SWISS INFOSEC

M365-Sicherheitscheckliste

Inhalt

Microsoft 365

30.06.2025, Version 1.0

1. Allgemeine Informationen

Die in diesem Dokument genannten Massnahmen sind nicht abschliessend, da neben technischen Aspekten auch organisatorische Gegebenheiten, Compliance-Vorgaben und vertragliche Regelungen berücksichtigt werden müssen. Wenn Sie jedoch die hier beschriebenen Punkte umsetzen, schaffen Sie eine solide Grundlage für den Basisschutz Ihrer Microsoft 365-Umgebung.

2. Organisatorische Massnahmen

Microsoft 365	**Berücksichtigung von CSPM (Cloud Security Posture Management) und Ressourcenplanung**
Rationale	Zur Sicherstellung einer durchgehend hohen Sicherheits- und Compliance-Posture in der Microsoft 365-Umgebung ist die kontinuierliche Überwachung und Pflege der Cloud Security Posture Management (CSPM)-Komponenten erforderlich.
Empfehlung	Die eingesetzten Tools, insbesondere Microsoft Secure Score, Microsoft Defender for Cloud und der Compliance Manager, sind regelmässig auszuwerten, damit erkannte Schwachstellen priorisiert und entsprechende Massnahmen zeitnah umgesetzt werden.
Config	N/A
Referenz	https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-cloud-security-posture-management

Microsoft 365	**Rollen und Berechtigungsvergabe**
Rationale	Globale Administratorrechte in Microsoft 365 stellen das höchste Berechtigungsniveau dar und müssen streng kontrolliert vergeben werden. Darüber hinaus ist auch der Umgang mit allen weiteren Administratorrollen sorgfältig zu gestalten, da jede administrative Rolle erweiterte Rechte über bestimmte Dienste oder Bereiche der Umgebung mit sich bringt. Eine unkontrollierte oder ungerechtfertigte Zuweisung solcher Rollen erhöht das Risiko von Fehlkonfigurationen, Datenverlust oder Sicherheitsvorfällen.
Empfehlung	Setzen Sie sich mit den standardmässig verfügbaren Entra ID-Rollen (z.B. User Administrator, Exchange Administrator oder Global Administrator) auseinander. Definieren Sie, welche Entra ID-Rollen in welchen Geschäftseinheiten benötigt werden (z.B. muss das Helpdesk Benutzer verwalten und erhält somit die User Administrator-Rolle). Die Anzahl der globalen Administratoren ist auf das notwendige Minimum zu begrenzen – Microsoft empfiehlt maximal zwei bis vier.
Config	N/A
Referenz	https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

Microsoft 365	**Sichere Vergabe und Überprüfung von Administratorrechten**
Rationale	Administratorgruppen, insbesondere mit globalen Rechten, stellen ein hohes Sicherheitsrisiko dar, wenn sie nicht regelmässig überprüft werden. Ohne Kontrolle können veraltete oder unberechtigte Zugriffe bestehen bleiben.
Empfehlung	Überprüfen Sie die verwendeten Administratorengruppen, insbesondere jene, die globale Administratoren enthalten, in regelmässigen Abständen. Rollenprüfungen sind regelmässig durchzuführen, idealerweise mithilfe von Access Reviews in Entra ID. Temporäre Rechtevergabe über Privileged Identity Management (PIM) mit Genehmigungsprozessen erhöht zusätzlich die Sicherheit. Administratoren müssen entsprechend geschult und für ihre Verantwortung sensibilisiert sein.
Config	N/A
Referenz	https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

