Sicherheitsvorschriften KOM SG

Version 7.0

Gültig ab 1. Januar 2023

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

Inhaltsverzeichnis

1 Einleitung

1.1 Ziel und Zweck

Die Interessengemeinschaft Kommunikationsnetz Kanton St. Gallen (KOM SG) unterhält eine Kommunikationsinfrastruktur, die alle Verwaltungsstellen von Gemeinden und Kanton verbindet und den elektronischen Informationsaustausch zwischen diesen gewährleistet. Dieses Verwaltungsnetzwerk wird im vorliegenden Dokument als KOMSG bezeichnet. Über das KOMSG erfolgen der Zugriff auf zentrale Daten sowie der Zugang zu externen Diensten wie beispielsweise dem Internet.
Diese Sicherheitsvorschriften beschreiben die notwendigen Rahmenbedingungen im Umgang mit den Dienstleistungen der KOM SG, um innerhalb des KOMSG ein sicheres Umfeld gewährleisten zu können und basieren teilweise auf dem SIK-Standard Dokument NSP-SIK-2017.

1.2 Anhang mit technischen Details und Checklisten

Technische Details und hilfreiche Links zu Herstellerdokumentationen bezüglich geforderter Konfigurationen sind jeweils dem Anhang zu entnehmen. Wenn für einen Punkt zusätzliche Informationen im Anhang existieren, ist dies jeweils vermerkt.

Im Anhang sind zudem Checklisten vorhanden, um möglichst einfach die in diesem Dokument geforderten Vorschriften zu prüfen. Darüber hinaus ist dort vermerkt, ob eine Vorgabe zwingend umzusetzen ist oder eine Empfehlung darstellt.

1.3 Geltungsbereich / Zielpublikum

Die vorliegenden Sicherheitsvorschriften definieren die Mindestanforderungen im Umgang mit den Diensten der KOM SG. Sie stützen sich auf die Rahmenbedingungen der Allgemeinen Geschäftsbedingungen für die Nutzung der Netzdienste der KOM SG.
Der Geltungsbereich für die vorliegenden Sicherheitsvorschriften umfasst sämtliche angeschlossenen Institutionen innerhalb des KOMSG-Verbundes, nachfolgend Partner genannt. Alle Vorgaben gelten aber auch für Dienstanbieter und Netzbetreiber, die Übergänge ins KOMSG betreuen.
Sind bei den angeschlossenen Institutionen eigene Sicherheitsvorschriften vorhanden, gelten diese ergänzend zu den Sicherheitsvorschriften der KOM SG. Die Sicherheitsvorschriften der KOM SG gelten dabei als Mindestanforderungen und müssen zwingend eingehalten werden.
Die vorliegenden Sicherheitsvorschriften richten sich an Informatikverantwortliche des Partners sowie deren IT-Leistungserbringer.

1.4 Betroffene Systeme

Die vorliegenden Sicherheitsvorschriften gelten für alle Systeme, die mit den internen Netzen des Partners verbunden werden. Systeme in Fremdnetzen (siehe Kapitel 5.2) sind von den Sicherheitsvorschriften ausgenommen.

1.5 Organisatorisches Umfeld

1.5.1 KOM SG

Die KOM SG vergibt den Auftrag für den operativen Betrieb des KOMSG und steuert diesen. Im Weiteren beschafft sie die Dienste des KOMSG-Netzes und stellt diese ihren Partnern zur Verfügung. Neben der Funktionalität des KOMSG und der KOMSG-Dienste ist sie auch für die Qualität und Sicherheit dieser verantwortlich. Um die Sicherheit des KOMSG und der

KOMSG-Dienste zu gewährleisten, überbindet sie die vorliegenden Sicherheitsvorschriften ihren Partnern, Dienstanbietern und Netzbetreibern.

1.6 Dienstanbieter und Netzbetreiber

Von der KOM SG beauftragte Dienstanbieter und Netzbetreiber stellen ihrerseits eine ausreichende sowie korrekte Umsetzung von Sicherheitsmassnahmen, inklusive der hier formulierten Anforderungen, sicher.

1.6.1 **Partner**

Der Partner ist der Vertragspartner der KOM SG. In dieser Eigenschaft akzeptiert er die vorliegenden Sicherheitsvorschriften und garantiert deren korrekten Umsetzung gegenüber der KOM SG.

1.7 Bewilligungen

Das Anbieten von eigenen Diensten des Partners über die Netzwerk-Infrastruktur der KOM SG[1] sowie Kommunikationsverbindungen von Partner-Netzen zu Stellen ausserhalb des KOMSG[2] (externe Verbindungen) verlangen eine Bewilligung. Diese wird von der Geschäftsstelle der KOM SG schriftlich erteilt, sofern die in den Allgemeinen Geschäftsbedingungen, Absatz C. 3 Netzwerksicherheit aufgeführten Bedingungen erfüllt und überprüft sind.

1.8 Ausnahmebewilligungen

Auf Antrag des Partners entscheidet die Geschäftsstelle der KOM SG über Ausnahmebewilligungen zu diesen Sicherheitsvorschriften. Im Eskalationsfall entscheidet der Vorstand der KOM SG. Für Partner, die Zertifizierungen (z. B. ISO 27001) nachweisen können, die über die vorliegenden Sicherheitsvorschriften hinausgehen, kann ein vereinfachtes Bewilligungsverfahren zur Anwendung kommen.
Die Ausnahmebewilligungen schwächen das Sicherheitsdispositiv und werden daher mit einer Risikobewertung versehen. Die Geschäftsstelle der KOM SG führt eine gesamthafte Übersicht der Ausnahmebewilligungen[3]. Diese wird für alle KOM SG-Partner publik gemacht (Vertrauen durch Transparenz).

1.9 Koordination

Sämtliche Kommunikation über die in diesen Sicherheitsvorschriften beschriebenen Bereiche und die Klärung allfälliger Unklarheiten wird über die Geschäftsstelle der KOM SG geführt (info.igkomsg@sg.ch oder Tel. 058 229 41 30).

