Anhang technische Details zu den Sicherheitsvorschriften KOM SG

Version 1.0

Gültig ab 1. Januar 2023

Das vorliegende Dokument verwendet für eine einfache flüssigere Lesbarkeit ausschliesslich die männliche Schreibform.

1. Einleitung ... 3
2. Links und technische Details ... 3
2.1. Schutz von Serversystemen ... 3
2.1.1. Einschränkung Netzwerkzugriffe ... 3
2.2. Schutz von Clientsystemen ... 3
2.2.1. Einschränkung Netzwerkzugriffe ... 3
2.2.2. Einschränkungen Office Makros ... 4
2.3. Active Directory Hardening ... 4
2.3.1. Anmeldebeschränkungen für Domain Admins ... 4
2.3.2. Erfordern von Signaturchecks ... 5
2.3.3. Deaktivieren von veralteten Features ... 6
2.3.4. Löschen von GPP Files mit Passwörtern ... 6
2.3.5. Aktivierug von Credential Guard ... 7
2.3.6. Einschränkung zur Erstellung von neuen Computeraccounts ... 7
2.4. Schutz in der M365/Azure Cloud ... 8
2.4.1. Sicherung der Authentisierung mittels Security Defaults ... 8
2.4.2. Sicherung der Authentisierung mittels Conditional Access policy ... 8
2.4.3. Endpoint Sicherheit mittels Intune ... 8
2.4.4. Mail Routing – Sicherheit im E-Mail Verkehr ... 8
2.4.5. Allgemeine Vorkehrungen ... 8
3. Checklisten ... 10
3.1. Checkliste Schutz von Serversystemen ... 10
3.2. Checkliste Schutz von Clients ... 10
3.3. Checkliste Active Directory Hardening ... 11
3.4. Checkliste Schutz des Netzwerks ... 12
3.5. Checkliste M365/Azure Cloud ... 14
3.6. Checkliste Schutz im E-Mail Verkehr ... 14

1. Einleitung

Dieser Anhang enthält technische Details zur Erfüllung der Anforderungen aus den Sicherheitsvorschriften. Der Inhalt des Anhangs wird regelmässig aktualisiert.

2. Links und technische Details

2.1. Schutz von Serversystemen

In folgendem Kapitel sind die benötigten Sicherheitsvorkehrungen für Serversysteme definiert, welche im Netzwerk des Partners betrieben werden.

2.1.1. Einschränkung Netzwerkzugriffe

Serversysteme innerhalb der Domäne sollen nur von bestimmten Endpunkten administriert werden können. Zugriffe auf Services, welche eine Remote-Administration ermöglichen, sind auf benötigte Netzwerke oder IP-Adressen eingeschränkt. Zu diesen Services gehören folgende:

- **RDP – Remote Desktop Protocol**
  Ports/Protokoll: 3389/TCP&UDP
- **PowerShell Remoting / WinRM**
  Ports/Protokoll: 5985, 5986/TCP
- **SSH – Secure Shell**
  Ports/Protokoll: 22/TCP
- **Telnet**
  Ports/Protokoll: 23/TCP
- **RPC/WMI (Remote Registry etc.)**
  Ports/Protokoll: 135/TCP
- **SMB**
  Ports/Protokoll: 445,139/TCP
- **HTTP/S***
  Ports/Protokoll: 80,443,8080,8443/TCP
- **SNMP**
  Ports/Protokoll: 161/UDP

Administrationsinterfaces jeglicher Art von unterschiedlicher Software wird teilweise auf nicht standard-Ports betrieben, welche hier nicht alle aufgelistet werden konnten. Grundsätzlich muss der Zugriff auf sämtliche Administrationsinterfaces eingeschränkt werden.
Nur die notwendigen Ports werden freigeschaltet, wenn beispielsweise ein Fileserver betrieben wird, kann SMB geöffnet bleiben.