Microsoft 365	**Gastzugriffe sicher verwalten**
Rationale	Externe Benutzer (Gäste) stellen ein potenzielles Sicherheits- und Compliance-Risiko dar, da sie ausserhalb der organisatorischen Kontrolle stehen. Ohne klare Richtlinien und regelmässige Überprüfung besteht die Gefahr von übermässigen oder veralteten Zugriffsrechten.
Empfehlung	Prüfen Sie, ob und in welchem Umfang externe Benutzer (Gäste) Zugriff auf Ihre Microsoft 365-Umgebung erhalten sollen. Definieren Sie klare Richtlinien für den Umgang mit Gastkonten, einschliesslich Zulassungsprozessen, Nutzungsbeschränkungen und Aufbewahrungsfristen. Gästeaccounts sollten regelmässig überprüft und bei Bedarf entfernt oder angepasst werden. Nutzen Sie dafür, falls lizenziert, Access Reviews aus Entra ID Governance. Diese ermöglichen es, Zugriffsrechte periodisch zu evaluieren und automatisiert Rückmeldungen von Verantwortlichen einzuholen. Vermeiden Sie dauerhaft privilegierte Rechte für Gäste und schränken Sie den Zugriff auf das Notwendige ein (Prinzip der minimalen Berechtigung). Verwenden Sie ggf. Conditional Access Policies (weitere Infos weiter unten), um Risiken weiter zu minimieren (z. B. Einschränkung auf bestimmte IP-Bereiche oder Geräteplattformen).
Config	N/A
Referenz	https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/manage-guest-access-in-groups?view=o365-worldwide https://learn.microsoft.com/en-us/entra/id-governance/create-access-review

Microsoft 365	**Security Monitoring**
Rationale	Die frühzeitige Erkennung von Angriffen in Microsoft 365 erfordert eine kontinuierliche und strukturierte Auswertung sicherheitsrelevanter Daten. Reports wie riskante Anmeldungen oder der Identity Security Score bieten wertvolle Einblicke in potenzielle Schwachstellen und Angriffsversuche.
Empfehlung	Microsoft stellt diverse Sicherheitsreports zur Verfügung, darunter riskante Anmeldungen und den Identity Secure Score. Diese sollten regelmässig und systematisch analysiert werden. Die Überwachung muss Tenant-weit erfolgen und Entra ID (z. B. Anmeldeprotokolle), Microsoft Defender und weitere sicherheitsrelevante Dienste einbeziehen. Sämtliche Aktivitäten privilegierter Konten sind zu protokollieren und regelmässig auszuwerten. Die Organisation sollte sicherstellen, dass ausreichende Ressourcen für die kontinuierliche Überprüfung und Anpassung dieser Massnahmen bereitstehen.
Config	N/A
Referenz	https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-investigate-risk https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-identity-secure-score

3. Technische Massnahmen

3.1 Microsoft Entra Admin Center

Empfehlung zur Verwaltung von Zugriffskontrollen
Zugriffssteuerungen und Zugriffsbedingungen, wie etwa Multi-Faktor-Authentifizierung (MFA), standortbasierte Einschränkungen (Geolocation), Gerätezustand oder risikobasierte Zugriffskriterien, sollten zentral über das Microsoft Entra Admin Center gesteuert und überwacht werden. Dies ermöglicht eine konsistente Umsetzung, eine bessere Nachvollziehbarkeit von Änderungen sowie eine lückenlose Protokollierung für Monitoring- und Compliance-Zwecke. Die Nutzung anderer Konfigurationspfade (Microsoft 365 bietet aufgrund des historischen Wachstums der Umgebung oftmals unterschiedliche Varianten, eine Konfiguration vorzunehmen) sollte vermieden werden, um Fragmentierung und Fehlkonfigurationen zu verhindern.

SWISS INFOSEC

	**Conditional Access**
Rationale	In modernen, cloudbasierten Umgebungen reicht die klassische Zugangskontrolle auf Basis von Benutzername und Passwort nicht mehr aus. Benutzer greifen zunehmend von verschiedenen Geräten, Netzwerken und Standorten auf Unternehmensressourcen zu – was die Angriffsfläche erheblich vergrössert. Conditional Access bietet die Möglichkeit, Zugriffe kontextbasiert zu steuern, etwa abhängig von Standort, Gerät, Benutzerrolle oder Anmelderisiko.
Empfehlung	Verwenden Sie Conditional Access Policies, um Zugriffe auf Ihre Microsoft 365-Umgebung gezielt zu steuern. Die folgenden Conditional Access Policies Templates von Microsoft sollten konfiguriert und wo möglich forciert werden: • **Multifaktorauthentifizierung (MFA)** Der Einsatz von Multifaktorauthentifizierung sollte für alle Benutzer als verpflichtende Vorgabe gelten. Dazu sollte die Anmeldehäufigkeit definiert und konfiguriert werden (z.B. täglich für Administratoren, wöchentlich für Standardbenutzer) • **Legacy-Authentifizierung** Blockiert unsichere Authentifizierungsprotokolle wie IMAP oder POP, die keine MFA unterstützen. • **Sichere Registrierung von Sicherheitsinformationen** Sichert den Registrierungsvorgang für Sicherheitsinformationen (z. B. Telefonnummern, Authenticator-App) durch Bedingungen wie MFA. • **Konformität der Geräte verlangen** Erlaubt nur Zugriff von Geräten, die den Unternehmensrichtlinien entsprechen (z. B. durch Intune verwaltet und compliant). • **Geolocations** Steuerung des Zugriffs basierend auf geografischen Standorten, z. B. Blockieren von Anmeldungen aus Hochrisikoregionen. • **Zugang zu Azure Admin-Portal** Beschränkt den Zugriff auf das Azure-Portal auf bestimmte Benutzergruppen, Standorte oder Geräte. • **Conditional Access Policy für Risky Sign-Ins und Risky User** Aktiviert MFA nur bei risikoreichen Anmeldungen, basierend auf Microsofts Risikoerkennung.
Config	Entra Admin Center ⇨ Protection ⇨Conditional Access ⇨ create new policy from templates ⇨*
Referenz	https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-policy-common?tabs=secure-foundation