1.10 Bedingungen zum Anschluss an das KOMSG

Beim Anschluss an das KOMSG wird zwischen zwei Partnern unterschieden.

- **Partner I**
  Organisationseinheiten oder Kunden, die im KOMSG als eigenständige Zone geführt werden, keine Übergänge zu Fremdnetzen betreiben und interne Systeme im KOMSG erreichen müssen, werden als Partner I bezeichnet

[1] z.B. Internet-Zugang für andere KOM SG Partner
[2] Z.B. für die Videoüberwachung oder Leitsysteme
[3] https://intranet.sg.ch/informatik/geschaeftsstellen/komsg/Seiten/Antrag_Ausnahmebewilligung.aspx

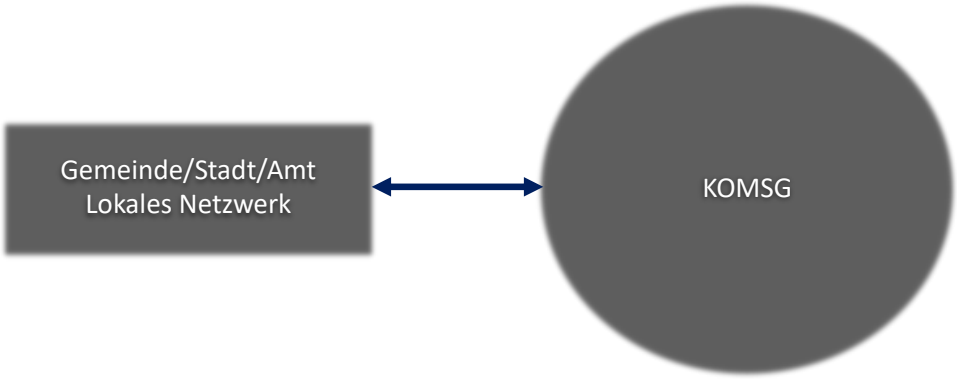

Abbildung 1 - Partner I

- **Partner II**
  Organisationseinheiten oder Kunden, die im KOMSG als eigenständige Zone geführt werden, eigene externe Übergänge betreiben und interne Systeme im KOMSG erreichen müssen, werden als Partner II bezeichnet. Deren Integration erfolgt ausschliesslich über eine DMZ im Perimeter.

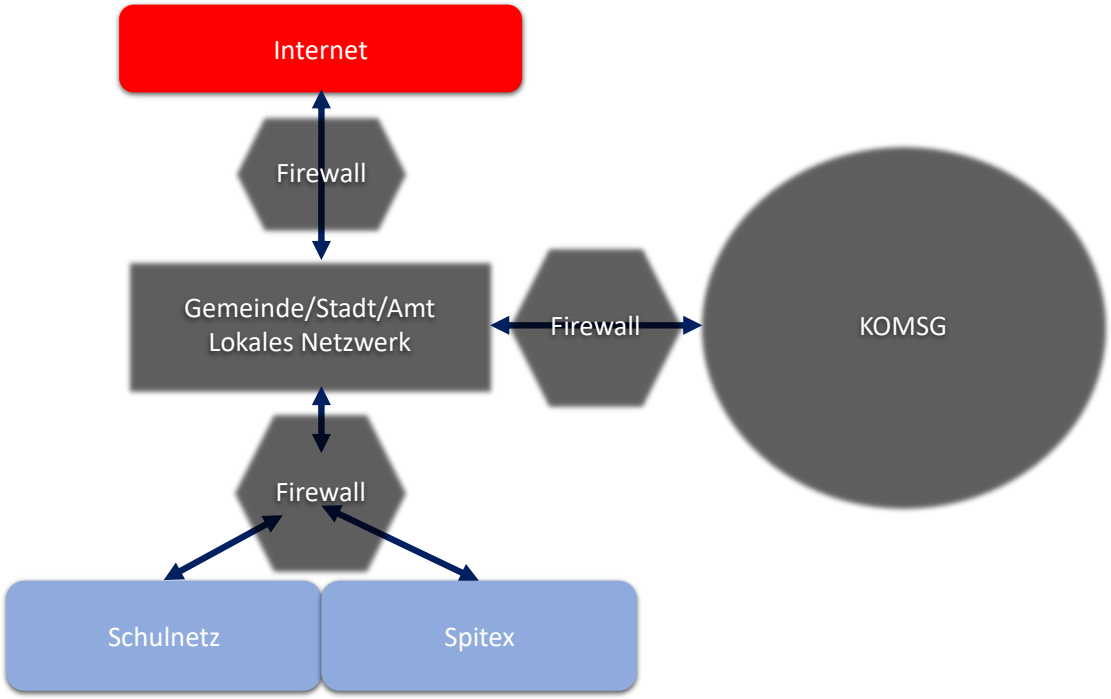

Abbildung 2 - Partner II

2 Organisatorische Massnahmen

2.1 Vorkehrungen der KOM SG

Zur Sicherstellung der Sicherheit im KOMSG-Netz führt die KOM SG regelmässig Überprüfungen durch. Die KOM SG besitzt, bezogen auf die Belange der im vorliegenden Dokument definierten Vorgaben und in Absprache mit Verantwortlichen, das Auditrecht des Partner-Netzwerks und an dessen angeschlossenen Systeme sowie der Netzwerke der Dienstanbieter und Netzbetreiber. Die Kosten für das Audit werden von der KOM SG getragen. Ausnahmen bilden wiederholte Sicherheitsverletzungen, die eine Nachprüfung erfordern sowie Zugänge von Dritten zum KOMSG.