2.2. Schutz von Clientsystemen

In folgendem Kapitel sind die benötigten Sicherheitsvorkehrungen für Clientsysteme definiert, welche im Netzwerk des Partners betrieben werden.

2.2.1. Einschränkung Netzwerkzugriffe

Grundsätzlich benötigen Clients in einer Windows Domäne keine offenen Ports. Eine Anmeldung am Domänencontroller, das Abholen von Gruppenrichtlinien etc. benötigt jeweils

nur offene Ports auf der Serverseite. Die Clients sollen daher möglichst alle eingehenden Verbindungen blockieren (Host-Firewall).
Mindestens gilt es folgende eingehenden Ports zu blockieren resp. einzuschränken (zugelassen nur von Administratoren):

- **RDP – Remote Desktop Protocol**
  Ports/Protokoll: 3389/TCP&UDP
- **SMB – Server Message Block**
  Ports/Protokoll: 445/TCP
- **NBT – NetBIOS over TCP**
  Ports/Protokoll: 137,138,139/TCP&UDP
- **RPC/DCOM/WMI - Remote Procedure Call**
  Ports/Protokoll: 135,593/TCP&UDP
- **PowerShell Remoting (Standardmässig deaktiviert auf Clients)**
  Ports/Protokoll: 5985, 5986/TCP

Administrationsinterfaces jeglicher Art von unterschiedlicher Software wird teilweise auf nicht standard-Ports betrieben, welche hier nicht alle aufgelistet werden konnten. Grundsätzlich muss der Zugriff auf sämtliche Administrationsinterfaces eingeschränkt werden.

2.2.2. Einschränkungen Office Makros

Zusatzinformationen zur Einschränkung der Office Makros:

Pfad in den Gruppenrichtlinen:
User configuration > Policies > Administrative templates > OFFICE_PROGRAMM > OFFICE_PROGRAMM options > Security > Trust Center.

Falls Windows Defender im Einsatz ist, empfiehlt es sich zusätzlich folgende ASR[1] Regeln zu aktivieren:

- https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide#block-all-office-applications-from-creating-child-processes
- https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide#block-office-applications-from-creating-executable-content
- https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide#block-office-applications-from-injecting-code-into-other-processes

2.3. Active Directory Hardening

In folgendem Kapitel sind Konfigurationen für die Härtung von Active Directory definiert. Active Directory kann durch viele Einstellungen gehärtet werden, in diesem Kapitel werden die wichtigsten festgehalten, selbstverständlich kann immer noch mehr gemacht werden.

2.3.1. Anmeldebeschränkungen für Domain Admins

Der verlinkte Microsoft Artikel beschreibt die notwendigen Schritte für die Konfiguration. Unterhalb ist das Vorgehen kurz zusammengefasst.
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-f--securing-domain-admins-groups-in-active-directory

[1] https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide

Eine GPO (oder mehrere einzelne) welche zu den OUs von Member Server und Clients verlinkt ist, soll unter folgendem Pfad mit den entsprechenden Eigenschaften konfiguriert werden, um das Login von Domain Admins dort zu verhindern. Als Zielgruppe/User ist jeweils die Gruppe der Domänen Administratoren zu wählen.

Pfad in den Gruppenrichtlinien: Computer Configuration > Windows Settings > Security Options > Local Policies > User Rights Assignments
Zu definierende Eigenschaften: - Deny access to this computer from the network - Deny log on as a batch job - Deny log on as a service - Deny log on locally - Deny log on through Remote Desktop Services user rights

2.3.2. Erfordern von Signaturchecks

Durch die fehlenden Signaturchecks für SMB und LDAP gelingt es Angreifern im lokalen Netzwerk gewisse Angriffe durchzuführen bei welchen Anmeldeinformationen zu beliebigen Systemen umgeleitet werden können.
Mehr Informationen zu den möglichen Angriffsszenarien ohne diese Sicherheitsvorkehrungen:

- SMB Signing: https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing
- LDAP Signing: https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/enable-ldap-signing-in-windows-server

2.3.2.1. SMB Signing

SMB-Signing[2] soll für sämtliche Systeme in der Domäne erfordert werden. Der Domänencontroller hat SMB-Signing standardmässig aktiviert. Die Konfiguration erfolgt mittels Gruppenrichtline.