	**Umgang mit privilegierten Accounts regeln**
Rationale	Administrative Aufgaben sollten niemals mit regulären Benutzerkonten durchgeführt werden. Stattdessen ist die Nutzung separater Administratorkonten erforderlich, die ausschliesslich für administrative Zwecke vorgesehen sind. Diese Konten dürfen keinen Zugriff auf benutzerspezifische Anwendungen wie E-Mail, Teams oder SharePoint erhalten, um das Risiko durch potenziell anfällige Dienste zu minimieren.
Empfehlung	Der Zugriff sollte strikt auf administrative Funktionen beschränkt sein. Als technische Massnahme empfiehlt sich der Einsatz von Privileged Identity Management (PIM), um Administratorrechte nur temporär, bei Bedarf und gegebenenfalls mit Genehmigung zu vergeben.
Config	N/A
Referenz	https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

	**Benutzerdefinierte gesperrte Passwörter aktivieren**
Rationale	Benutzer neigen dazu, schwache oder naheliegende Passwörter zu wählen – oft mit direktem Bezug zur Organisation. Durch die Kombination globaler und benutzerdefinierter Sperrlisten hilft Entra Password Protection, gängige und unternehmensspezifisch riskante Passwörter effektiv zu blockieren und so die Kontosicherheit nachhaltig zu erhöhen.
Empfehlung	Mit Microsoft Entra Password Protection (custom banned password list) wird standardmässig geprüft, ob Benutzer Passwörter verwenden möchten, die auf einer globalen Sperrliste stehen. Solche Passwörter werden für alle Benutzer eines Mandanten blockiert. Um geschäftliche und sicherheitsrelevante Anforderungen zu unterstützen, können zusätzlich benutzerdefinierte Listen gesperrter Passwörter erstellt werden. Beim Ändern oder Zurücksetzen eines Passworts wird geprüft, ob es sich auf einer dieser Listen befindet, um die Verwendung sicherer Passwörter durchzusetzen.
Config	Entra Admin Center ⇨ Protection ⇨ Authentication Methods ⇨ Password Protection
Referenz	https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-configure-custom-password-protection

	**Unternehmensbranding realisieren**
Rationale	Phishing-Angriffe zielen häufig darauf ab, Benutzer über gefälschte Anmeldeseiten zur Preisgabe ihrer Zugangsdaten zu verleiten. Ein individuell gestaltetes Unternehmens-Branding auf der Anmeldeseite stärkt die visuelle Wiedererkennung und reduziert die Wahrscheinlichkeit, dass Benutzer auf gefälschte Login-Seiten hereinfallen.
Empfehlung	Nutzen Sie das Unternehmens-Branding in Office 365, um die Standard-Anmeldeseiten mit eigenen Logos, Bildern und Farben individuell zu gestalten. Dadurch lässt sich die Verwechslungsgefahr mit einer häufig nachgeahmten Anmeldeseite deutlich verringern und das Risiko von Phishing-Angriffen reduzieren.
Config	Entra Admin Center ⇨ User experience ⇨ Company Branding
Referenz	https://learn.microsoft.com/en-us/microsoft-365/admin/setup/customize-sign-in-page?view=o365-worldwide