Die Dienstanbieter und Netzbetreiber überwachen zur Feststellung und Auswertung von Sicherheitsvorfällen, unter Einhaltung der Datenschutzbestimmungen, laufend die technischen Ressourcen in Form von automatisierten Protokollierungen.
Um die Gefährdung ausgehend von Schadsoftware zu reduzieren, wird beim Internetzugang der KOM SG bzw. deren Vertragspartner der Datenverkehr analysiert. Die auf das Auffinden von Schadsoftware beschränkte Inspektion betrifft mit wenigen Ausnahmen den gesamten Datenverkehr. Die Inspektion des Datenverkehrs erfolgt datenschutzkonform.
Die KOM SG teilt schriftlich festgestellte Missbräuche dem Verantwortlichen des Partners mit. Missbräuchlich ist jede Verwendung der Informatikmittel, die:

a) gegen diese Sicherheitsvorschriften verstösst;

b) gegen andere Bestimmungen der Rechtsordnung verstösst.

2.2 Verantwortung des Partners

Die Verantwortlichkeiten für die Sicherheit innerhalb der angeschlossenen Institutionen müssen geregelt und dokumentiert sein. Jede Institution (Amtsstelle, Gemeinde, öffentlich-rechtliche Anstalt, Dritte) hat einen Informatik- und Sicherheitsverantwortlichen zu benennen und der KOM SG mitzuteilen. Dieser sorgt für die korrekte Umsetzung der vorliegenden Sicherheitsvorschriften.
Die eingesetzten Informatikmittel sind gemäss den vorliegenden Sicherheitsbestimmungen zu schützen. Die Partner sind verpflichtet, die diesbezüglichen Rechte und Pflichten gegenüber den betroffenen Benutzern mittels einer schriftlichen Nutzungsvereinbarung zu regeln.
Es steht dem Partner frei, die Umsetzung von Teilen oder der Gesamtheit der hier beschriebenen Vorgaben an einen IT-Leistungserbringer zu überbürden. Seitens des Partners müssen entsprechende vertragliche Regelungen getroffen werden, welche die Einhaltung der Sicherheitsvorschriften von seinem IT-Leistungserbringer verlangen. Diese Weitergabe entbindet den Partner nicht von der Verantwortung gegenüber der KOM SG.
Im Rahmen seiner Verantwortung ist der Partner insbesondere für eine regelmässige Prüfung der Konformität seiner Installationen mit diesen Sicherheitsvorschriften besorgt. Die KOM SG stellt dafür entsprechende Checklisten zur Verfügung. Der Partner ist verpflichtet seine Informationssicherheit mindestens einmal jährlich mit Hilfe dieser Checklisten zu überprüfen und das Ergebnis der KOM SG mitzuteilen. Die KOM SG wertet diese aus und leitet notwendige Korrekturen oder Sanktionen ein.

2.3 Bewältigung ausserordentliche Lage

Der Verantwortliche des Partners ist zusammen mit seinen IT-Leistungserbringern für das Erstellen und Einhalten der notwendigen Prozesse beim Auftreten von ausserordentlichen Lagen, wie zum Beispiel das Auftreten von Schadsoftware verantwortlich. Sie haben sämtliche ihnen zur Verfügung stehenden Mittel bereitzuhalten und anzuwenden, damit sich zum Beispiel die Schadsoftware nicht im KOMSG verbreiten kann. Notfalls müssen bestimmte Systeme vom Netzwerk getrennt werden.
Besteht die Gefahr einer Verbreitung eines Sicherheitsvorfalls, muss umgehend die KOM SG (info.igkomsg@sg.ch, Tel. 058 229 41 30) und der Service Desk der Abraxas Informatik AG (servicedesk@abraxas.ch, 058 660 00 10) informiert werden. Die KOM SG informiert ihrerseits die Partner bei der Gefahr einer Verbreitung eines Sicherheitsvorfalls.
Die KOM SG behält sich bei einem allfälligen Notfall vor, aus Sicherheitsgründen bestimmte Teile vom Netz abzutrennen, um die weitere Verbreitung im KOMSG einzugrenzen.

3 Schutz der Systeme

3.1 Schutz von Serversystemen

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

3.1.1 Administrierung / Zugriffe

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

Im Anhang, Kapitel 2.1.1 ist definiert, welche Ports mindestens eingeschränkt werden müssen.

Wenn die Serversysteme nicht in einem anderen Netzwerk als die Clients verweilen und keine Firewall die beiden Netzwerke trennt, sollen die Einschränkungen mittels Host-Firewall (z.B. Windows Firewall) realisiert werden. Die in Windows integrierte Firewall kann mittels Gruppenrichtlinien gesteuert werden und kann diese Anforderungen erfüllen.

Grundsätzlich soll verhindert werden, dass sämtliche Clients diese Ports auf den Servern via Netzwerk erreichen. Nur Administratoren oder sonstiges Personal, das für dessen Arbeitserfüllung Zugriffe benötigt, soll auch effektiv die Systeme mit den entsprechenden Ports erreichen können.

Für administrative Zugriffe soll eine Nachvollziehbarkeit gewährleistet sein (wer hat wann auf das System zugegriffen). Dies kann beispielsweise durch die Nutzung von personalisierten Accounts gelöst werden. Grundsätzlich sollen keine unpersönlichen Accounts verwendet werden.

Darüber hinaus dürfen keine Zugriffsmethoden verwendet werden, die das Passwort im Klartext übermitteln.

3.1.2 Aktualisierung

Updates, die Sicherheitslücken ab einem CVSSv3 Score[4] von 5.0 beheben, werden innerhalb von 30 Tagen auf sämtlichen Serversystemen installiert. Ist eine Installation aus bestimmten Gründen nicht sofort möglich, werden diese schriftlich dokumentiert. Eine Installation muss spätestens nach 60 Tagen stattfinden. Ausnahmen können gemacht werden, wenn das Ausnutzen einer Sicherheitslücke durch andere Mittel (beispielsweise deaktivieren eines Service) verhindert wird.