Pfad für Server: *Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > Microsoft network server: Digitally sign communications (always)*
Pfad für Clients: *Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > Microsoft network client: Digitally sign communications (always)*

2.3.2.2. LDAP Signing

LDAP-Signing[3] soll für alle Systeme in der Domäne konfiguriert werden. Die Konfiguration erfolgt mittels Gruppenrichtlinie.

Pfad für Server: *Default Domain Controller Policy > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > Domain controller: LDAP server signing requirements*
Pfad für Clients: *Default Domain Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Network security: LDAP client signing requirements*

[2] https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing
[3] https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/enable-ldap-signing-in-windows-server

2.3.3. Deaktivieren von veralteten Features

Veraltete Features stellen Sicherheitsrisiken dar und sollen deaktiviert werden.

2.3.3.1. NT LAN Manager Version 1 (NTLMv1)

In gewissen Sonderfällen kann es sein, dass alte Komponenten lediglich NTLMv1 unterstützen. Die Nutzung des Protokolls sollte daher vor einer Umstellung auf deren Nutzen in der Domäne geprüft werden:
https://docs.microsoft.com/de-de/archive/blogs/miriamxyra/stop-using-lan-manager-and-ntlmv1#why-you-should-not-use-ntlmv1-anymoret

Pfad in den Gruppenrichtlinien:
Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Network security: LAN Manager authentication level

Der Wert sollte schlussendlich auf 5 gestellt werden, zunächst kann wie in der Dokumentation beschrieben mit tieferen Werten begonnen werden, um die Nutzung von NTLMv1 zu prüfen.

2.3.3.2. Link-Local Multicast name Resolution (LLMNR) deaktivieren

LLMNR kann via Gruppenrichtlinien deaktiviert werden.

Pfad in den Gruppenrichtlinien:
Computer Configuration > Administrative Templates > Network > DNS Client > Turn Off Multicast Name Resolution

Die Policy muss auf ‘Enabled‘ gesetzt werden.

2.3.3.3. NetBIOS-NS (NBT-NS) deaktivieren

Das Protokoll lässt sich leider nicht mittels Gruppenrichtlinien deaktivieren, sondern muss auf einer per-Host Basis deaktiviert werden.

Eine Alternative stellt die Deaktivierung mittels DHCP Optionen dar (https://docs.microsoft.com/en-US/troubleshoot/windows-server/networking/disable-netbios-tcp-ip-using-dhcp). Im Normalfall ist die Konfiguration via PowerShell jedoch einfacher, da dies relativ einfach automatisiert auf allen Hosts durchgeführt werden kann (z.B. mittels PowerShell Remoting)

Folgendes Powershell Query deaktiviert NBT-NS auf sämtlichen Interfaces des aktuellen Computers, dafür sind administrative Rechte notwendig.

```
$key = "HKLM:SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces"
Get-ChildItem $key |foreach { Set-ItemProperty -Path "$key\$($_.pschildname)" -Name
NetbiosOptions -Value 2}
```

2.3.4. Löschen von GPP Files mit Passwörtern

Group Policy Preference, ein Feature, welches mit Server 2008 eingeführt wurde, erlaubte es Administratoren Zugangsdaten für verschiedene Tasks auf den Clients der Domäne zu nutzen. Passwörter von privilegierten Accounts konnten in den Gruppenrichtlinien (GPO) hinterlegt werden, um verschiedenste Aufgaben durchzuführen.
Die hinterlegten Passwörter sind mit AES verschlüsselt, Microsoft hat den dabei verwendeten Key jedoch in der Dokumentation veröffentlicht:
https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-gppref/2c15cbf0- f086-4c74-8b70-1f2fa45dd4be?redirectedfrom=MSDN