3.2 Microsoft Admin Center

	**Anmeldung für freigegebene Postfächer blockieren**
Rationale	Freigegebene Postfächer sind nicht für die direkte Anmeldung vorgesehen, sondern sollten ausschliesslich über delegierten Zugriff genutzt werden. Eine direkte Anmeldung stellt ein Sicherheitsrisiko dar, da diese Konten oft über systemgenerierte, nicht geänderte Passwörter verfügen und nicht durch Multifaktorauthentifizierung abgesichert sind. Das Blockieren der Anmeldung verhindert potenziellen Missbrauch und erhöht die Sicherheit der Umgebung.
Empfehlung	Freigegebene Postfächer werden genutzt, wenn mehrere Personen Zugriff auf dieselbe E-Mail-Adresse benötigen, z. B. für Support oder Empfang. Die zugehörigen Konten haben ein systemgeneriertes Passwort, das unbekannt ist. Empfohlen wird, die Anmeldung für freigegebene Postfächer zu blockieren.
Config	Microsoft Admin Center ⇨ Active Users ⇨ Filter for unlicensed ⇨ block sign in for shared mail-box
Referenz	https://learn.microsoft.com/en-us/microsoft-365/admin/email/about-shared-mailboxes?view=o365-worldwide

	**Password Policy**
Rationale	Eine klar definierte Passwortablaufregelung trägt zur Einhaltung interner Sicherheitsrichtlinien bei und hilft, die regelmässige Erneuerung schwacher oder kompromittierter Passwörter sicherzustellen.
Empfehlung	Ob und nach wie vielen Tagen ein Passwort abläuft, lässt sich einstellen. Es muss bewusst festgelegt werden, ob eine Passwortablauffrist aktiviert wird und diese sollte an die unternehmensinterne Passwortrichtlinie angepasst werden.
Config	Microsoft Admin Center ⇨ Settings ⇨ Org Settings ⇨ Security & Privacy ⇨ Password expiration policy
Referenz	https://learn.microsoft.com/en-us/microsoft-365/admin/manage/set-password-expiration-policy?view=o365-worldwide

3.3 Exchange Admin

	**Automatische Weiterleitung deaktivieren**
Rationale	Automatische E-Mail-Weiterleitungen stellen ein erhebliches Sicherheits- und Datenschutzrisiko dar, da vertrauliche Informationen unkontrolliert an externe Empfänger gelangen können. Angreifer nutzen diese Funktion häufig, um Daten unbemerkt aus dem Unternehmen zu exfiltrieren. Durch das gezielte Deaktivieren oder Einschränken automatischer Weiterleitungen kann dieses Risiko deutlich reduziert und die Kontrolle über den E-Mail-Verkehr verbessert werden.
Empfehlung	Exchange Online bietet verschiedene Möglichkeiten, den E-Mail-Verkehr zu steuern, darunter Remote Domains, Transportregeln und Anti-Spam-Richtlinien für ausgehende E-Mails. Damit lassen sich automatische Weiterleitungen über verschiedene Kanäle verhindern – etwa durch Posteingangsregeln, Abwesenheitsnotizen (Out of Office), Outlook im Web (Outlook Web App), Administrator-Weiterleitungen oder Power Automate Flows. Stellen Sie sicher, dass Transportregeln und Anti-Spam-Richtlinien gezielt eingesetzt werden, um unerwünschte Weiterleitungen zu unterbinden. Sollte die Weiterleitungsfunktion dennoch zwingend erforderlich sein, sollten zumindest Benachrichtigungen über derartige Vorgänge aktiviert werden.
Config	Exchange Admin Center ⇨ Mail Flow ⇨ Rules
Referenz	https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/manage-mail-flow-rules