Systeme, die vom Internet her erreichbar sind (mit oder ohne Reverse Proxy/WAF), müssen alle vom Betriebssystem- und Applikations-Hersteller «kritisch» (CVSSv3 Score ab 9.0) eingestuften Sicherheitsupdates innerhalb von 14 Tagen installieren und sicherstellen, dass diese aktiv sind (möglicherweise Reboot).
Für kritische Sicherheitsupdates, die Lücken schliessen, die von Angreifern bereits ausgenutzt werden, ist eine zeitnahe Installation (innerhalb von 14 Tagen) durchzuführen. Die KOM SG nimmt in Spezialfällen Kontakt mit den Partnern auf und informiert, bis wann die Patches installiert werden müssen.

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

Falls eine Installation von Updates längerfristig nicht möglich ist, muss das System netzwerktechnisch abgeschirmt werden (Verbindungen nur von einzelnen Endpunkten ermöglicht, keine Verbindung von Clients zum System). Gründe und Massnahmen werden schriftlich dokumentiert.

Identische Regelungen gelten für sonstige auf dem Server betriebene Software/Services. Wird auf einem Windows Server beispielsweise eine Software für die Zeit-Erfassung betrieben, wird auch diese mit Sicherheitsupdates gemäss Regelungen oberhalb versorgt. Ausnahmen können gemacht werden, wenn das Ausnutzen einer Sicherheitslücke durch andere Mittel (beispielsweise deaktivieren eines Service) verhindert wird.

3.1.3 Schutz vor Malware

Alle Serversysteme sind mit einem aktuellen Virenschutz ausgestattet. Security Produkte, die oftmals einen zusätzlichen Schutz bieten und meistens unter den Akronymen EDR/XDR (Endpoint bzw. Extended Detection und Response) bekannt sind, werden ebenfalls für den Einsatz empfohlen.

Auswertungen vom eingesetzten Virenschutz werden zentral gesammelt und wöchentlich geprüft. Administratoren müssen Einsicht in Befunde und Warnungen an einer zentralen Stelle haben. Bei einem Vorfall werden Administratoren automatisch alarmiert. Virensignaturen werden mindestens täglich erneuert.

3.1.4 Installierte Software

Auf den Server wird nur die für den Betrieb notwendige Software installiert. Keine zusätzlichen Installationen von Webbrowsern oder sonstigen Client-Applikationen (Adobe Reader, Office Programme etc.) sind zulässig, ausser diese sind für den Betrieb des Servers unerlässlich.

3.2 Schutz von Clients (Endpoint Security)

3.2.1 Benutzerrechte

Benutzer haben auf den Clients eingeschränkte Rechte. Mitarbeitende haben keine Admin-Rechte auf Ihren Clients.
Für Ausnahmen und Spezialfälle (z.B. die Installation einer Software) können die temporären Passwörter von LAPS an Benutzer ausgehändigt werden. Siehe Kapitel 4.3 für mehr Informationen bezüglich LAPS.

3.2.2 Administrierung / Zugriffe

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). Die in Windows integrierte Firewall kann mittels Gruppenrichtlinien gesteuert werden und kann diese Anforderungen erfüllen.
Eingehende Zugriffe sollen lediglich von Netzwerken/IP-Adressen der Administratoren erlaubt werden.

Im Anhang Kapitel 2.2.1 ist definiert, welche Ports mindestens eingeschränkt werden müssen.

Für administrative Zugriffe sollen bestenfalls lokale Accounts via LAPS genutzt werden.
Siehe Kapitel 4.3 für mehr Informationen bezüglich LAPS.

3.2.3 Aktualisierung

Updates, die Sicherheitslücken in Betriebssystem und Clientapplikationen (Browser, Reader etc.) ab einem CVSSv3 Score[5] von 5.0 beheben, werden innerhalb von 30 Tagen installiert. Ist eine Installation aus bestimmten Gründen nicht sofort möglich werden diese schriftlich dokumentiert. Eine Installation muss spätestens nach 60 Tagen stattfinden. Ausnahmen können gemacht werden, wenn das Ausnutzen einer Sicherheitslücke durch andere Mittel (beispielsweise deaktivieren eines Service) verhindert wird.

Die Zeitdauer gilt zudem nur für Clients, die in der entsprechenden Zeit online waren. Ein Client, der über längere Zeit offline ist, muss nicht extra gestartet werden für die Updates, eine Installation muss sichergestellt werden, sobald das Gerät wieder genutzt wird.

Für kritische Sicherheitsupdates, die Lücken schliessen, die von Angreifern bereits ausgenutzt werden, ist eine zeitnahe Installation (innerhalb von 14 Tagen) durchzuführen. Die KOM SG nimmt in Spezialfällen Kontakt mit den Partnern auf und informiert, bis wann die Patches installiert werden müssen.

3.2.4 Schutz vor Malware

Alle Clients sind mit einem aktuellen Virenschutz ausgestattet. Auswertungen vom eingesetzten Virenschutz werden zentral gesammelt und wöchentlich geprüft. Administratoren müssen Einsicht in Befunde und Warnungen an einer zentralen Stelle haben.

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

Bei einem Vorfall werden Administratoren automatisch alarmiert. Virensignaturen werden mindestens täglich erneuert.
Security Produkte, die oftmals einen zusätzlichen Schutz bieten und meistens unter den Akronymen EDR/XDR (Endpoint bzw. Extended Detection und Response) bekannt sind, werden ebenfalls für den Einsatz empfohlen.
Der Virenschutz darf von den Benutzern nicht manipuliert (deaktivieren, Hinzufügen von Ausnahmen etc.) werden können.

3.2.5 Einschränkung von Office Makros

Die Makro Einstellungen von Office Programmen muss via Gruppenrichtlinie erfolgen. Bestenfalls wird die Ausführung von Makros komplett deaktiviert. Falls Makros eingesetzt werden, muss mindestens folgende Option definiert werden: «Mit Benachrichtigung deaktivieren»

Im Anhang, Kapitel 2.2.2, sind einstechende Zusatzinformationen zur Konfiguration dokumentiert.

