bei nicht Umsetzung	Einschätzung, was bei nicht Umsetzung des entsprechenden Checks für ein Risiko für die Unternehmung entsteht.
Mitigation	Anleitung, wie die Best-Practice Ansätze erfolgreich implementiert werden können.
Risiko	Klassifizierung des Risikos basierend auf der Schwachstellenklassifikation aus dem Kapitel 3.2.
Priorität	Umsetzungspriorität basierend auf den Werten aus dem Kapitel 2.4.1 oder den organisationsinternen Umsetzungsprioritäten (Optional, muss von der Unternehmung nachträglich vergeben werden.).
Zuständig	Definition des Besitzers des aktuellen Checks.
Status	Aktueller Status des Checks: • **«Offen»:** Der Prüfpunkt ist offen und wurde noch nicht bearbeitet. • **«In Bearbeitung»:** Die Bearbeitung des Prüfpunktes wurde gestartet. • **«Erledigt»:** Der Prüfpunkt ist erledigt. • **«Nicht Zutreffend»:** Der Prüfpunkt trifft nicht auf die Umgebung der Unternehmung zu. • **«Wird nicht umgesetzt»:** Das Risiko des Prüfpunktes wurde anderweitig adressiert oder gänzlich akzeptiert.
Erledigt per	Definition bis wann die Mitigation implementiert wird.
Bemerkungen	Freifeld, um allfällige Bemerkungen zu erfassen und allenfalls Risiken zu dokumentieren.

Tabelle 2 Excel-Taskliste Legende

3 ANHANG

3.1 Begriffsverzeichnis

BEGRIFF	BESCHREIBUNG
Microsoft Tenant	Ein Microsoft Tenant bezieht sich auf die Instanz einer Cloud-Umgebung, die von einem Kunden in der Microsoft Cloud genutzt wird. Ein Tenant repräsentiert die organisierte Struktur von Ressourcen, Benutzern und Diensten innerhalb der Microsoft Cloud-Plattform. Jeder Kunde hat einen eigenen separaten Cloud Tenant, welcher sicherheits- und identitätsmässig isoliert ist.
Microsoft Defender XDR	Microsoft Defender XDR ist eine vereinheitlichte Enterprise Defense Suite vor und nach der Verletzung, die Erkennung, Prävention, Untersuchung und Reaktion nativ über Endpunkte, Identitäten, E-Mails und Anwendungen hinweg koordiniert, um integrierten Schutz vor komplexen Angriffen zu bieten. Microsoft Defender XDR Produkte und Lösungen: • Defender for Endpoint • Defender for Office 365 • Defender for Identitiy • Defender for Cloud Apps • Defender Vulnerability Management • Entra ID Protection • Data Loss Prevention • App Governance
Microsoft Entra ID	Microsoft Entra ID (ehemalig: Azure Active Directory) ist ein Identitäts- und Zugriffsverwaltungsdienst von Microsoft, welcher in der Azure-Cloud-Plattform integriert ist. Entra ID ermöglicht die sichere Verwaltung von Benutzeridentitäten, Authentifizierung und Autorisierung für Cloud-basierte Anwendungen und Dienste.
Conditional Access (CA)	Conditional Access ist eine Funktion von Microsoft Entra ID, die es Administratoren ermöglicht, den Zugriff auf Ressourcen basierend auf bestimmten Bedingungen zu steuern. Diese Bedingungen können Signale wie Benutzerstandort, Gerätetyp, Sicherheitsstatus und andere Attribute umfassen. Durch die Implementation von Conditional Access können Organisationen ihr Sicherheitsdispositiv stärken, indem gezielte Zugriffskontrollen für digitale Ressourcen festgelegt werden können.
Break-Glass-Administrator	Ein Break-Glass-Administrator ist ein spezieller Administrator-Account, der für Notfälle oder aussergewöhnliche Situationen vorgesehen ist. Der Zugriff auf diesen Account wir streng kontrolliert und erfordert besondere Genehmigungsverfahren. Der Account wird nur in dringenden Fällen verwendet, wenn der normale Zugang zum Microsoft Tenant nicht verfügbar ist.