3.4 Microsoft 365 Defender

	**Anti-Phishing-Richtlinie**
Rationale	Phishing zählt zu den häufigsten Einfallstoren für Sicherheitsvorfälle in Microsoft 365-Umgebungen. Die integrierten Schutzmechanismen bilden eine wichtige Grundlage, reichen jedoch oft nicht aus, um gezielte Angriffe wie Identitäts- oder Domain-Spoofing zuverlässig zu erkennen. Durch individuelle Anti-Phishing-Richtlinien kann der Schutz gezielt auf besonders gefährdete Benutzergruppen oder geschäftskritische Bereiche abgestimmt werden. So lässt sich das Risiko von erfolgreichen Angriffen deutlich reduzieren.
Empfehlung	Standardmässig enthält Office 365 integrierte Funktionen zum Schutz vor Phishing-Angriffen. Um diesen Schutz zu verbessern, sollten Anti-Phishing-Richtlinien eingerichtet werden, etwa durch gezielte Einstellungen zur Erkennung und Verhinderung von Identitäts- oder Spoofing-Angriffen. Die Standardrichtlinie gilt für alle Benutzer der Organisation und bietet eine zentrale Möglichkeit zur Feinabstimmung des Phishing-Schutzes. Zusätzlich können benutzerdefinierte Richtlinien für bestimmte Benutzer, Gruppen oder Domains erstellt werden, die dann Vorrang vor der Standardrichtlinie haben.
Config	Microsoft Defender ⇨ email & collaboration ⇨ Policies & rules ⇨ Threat policies ⇨ Anti-Phishing ⇨ create ⇨ add users for impersonation protection; select all recommended check-boxes
Referenz	https://learn.microsoft.com/en-us/defender-office-365/anti-phishing-policies-about

	**Malware-Erkennung im E-Mail-Verkehr - Benachrichtigungen aktivieren**
Rationale	Eine automatische Benachrichtigung bei erkannten Malware-Versendungen ermöglicht eine schnelle Reaktion auf potenzielle Sicherheitsvorfälle. So können infizierte Konten frühzeitig identifiziert, isoliert und weitere Schäden verhindert werden. Dies erhöht die Reaktionsgeschwindigkeit und unterstützt eine effektive Incident Response.
Empfehlung	Exchange Online Protection (EOP) ist der cloudbasierte Filterdienst zum Schutz vor Spam, Malware und anderen E-Mail-Bedrohungen und ist in allen Microsoft 365 Tenants mit Exchange Online enthalten. Stellen Sie sicher, dass EOP aktiviert ist und konfigurieren Sie angepasste Anti-Malware-Richtlinien, die verdächtige Aktivitäten erkennen und Administratoren automatisch benachrichtigen.
Config	Microsoft Defender ⇨ email & collaboration ⇨ Policies & rules ⇨ Threat policies ⇨Anti malware ⇨ default ⇨ edit protection settings ⇨ enable admin notifications
Referenz	https://learn.microsoft.com/en-us/defender-office-365/anti-malware-policies-configure

3.4 SharePoint Admin Center

	**Linkfreigabe in SharePoint und OneDrive einschränken**
Rationale	Diese Einstellung legt den Standard-Linktyp fest, den ein Benutzer beim Teilen von Inhalten in OneDrive oder SharePoint sieht. Andere Optionen werden dadurch nicht ausgeschlossen oder eingeschränkt.
Empfehlung	Empfohlen wird die Einstellung „Bestimmte Personen“ (nur die vom Benutzer angegebenen Empfänger)
Config	SharePoint Admin Center ⇨ Policies ⇨ Sharing
Referenz	https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off

	**Externes Teilen von Inhalten**
Rationale	Zentral gesteuerte Freigabeeinstellungen stellen sicher, dass externe Zugriffe auf Inhalte kontrolliert und nachvollziehbar bleiben. Die Vorgabe, dass einzelne SharePoint-Websites keine grosszügigeren Freigabeeinstellungen als die Organisation selbst haben dürfen, sorgt dafür, dass keine unbeabsichtigten Datenfreigaben nach aussen erfolgen. Die empfohlene Einstellung „Neue und vorhandene Gäste“ ermöglicht einen sicheren Austausch mit externen Partnern bei gleichzeitigem Identitätsnachweis.
Empfehlung	Die Freigabeeinstellungen für externes Teilen gelten für die gesamte Organisation. Einzelne SharePoint-Websites können eigene Einstellungen haben, dürfen dabei aber nicht offener sein als die Einstellungen der Organisation. Die empfohlene Einstellung ist „Neue und vorhandene Gäste“. Dabei müssen eingeladene Personen ihre Identität per Microsoft-Konto, Geschäfts-/Schulkonto oder Verifizierungscode bestätigen. Neue Gäste werden automatisch ins Entra-ID Verzeichnis aufgenommen.
Config	SharePoint Admin Center ⇨ Policies ⇨ Sharing
Referenz	https://learn.microsoft.com/en-us/sharepoint/external-sharing-overview