3.2.6 Festplattenverschlüsselung

Die Festplatten von Clients sind komplett verschlüsselt, insofern diese Mobil sind (Notebooks / Tablets / Desktops, die das Unternehmen verlassen). Eine Verschlüsselung wird ebenfalls für stationäre Desktop Clients empfohlen. Eine mögliche Lösung zur Verschlüsselung ist Bitlocker von Microsoft.

Datenträger, die entsorgt werden, sollen ebenfalls verschlüsselt oder durch geeignete Methoden ‘gesäubert’ werden.

3.2.7 Sperrbildschirm

Mittels Gruppenrichtlinien muss konfiguriert werden, dass Geräte nach maximal 15 Minuten automatisch gesperrt werden, insofern keine Userinteraktion erfolgt.

Betriebsnotwendige Ausnahmen sind zulässig, beispielsweise auf einer Notfall-Station. Jegliche Ausnahmen sollen schriftlich dokumentiert werden.

3.2.8 Schutz von geschäftlichen Smartphones

Smartphones, die für geschäftliche Zwecke genutzt werden, wie beispielsweise einer E-Mail und oder Kalendersynchronisation müssen folgende Vorgaben erfüllen:

- Verschlüsselter Speicher (Standard bei heutigen Geräten)
- Erzwungene Passwort-, PIN- (mindestens 4 Zeichen) und oder Biometrische-Sperrung
- Möglichkeit für den Remote-Wipe (Löschen der Unternehmensdaten von remote) muss bestehen
- Mitarbeitende sind darauf aufmerksam zu machen, dass Sicherheitsupdates auf den Smartphones regelmässig, mindestens alle 60 Tage, installiert werden müssen.

4 Active Directory Hardening

4.1 Anmeldebeschränkungen für Domain Admins

Diese Konfiguration richtet sich an reine On-Premise Active Directory Umgebungen, die keine Privileged Access Strategien aus der Cloud[6] nutzen.

Domänen Administratoren sollen, beispielsweise mittels Gruppenrichtlinien, in Ihren Anmeldungsmöglichkeiten eingeschränkt werden.
Domänen-Administratoren sollen sich ausschliesslich auf Domänen-Controller einloggen können. Ein Login auf Member-Server oder auf Clients soll verhindert werden. Grund dafür sind die damit verbundenen Risiken betreffend Anmeldeiformationen. Wenn ein Angreifer beispielsweise einen Client eines Mitarbeitenden kompromittiert, wo sich zuvor ein Domänen-Administrator eigeloggt hat, sind dessen Anmeldeinformationen gefährdet, da Windows gewisse Daten zwischenspeichert.

Die erforderlichen Schritte für die Konfiguration sind im Anhang, Kapitel 2.3.1 dokumentiert.

4.2 Schutz von Domain Admins

Für sämtliche Accounts in der 'Domänen-Administratoren' Gruppe gilt es folgende Konfigurationen vorzunehmen.

- Alle Mitglieder sind in der 'Protected Users'[7] Gruppe.
- Keine Mitglieder haben einen SPN (Service Principal Name) definiert.
- Die Anmeldebeschränkung (Kapitel 4.1) wurde komplett konfiguriert.

4.3 Management von lokalen Administratoren

Auf Computer-Systemen (Clients und Server) in der Domäne sollen einzigartige Passwörter für den lokalen Administrator konfiguriert werden. Sämtliche Clients und Sever sollen ein einzigartiges Passwort für den lokalen Administrator verwenden. Microsoft bietet dafür den Service LAPS[8] an, der frei genutzt werden kann.
Durch die Konfiguration von LAPS wird verhindert, dass identische Passwörter für den lokalen Admin-Account auf mehreren Systemen konfiguriert ist.

4.4 Passwortrichtlinien

Folgende Passwortrichtlinien stellen für sämtliche Benutzeraccounts die Mindestanforderung dar:

- 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

Die Konfiguration ist mittels Gruppenrichtlinie vorzunehmen.

Wenn diese Anforderungen nicht eingehalten werden können, muss dies schriftlich dokumentiert werden, die KOM SG soll entsprechend informiert werden.

---

[6] https://docs.microsoft.com/en-us/security/compass/privileged-access-strategy
[7] https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group
[8] https://www.microsoft.com/en-us/download/details.aspx?id=46899

4.5 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.

Daher wird empfohlen SMB Signing sowie LDAP Signing zu aktivieren. Im Anhang, Kapitel 2.3.2, sind die technischen Details sowie Links dokumentiert.

4.6 Deaktivieren von veralteten Features

4.6.1 NT LAN Manager Version 1 (NTLMv1)

NTLMv1 ist stark veraltet und stellt eine hohe Gefährdung für interne Authentisierung dar. NTLMv1 soll in der Domäne deaktiviert werden.

Im Anhang, Kapitel 2.3.3.1, sind die technischen Details sowie Links dokumentiert.

4.6.2 Link-Local Multicast name Resolution (LLMNR) deaktivieren

LLMNR ist ein veraltetes Protokoll, das als Fallback für DNS eingesetzt wurde. In lokalen Netzwerken erlaubt es Angreifern auf LLMNR Anfragen zu antworten, um so an Zugangsdaten zu gelangen. Das Feature wird nicht benötigt und kann in den Gruppenrichtlinien deaktiviert werden.

Im Anhang, Kapitel 2.3.3.2, sind die technischen Details sowie Links dokumentiert.

4.6.3 NetBIOS-NS (NBT-NS) deaktivieren

Genau wie LLMNR ist NBT-NS ein Protokoll für die Namensauflösung, wenn kein DNS-Server zur Verfügung steht. NBT-NS ist sogar noch älter als LLMNR und sorgt für identische Schwachstellen.

Im Anhang, Kapitel 2.3.3.3, sind die technischen Details sowie Links dokumentiert.

4.7 Löschen von GPP Files mit Passwörtern

Falls noch veraltete Group Policy Preference Konfigurationsdateien vorhanden sind, mit welchen Passwörter für lokale Administratoren definiert werden konnten, so müssen diese gelöscht werden.