Da Microsoft den Key veröffentlicht hat, können sämtliche Domain User die Passwörter entschlüsseln, welche in den betroffenen Files gespeichert wurden (Sämtliche Nutzer haben Zugriff auf den SYSVOL Share, wo GPO Konfigurationen abgelegt werden).
Mittlerweile wurde das Feature entfernt, resp. die Möglichkeit Passwörter zu hinterlegen wurde deaktiviert. GPP Konfigurationen, welche zuvor erstellt wurden, wurden dabei aber nicht automatisch entfernt. Daher ist es wichtig zu prüfen ob solche Files vorhanden sind und diese zu entfernen, falls vorhanden.

Mit folgendem Befehl (cmd.exe) kann nach Files mit diesen Passwörtern gesucht werden. Die '<FQDN>' Platzhalter müssen dabei mit dem Namen der Domäne ersetzt werden.

```
findstr /S /I cpassword \\<FQDN>\sysvol\<FQDN>\policies\*.xml
```

Innerhalb der Gruppenrichtlinien (Group Policy Management Editor) sind die GPP Konfigurationen unter folgendem Pfad zu finden:

User/Computer Configuration > Preferences

2.3.5. Aktivierug von Credential Guard

Für Credential Guard gibt es einige Voraussetzungen. Prüfen Sie, ob diese erfüllt, sind mit einigen Testclients, bevor das Setting global ausgerollt wird: https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-requirements
Aktivierung von Credential Guard: https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage#enable-windows-defender-credential-guard

Pfad in den Gruppenrichtlinien:
Computer Configuration **>** Administrative Templates **>** System **>** Device Guard **>** Turn On Virtualization Based Security

Die Policy muss auf 'Enabled' gesetzt werden.

2.3.6. Einschränkung zur Erstellung von neuen Computeraccounts

Es sollte sichergestellt werden, dass nur spezifische Accounts neue Geräte hinzufügen können, resp. neue Computeraccounts anlegen können. Dazu muss das Attribut 'ms-DS-MachineAccountQuota'[4] angepasst werden.
Für die Anpassung des Attributes kann das ADSI Edit Tool verwendet werden, eine entsprechende Guideline ist unter folgendem Link einsehbar: https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/default-workstation-numbers-join-domain

Alternativ kann die Einschränkung auch mittels Gruppenrichtline erfolgen:

Pfad in den Gruppenrichtlinien:
Computer Configuration **>** Windows Settings **>** Security Settings **>** Local Policies **>** User Rights Assignment **>** Add Workstations to domain

Die GPO muss zum Domänencontroller verlinkt werden.

[4] https://docs.microsoft.com/en-us/windows/win32/adschema/a-ms-ds-machineaccountquota

2.4. Schutz in der M365/Azure Cloud

Hier werden Details zu den benötigten Konfigurationen festgehalten.

2.4.1. Sicherung der Authentisierung mittels Security Defaults

Die Security Defaults lassen sich unter folgendem Link aktivieren:
https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Properties
Dokumentation von Microsoft betreffend Security Defaults:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

2.4.2. Sicherung der Authentisierung mittels Conditional Access policy

Der Partner sollte Conditional Access nur dann einsetzen, wenn entsprechendes Know-How bezüglich AAD resp. Conditional Access besteht.
Informationen zu Conditional Access:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview
Conditional Access kann unter folgendem Link konfiguriert werden:
https://portal.azure.com/#blade/Microsoft_AAD_IAM/ConditionalAccessBlade/Policies