Tabelle 3 Begriffsverzeichnis

3.2 Schwachstellenklassifikation

Die folgende Tabelle listet die verschiedenen Klassen von Schwachstellen auf und gibt eine Standardmassnahme für das Beheben der Sicherheitsrisiken vor. Dies stellt eine rein technische Einschätzung unter dem Gesichtspunkt der Security dar. Daher soll diese Empfehlung lediglich als Standardempfehlung verstanden werden. Grundsätzlich sollte für jede Massnahme vor der Umsetzung eine Kosten-/Nutzen Analyse durchgeführt werden, sofern dies für das jeweilige Risiko vertretbar ist.

SYMBOL	HINTERGRUNDINFORMATION
 Hohe Schwachstelle	**TECHNISCH** Unmittelbare Bedrohung des Systems: ein Ausnutzen der Schwachstelle kann zur Übernahme der Kontrolle über ein System bzw. zum Abfluss von sensitiven Informationen führen. **KONZEPTIONELL / ORGANISATORISCH** Grobe Fehler im Design des Netzwerks oder ein komplettes Fehlen von konzeptionellen/organisatorischen Sicherheitsvorkehrung.
 Mittlere Schwachstelle	**TECHNISCH** Mittelschwere Schwachstelle: keine direkte Bedrohung des Systems (in Kombination mit anderen mittelschweren Schwachstellen ist eine Bedrohung aber nicht ausgeschlossen). **KONZEPTIONELL / ORGANISATORISCH** Fehler im Design des Netzwerks oder eine massgebliche Schwächung von konzeptionellen/organisatorischen Sicherheitsvorkehrungen.
 Geringe Schwachstelle	**TECHNISCH** Geringfügige Schwachstelle: keine unmittelbare Bedrohung des Systems. Die aktuelle technische Umsetzung entspricht nicht momentanen «Best Practices» **KONZEPTIONELL / ORGANISATORISCH** Abweichungen von Best Practice Ansätzen bezüglich Konzeption und Organisation.
 Information	Während der Überprüfung wurden keine Sicherheitsprobleme detektiert. Die Prüfpunkte gelten als «OK».
 Unlizenziert	Die Überprüften Funktionen sind im derzeitigen Lizenzumfang der Unternehmung nicht enthalten.

Tabelle 4 Übersicht über die Schwachstellenklassifikation

3.3 Schwachstellenklassifikation zu Risiko Mapping

Die nachfolgende Tabelle listet das Mapping der verschiedenen Schachstellenklassifikationen unter der Berücksichtigung der «Status» Spalte aus der Excel-Taskliste zu den jeweiligen generischen Risiko-Leveln. Diese generischen Risiko-Level sollen an die organisationsinternen Klassifikationen angenähert werden.

SCHWACHSTELLENKLASSIFIKATION	STATUS	RISIKO-LEVEL	BESCHREIBUNG
Hohe Schwachstelle	«Offen», «in Bearbeitung»	Hoch	Kritische Auswirkungen auf die Sicherheit oder Geschäftskontinuität.
Mittlere Schwachstelle	«Offen», «In Bearbeitung»	Mittel	Potenziell Schädliche Auswirkungen auf Sicherheit oder Geschäftskontinuität.
Geringe Schwachstelle	«Offen», «In Bearbeitung», «Wird nicht umgesetzt»	Gering	Geringfügige Schädliche Auswirkungen auf Sicherheit oder Geschäftskontinuität.
Information	«Nicht Zutreffend», «Erledigt»	Information	Information, welche keinerlei Auswirkungen auf die Sicherheit oder Geschäftskontinuität haben.

Tabelle 5 Übersicht über das Mapping der Schwachstellenklassifikationen zu den Risiko-Level

3.4 Abbildungsverzeichnis

3.5 Tabellenverzeichnis