Entsprechende Hintergründe und Details sind im Anhang, Kapitel 2.3.4 dokumentiert.

4.8 Aktivierung Credential Guard

Credential Guard schützt Anmeldeinformationen auf den Endgeräten und sollte nach Möglichkeit aktiviert werden.

Im Anhang, Kapitel 2.3.5, sind die technischen Details sowie Links dokumentiert.

4.9 Einschränkung zur Erstellung von neuen Computeraccounts

Standardmässig kann jeder Useraccount in der Domäne 10 neue Geräte der Domäne hinzufügen resp. 10 neue Computeraccounts in der Domäne erstellen. Diese Funktionalität hilft Angreifern bei mehreren Angriffsvektoren und soll unterbunden werden.

Im Anhang, Kapitel 2.3.6, sind die technischen Details sowie Links dokumentiert.

5 Schutz des Netzwerks

5.1 Schutz innerhalb des internen Netzwerks

5.1.1 Administrierung von Netzkomponenten, IoT und sonstigen Geräten mit Netzwerkverbindung

Wenn Netzkomponenten oder sonstige Geräte mit Netzwerkverbindung (Router, Switches, WLAN Access Points, Drucker, Kameras, Firewalls etc.) Services für eine aktive Administration anbieten (Webinterface, SSH etc.), muss der Zugriff darauf eingeschränkt werden. Eingehende Zugriffe sollen lediglich von Netzwerken/IP-Adressen der Administratoren erlaubt werden. Dies kann durch dedizierte Firewalls, Host-Firewalls oder ACL (Access Control Lists) realisiert werden.

Eine Segmentierung durch VLANs oder eine physische Trennung mit Routing über eine Firewall wird empfohlen. Wenn ein einzelnes Netzwerk für alle Komponenten verwendet wird, sollen entsprechende Host-basierte Einschränkungen vorgenommen werden.

Es dürfen keine Standardpasswörter des Herstellers verwendet werden. Darüber hinaus dürfen keine Zugriffsmethoden verwendet werden, die das Passwort im Klartext übermitteln.

5.1.2 Aktualisierung von Netzkomponenten, IoT und sonstigen Geräten mit Netzwerkverbindung

Updates, die Sicherheitslücken ab einem CVSSv3 Score von 5.0 beheben, werden innerhalb von 60 Tagen installiert. Ist eine Installation aus bestimmten Gründen nicht möglich, werden diese schriftlich dokumentiert und bei Bedarf vorgewiesen. Eine Installation ist zeitnah durchzuführen.

Auf Systemen, die aus dem Internet oder sonstigen Fremdnetzen erreichbar sind, müssen Updates, die Sicherheitslücken ab einem CVSSv3 Score von 5.0 beheben, innerhalb von 30 Tagen installiert werden. Für kritische Sicherheitsupdates, die Lücken schliessen, die von Angreifern bereits ausgenutzt werden, ist eine zeitnahe Installation (innerhalb von 14 Tagen) durchzuführen. Die KOM SG nimmt in Spezialfällen Kontakt mit den Partnern auf und informiert, bis wann die Patches installiert werden müssen.

Ausnahmen können gemacht werden, wenn das Ausnutzen einer Sicherheitslücke durch andere Mittel (beispielsweise deaktivieren eines Service) verhindert wird.

5.1.3 Aktivierung von Sicherheitsfeatures

Unterstützen Netzkomponenten zusätzliche Security Features (beispielsweise Schutz vor ARP-Spoofing oder Rouge DHCP Server) sollten diese aktiviert werden.

5.1.4 VLAN Konfiguration

Werden VLANs zur Trennung von Netzzonen eingesetzt, so müssen folgende Punkte in Bezug auf deren Konfiguration beachtet werden:

- Das VLAN 1 (Default VLAN) wird nicht verwendet. Falls ein default VLAN benötigt wird, ist ein dediziertes anderes VLAN zu verwenden.
- Netzwerkanschlüsse sind gezielt für den Gebrauch als Benutzerport (Access) oder als Backbone-Port (Trunk) konfiguriert.
- Es werden nur die nötigen VLANs auf dem Trunk erlaubt.

- Allenfalls vorhandene Protokolle wie VTP zur automatischen Konfiguration von VLANs sind ausgeschaltet (bzw. mode transparent) oder wenn benötigt sind VTP-Passwörter konfiguriert.

5.1.5 Network Access Control (NAC)

Es wird empfohlen ein NAC für sämtliche Netzwerkanschlüssen zu verwenden. Dies kann mittels MAC-Adressfilterung erfolgen, bestenfalls jedoch mittels Client-/Userzertifikat (802.1x).

Bei öffentlich zugänglichen Netzwerkanschlüssen (z.B. Drucker auf dem Korridor), muss mindestens eine Einschränkung auf die MAC-Adresse erfolgen, bestenfalls jedoch mittel Client-/Userzertifikat (802.1x).

5.1.6 Dokumentation

Eine aktuelle Dokumentation von sämtlichen Netzkomponenten, IoT und sonstigen Geräten mit Netzwerkverbindung existiert, beispielsweise in Form eines Netzplans oder einer Tabelle.
Eine aktuelle Dokumentation zur Installation und Konfiguration dieser Netzkomponenten existiert.

5.2 Schutz vor Fremdnetzen

5.2.1 Definition Fremdnetz

Als Fremdnetz gelten sämtliche Netzwerke, die nicht direkt von Mitarbeitenden des Partners (Gemeindeverwaltung, Spital etc.) genutzt werden.
Das Netzwerk von einer angeschlossenen sozialen Fachstelle, eines Schülerhorts oder einer Schule sind beispielsweise als Fremdnetze zu betrachten. Weitere Beispiele für Fremdnetze:

- Netzwerk des IT-Dienstleisters
- Internet (eigener Internetanschluss)
- Netzwerk eines Lieferanten
- Netzwerke mit Nutzern, die nicht Angestellte des Partners sind, Steuerkommissär ausgenommen)
- Netzwerke mit Systemen, die nicht den KOMSG Richtlinien unterliegen

Anmerkung: Sobald ein User oder ein System die oben genannten Kriterien erfüllt, gilt das gesamte Netzwerk als Fremdnetz.