2.4.3. Endpoint Sicherheit mittels Intune

Für die meisten Konfigurationen reichen die ‘Compliance Policies‘ aus. Diese können unter folgendem Pfad erstellt und konfiguriert werden:
https://endpoint.microsoft.com/#blade/Microsoft_Intune_DeviceSettings/DevicesComplianceMenu/policies
Für spezifischere Konfigurationen, beispielsweise dem Definieren und Verteilen von Firewall-Regeln für die Windows-Firewall, müssen ‘Configuration Profiles‘ angelegt werden. Diese können unter folgendem Pfad gefunden werden:
https://endpoint.microsoft.com/#blade/Microsoft_Intune_DeviceSettings/DevicesMenu/configurationProfiles

2.4.4. Mail Routing – Sicherheit im E-Mail Verkehr

Microsoft bietet für M365 folgende Dienste an, welche Prüfungen von Attachments und Links innerhalb empfangener E-Mails/Anhänge durch eine Sandbox ermöglichen und den Anforderungen entsprechen.

- Safe Attachments: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments
- Safe Links: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links?view=o365-worldwide

Um diese Features nutzen zu können, wird der “Microsoft Defender for Office 365 Plan 1“ benötigt, dieser ist beispielsweise im Abonnement “Microsoft 365 Business Premium“ inkludiert.

2.4.5. Allgemeine Vorkehrungen

2.4.5.1. Consent Grant

Die Möglichkeit zur Zustimmung zu Apps kann unter folgendem Link konfiguriert werden:
https://portal.azure.com/#blade/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/UserSettings
Die Einstellung sollte bestenfalls auf ‘Do not allow user consent’ gestellt werden, sodass Benutzer keinen Drittapplikationen Zugriff auf Unternehmensdaten gewähren können.

Mindestens muss die Einstellung auf ‘Allow user consent for apps from verified publishers, for selected permissions’ gestellt werden.

2.4.5.2. Notfall Account (Break-Glass Account)
Die Dokumentation von Microsoft zu solchen Accounts kann unter folgendem Link eingesehen werden:
https://docs.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access

3. Checklisten

In diesem Abschnitt sind die Checklisten für die einzelnen Bereiche aufgelistet.

3.1. Checkliste Schutz von Serversystemen

Prüfpunkt	Pflicht / Empfehlung	Umgesetzt (Ja/Nein)
Ports, welche eine Administrierung erlauben, sind entsprechend eingeschränkt.	Pflicht	
Zugriffe auf Server erfolgen stets mit personalisierten Accounts.	Pflicht	
Updates welche Sicherheitslücken ab einem CVSSv3 Score[5] von 5.0 beheben, werden innerhalb von 30 Tagen installiert.	Pflicht	
Systeme und Applikationen in der DMZ, werden bei kritischen Schwachstellen innerhalb von 14 Tagen aktualisiert.	Pflicht	
Sämtliche Server verfügen über einen aktuellen Virenschutz oder eine EDR/XDR Lösung.	Pflicht	
Der eingesetzte Virenschutz wird zentral veraltet, eine Alarmierung für Administratoren besteht.	Pflicht	
Auf den Server sind nur die für den Betrieb notwendige Software installiert.	Pflicht	

3.2. Checkliste Schutz von Clients

Prüfpunkte – Schutz von Clients	Pflicht / Empfehlung	Umgesetzt (Ja/Nein)
Benutzer haben keine lokalen Admin-Rechte auf den Clients oder virtualisierten Umgebungen (z.B. VDI).	Pflicht	
Ports, welche eine Administrierung erlauben sind eingeschränkt.	Empfehlung	
Updates welche Sicherheitslücken ab einem CVSSv3 Score von 5.0 beheben, werden innerhalb von 30 Tagen installiert.	Pflicht	
Sämtliche Clients verfügen über einen aktuellen Virenschutz.	Pflicht	
Der eingesetzte Virenschutz wird zentral veraltet. Eine Alarmierung für Administratoren besteht.	Pflicht	
Office Makros werden via Gruppenrichtlinien eingeschränkt.	Pflicht	
Die Festplatten von mobilen Clients sind komplett verschlüsselt.	Pflicht	
Die Festplatten von Desktop Clients sind komplett verschlüsselt.	Empfehlung	

[5] https://nvd.nist.gov/vuln-metrics/cvss

Der Sperrbildschirm wurde mittels Gruppenrichtlinien nach maximal 15 Minuten konfiguriert.	Pflicht	
Der Datenspeicher geschäftlicher Smartphones ist verschlüsselt.	Pflicht	
Geschäftliche Smartphones werden durch PIN, Passwort oder biometrische Wege gesichert.	Pflicht	
Die Möglichkeit für ein Remote-Wipe bei geschäftlich genutzten Smartphones besteht.	Pflicht	
Mitarbeitende sind angewiesen Sicherheitsupdates auf Ihren geschäftlichen Smartphones mindestens alle 60 Tage installiert.	Pflicht	

3.3. Checkliste Active Directory Hardening

Prüfpunkt	Pflicht / Empfehlung	Umgesetzt (Ja/Nein)
Anmeldebeschränkungen für Domain Admins durchgeführt	Empfehlung	
Domain Admins in ‘Protected Users’ Gruppe aufgenommen	Empfehlung	
Keine SPNs für Domain Admins registriert	Empfehlung	
Die Passwörter für lokale Administratoren auf sämtlichen Systemen in der Domäne sind einzigartig (LAPS kann dafür genutzt werden)	Empfehlung	
Passwortrichtlinen für Benutzeraccounts sind umgesetzt • Mindestens 12 Stellen lang • Erneuerung nach 365 Tage • Komplexität aktiviert • Sperrung des Accounts nach 10-maliger Fehleingabe • Letzte 10 Passwörter dürfen nicht wiederverwendet werden • Passwortalter mindestens 1 Tag	Pflicht	
SMB- und LDAP-Signing wurden konfiguriert	Empfehlung	
NTLMv1 wurde deaktiviert	Pflicht	
LLMNR wurde deaktiviert	Empfehlung	
NBT-NS wurde deaktiviert	Empfehlung	
Es existieren keine GPP Files mit Passwörtern	Pflicht	
Credential Guard ist aktiviert	Empfehlung	
Das Hinzufügen von Computeraccounts wurde auf bestimmte Gruppen/User limitiert	Pflicht	

3.4. Checkliste Schutz des Netzwerks

Prüfpunkt	Pflicht / Empfehlung	Umgesetzt (Ja/Nein)
Der Netzwerk-Zugriff auf Administrationsinterfaces von Netzkomponenten, IoT etc. wurde eingeschränkt.	Pflicht	
Es werden keine Standardpasswörter für Netzkomponenten, IoT etc. verwendet.	Pflicht	
Es werden keine Protokolle genutzt, welche Zugangsdaten im Klartext übermitteln (z.B. Telnet).	Pflicht	
Sicherheitsupdates werden nach 60 Tagen installiert. Für Systeme welche aus Fremdnetzen erreichbar sind, nach 30 Tagen. Kritische Lücken werden nach 14 Tagen geschlossen.	Pflicht	
Zusätzlich angebotene Sicherheitsfeatures der Komponenten wurden aktiviert.	Empfehlung	
Die VLAN Konfiguration erfüllt die Vorgaben gemäss Kapitel 5.1.4.	Pflicht	
Es wird für sämtliche Netzwerkanschlüsse ein NAC verwendet.	Empfehlung	
Es wird für alle öffentlich zugängliche Netzwerkanschlüsse ein NAC eingesetzt (MAC-Filter oder 802.1x).	Pflicht	
Eine aktuelle Dokumentation (z.B. Netzplan) der genutzten Komponenten existiert.	Pflicht	
Das Interne Netzwerk ist von Fremdnetzen ausreichend getrennt.	Pflicht	
Systeme, welche aus dem Internet erreichbar sind, werden in einer DMZ betrieben.	Pflicht	
Webapplikationen, welche aus dem Internet erreichbar sind und im Netzwerk des Partners betrieben werden, werden mit einer WAF geschützt.	Empfehlung	
Für den Zugriff auf interne Daten aus dem Internet wird eine starke Authentisierung genutzt (2-Faktor).	Pflicht	
Von Fremdnetzen werden keine Verbindungen zum KOMSG ermöglicht.	Pflicht	
Verbindungen vom internen Netzwerk zum KOMSG sind eingeschränkt, wenn Verbindungen mit einem Fremdnetz bestehen.	Pflicht	
Enduser müssen einen Zugriff für den Remote-Support aktiv bestätigen.	Pflicht	
Für Remote-Support via Internet wird eine starke Authentisierung (2-Faktor) genutzt.	Pflicht	
Für die Fernwartung via Internet wird eine starke Authentisierung (2-Faktor) verwendet.	Pflicht	