5.2.2 Trennung zu Fremdnetzen

Wenn das interne Netzwerk über Verbindungen zu einem Fremdnetz verfügt, muss eine Trennung mittels dedizierter Firewall erfolgen. Die Firewall muss die möglichen Verbindungen zwischen den beiden Netzwerken auf das Nötigste beschränken. Ausschliesslich benötigte Ports sowie Endpunkte sollen zugelassen werden, das Firewall-Regelwerk ist restriktiv zu gestalten. Dies gilt auch für die Verbindung zum Internet.
Eine abschliessende ‘deny any‘ Regel stellt die Blockierung sämtlicher Verbindung sicher, die nicht explizit erlaubt wurden.

Die eingesetzte Firewall muss folgende Anforderungen erfüllen, resp. die entsprechenden Features müssen aktiviert sein.

- SSL/TLS Inspection Richtung WAN muss aktiviert werden, wenn der eigene Internetzugang von den Mitarbeitenden des Partners genutzt wird.
- Content Filtering (DNS/URL) Richtung WAN muss aktiviert werden, wenn der eigene Internetzugang von den Mitarbeitenden des Partners genutzt wird.
- Intrusion Detection System (IDS) inkl. Intrusion Prevention System (IPS)

Entsprechende Ausnahmen für die TLS Inspection, beispielsweise für E-Banking wurden dokumentiert.

Eine Trennung mittels Firewall ist NICHT notwendig, wenn das Fremdnetz getrennt vom Netzwerk des Partners ist (logisch oder physisch).
Beispiel: Ein eigener Internetanschluss besteht, wird jedoch nur für das Gäste-WLAN verwendet und nutzt eigenständige Hardware. Keine direkten Verbindungsmöglichkeiten dürfen zwischen den Netzwerken bestehen.

5.2.3 Anforderungen bei Systemen mit Erreichbarkeit aus dem Internet

Werden Systeme im internen Netzwerk betrieben, die vom Internet erreicht, werden können (beispielsweise eigener Exchange Server mit verfügbarem OWA), so müssen diese Systeme in einer DMZ betrieben werden. Verbindungen zwischen internen Netzwerken und der DMZ sind mittels Firewall restriktiv einzuschränken.

Für Web-Dienste sollte bestenfalls eine Web-Application-Firewall (WAF) eingesetzt werden.

Wenn ein Datenzugriff via Internet ermöglicht wird, so muss der Zugriff mittels starker Authentisierung (mindestens 2-Faktor) erfolgen.
Beispiel: Ein Zugriff aus dem Internet auf Geschäftsdaten oder Geschäftsemails.

5.2.4 Trennung zum KOMSG

Fremdnetze sind komplett vom KOMSG zu trennen. Aus Fremdnetzen darf keine Verbindung zum KOMSG ermöglicht werden.

5.3 Remote Unterstützung und Fernwartung

5.3.1 Anforderungen Remote Unterstützung (User Support)

Der Zugriff muss von den betroffenen Nutzern aktiv gewährt werden, es darf kein Zugriff ohne manuelle Bestätigung durch den User erfolgen.
Falls der Support via Internet stattfindet, muss zwingend eine starke Authentisierung (2-Faktor) eingesetzt werden. Eine Lösung wie TeamViewer Quicksupport, wobei User zunächst manuell ein Verbindungsfile herunterladen müssen, erfüllt diese Anforderung ebenfalls.
Die Kommunikation muss in jedem Fall mit einem als aktuell sicher geltenden Protokoll verschlüsselt werden.

5.3.2 Anforderungen für die Fernwartung (Wartung von Systemen)

Für die Fernwartung via Internet muss zwingend eine starke Authentisierung (2-Faktor) eingesetzt werden.
Es dürfen keine Systeme, die nicht in einer DMZ angesiedelt sind, direkt aus dem Internet erreichbar sein, siehe dazu auch Kapitel 5.2.3. Nicht zulässig wäre beispielsweise ein RDP Zugriff aus dem Internet direkt auf einen Server im internen Netzwerk.
Zugriffe mittels Fernwartung müssen in jedem Fall protokolliert werden. Es muss eine Nachvollziehbarkeit bestehen, wer wann auf welche Systeme zugegriffen hat.
Für den Zugriff werden in jedem Fall personifizierte Accounts genutzt.
Die Freischaltung von temporären Zugriffen externer Partner erfolgt zentral und ist zeitlich auf ein absolutes Minimum beschränkt. Muss beispielsweise der Lieferant einer Software kurzzeitig auf einen Server zugreifen, so wird der Zugriff nur zeitlich begrenzt ermöglicht und nach Durchführung der Konfiguration sofort wieder deaktiviert. Zudem muss eine Vertraulichkeitsvereinbarung von den Partnern unterzeichnet werden.

5.4 Drahtlose Netzwerke – WLAN

5.4.1 **WLAN als internes Netzwerk**

Wenn das WLAN, Zugriffe auf interne Ressourcen des Partners ermöglicht, z.B. auf die Fileablage oder eine interne Webapplikation, gilt das WLAN als internes Netzwerk. Für drahtlose interne Netzwerke müssen folgende Bedingungen erfüllt werden:

- Die Authentisierung zum Netzwerk muss mittels starker Authentisierung (2-Faktor) erfolgen (bestenfalls zertifikatsbasiert). Möglich wäre z.B. eine Authentisierung mittels Username, Passwort und einem Gerätezertifikat.
- Die Daten werden auf der Luftstrecke mit einem heute als sicher geltenden Algorithmus verschlüsselt.
- Die WLAN-Accesspoints werden zentral verwaltet
- Die Benutzerverwaltung des WLAN wird kontinuierlich gepflegt. Es ist sicherzustellen, dass austretende Mitarbeiter keinen Zugriff mehr auf das WLAN erhalten.