Zugriffe für die Fernwartung werden protokolliert und erfolgen stets mit personifizierten Accounts.	Pflicht	
Die Authentisierung zum internen WLAN erfolgt mittels starker Authentisierung (2-Faktor).	Pflicht	
Das Gäste WLAN hat keinerlei Zugriffsmöglichkeiten zum internen Netzwerk oder KOMSG.	Pflicht	
Die Vorgaben an VPN Verbindungen werden gemäss Kapitel 5.5 eingehalten.	Pflicht	
Die eingesetzte VoIP Variante erfüllt die entsprechenden Vorgaben gemäss Kapitel 5.6 aus den Sicherheitsvorschriften.	Pflicht	

3.5. Checkliste M365/Azure Cloud

Prüfpunkt	Pflicht / Empfehlung	Umgesetzt (Ja/Nein)
Sämtliche User sind für eine 2-Faktor Authentisierung registriert.	Pflicht	
Legacy Authentisierungsprotokolle sind deaktiviert.	Pflicht	
Benutzer mit Administrationsrechten werden bei jedem Login zu einer Authentisierung mittels 2-Faktor gezwungen.	Pflicht	
Wenn Bedarf besteht, (z.B. Login aus einer unbekannten Lokation) werden sämtliche User beim Login zu einer Authentisierung mittels 2-Faktor gezwungen.	Pflicht	
Eingehende Mails werden entweder via Abraxas geroutet, durch die Features «Safe-Links» und «Safe-Attachments» geschützt oder es wird eine andere Sandbox-Lösung gemäss Kapitel 7.3 aus den Sicherheitsvorschriften eingesetzt.	Pflicht	
Die Möglichkeiten für Benutzer, Apps Berechtigungen zu erteilen, wurde mindestens auf die Option ‘Allow user consent for apps from verified publishers, for selected permissions’ gestellt.	Pflicht	
Es wurde mindestens 1 Notfall Account erstellt.	Empfehlung	

3.6. Checkliste Schutz im E-Mail Verkehr

Prüfpunkt	Pflicht / Empfehlung	Umgesetzt (Ja/Nein)
Die Anzahl Empfänger im Emailverkehr wurde auf 200 Empfänger beschränkt.	Pflicht	
Die Grösse von Attachments im Emailverkehr wurde auf 20 MB eingeschränkt.	Pflicht	
Die automatische Weiterleitung an private Emailadressen wurde technisch unterbunden.	Pflicht	
Falls eine eigene Sandboxlösung eingesetzt wird, erfüllt diese sämtliche Anforderungen aus dem Kapitel 7.3 der Sicherheitsvorschriften.	Pflicht	
Mittels Transport-Rules wurde das Empfangen von Emails mit der Domäne des Partners von extern eingeschränkt (Schutz vor Spoofing)	Empfehlung	
Externe Mailadressen im globalen Adressbuch des KOMSG-Verbundes, sind mit „EXT“ gekennzeichnet.	Pflicht	