Betriebsnotwendige Ausnahmen sind zulässig, beispielsweise bei medizinischen Geräten, welche die Anforderungen nicht erfüllen. Zugriffe für diese Geräte sollen möglichst stark eingeschränkt werden. Jegliche Ausnahmen sollen schriftlich dokumentiert werden.

5.4.2 **Gäste WLAN**

Gewährt ein WLAN keinerlei Zugriffe auf interne Ressourcen, so gilt dieses als Gäste WLAN. Folgende Punkte müssen sichergestellt werden, wenn ein Gäste WLAN betrieben, wird:

- Das WLAN ist durch eine Firewall (oder physisch) vom restlichen Netzwerk abgetrennt, direkte Zugriffe auf interne Netzwerke oder dem KOMSG müssen unterbunden werden.
- Die Firewall erlaubt nur den Zugriff mit den nötigsten Diensten ins Internet.

5.5 VPN

5.5.1 VPN Tunnel aus dem Internet zum Partner

Ein VPN-Zugang zum KOMSG und dem Netzwerk des Partners wird grundsätzlich durch die KOM SG bzw. deren Vertragspartner (aktuell Abraxas) angeboten. Hat der Partner das Bedürfnis eine eigene Lösung zu betreiben, müssen dabei die folgenden Grundsätze befolgt werden:

- Der VPN Tunnel muss auf der Firewall oder einem dedizierten System in der DMZ des Partners terminiert werden.
- Die Verbindung wird im Transport mit einem heute als sicher geltenden Algorithmus/Protokoll verschlüsselt.
- Die VPN Konfiguration darf kein Split-Tunneling erlauben. Sämtliche Kommunikation muss durch den VPN-Tunnel gesendet werden (Full-Tunneling).
- Die Benutzer-Authentisierung nutzt eine starke Authentisierung (2-Faktor) und ist personifiziert.
- Mobile Endgeräte wie Smartphones und Tablet-PC, die sich mittels VPN verbinden, müssen über eine Verwaltungsinstanz administriert werden (z.B. MDM)
- Die authentisierte Kommunikation wird durch die Firewall bzw. dem dedizierten System in der DMZ nach einer definierten Lebensdauer, maximal acht Stunden, terminiert.

5.5.2 VPN Tunnel innerhalb der Infrastruktur des Partners (Site to Site)

Nutzt der Partner innerhalab seiner Netzwerke Site to Site Tunnel, beispielsweise um Aussenstandorte anzubinden müssen folgende Punkte beachtet werden:

- Der VPN Tunnel muss beidseitig auf einer Firewall oder einem dedizierten System in der DMZ des Partners terminiert werden.
- Die Verbindung wird im Transport mit einem heute als sicher geltenden Algorithmus/Protokoll verschlüsselt.
- Die genutzten Schlüssel zur Authentisierung werden verschlüsselt aufbewahrt und nicht im Klartext übermittelt.
- Über den Tunnel werden nur benötigte Netzwerke transportiert.

5.5.3 VPN Tunnel innerhalb des KOMSG

Grundsätzlich sind direkte VPN Tunnels innerhalb des KOM SG verboten, wenn sie dem Zweck dienen Verbindungen zwischen einzelnen Partnern oder zwischen Partner und internen oder externen Rechenzentren aufzubauen. Vor allem wenn der Tunnel dazu dient die gesamte Kommunikation eines KOM SG-Partner oder -Standortes über den Tunnel zu transportieren. Bei den VPN Tunnels sind Tunnels gemeint, welche die Tunneltechnologien PPTP, L2TP, GRE, SSL, IPsec, etc. verwenden.
Unter bestimmten Voraussetzungen und in Rücksprache mit der KOM SG können bestimmte VPN Tunnels innerhalb des KOM SG eingesetzt werden. Hierfür wird ein schriftlicher Antrag des Partners benötigt.

5.6 Voice over IP (VoIP)

Die KOM SG bietet den Dienst Voice over IP (VoIP) in vier verschiedenen Varianten an. Die fünfte Variante ist unabhängig vom KOM SG. Für die Umsetzung des Quality of Service (QoS) gilt als Grundlage das Quality of Service Konzept der KOM SG.

5.6.1 Variante 1: VoIP Kommunikation mittels Skype 4 Business (S4B) über das KOMSG

Alle Partner der Variante 1 telefonieren mittels S4B der KOM SG. Für die Kommunikation in das öffentliche Telefonnetz wird ein zentraler SIP-Gateway der KOM SG (SBC) verwendet. Ergänzend zu den übrigen Vorschriften zum Schutz des Netzwerks müssen im Netzwerk des Partners die folgenden Anforderungen erfüllt sein:

- Die Anforderungen an das Netzwerk des Partners sind im Detailkonzept Skype 4 Business der KOM SG definiert. Diese werden dem Partner zur Verfügung gestellt.

5.6.2 Variante 2: VoIP Kommunikation mittels KOMSG SIP über das KOMSG

Alle Partner der Variante 2 telefonieren mittels des KOM SG SIP. Für die Kommunikation in das öffentliche Telefonnetz wird ein zentraler SIP-Gateway der KOM SG verwendet. Ergänzend zu den übrigen Vorschriften zum Schutz des Netzwerks müssen im Netzwerk des Partners die folgenden Anforderungen erfüllt sein:

- Die IP-Adressierung des VoIP-Netzes muss zwingend aus dem Adressbereiche der KOM SG erfolgen.
- Für die Einspeisung des VoIP-Netzes zwischen der KOM SG und des Partners wird ein zusätzlicher Netzwerkport eingerichtet. Dieser ist kostenpflichtig.
- Um einen durchgängigen QoS Transport zu gewährleisten, müssen die verwendeten Netzwerkports der VoIP-Systeme den QoS Parametern der KOM SG entsprechen. Ansonsten gilt als Qualitäts-Grenze der Netzwerkport des VoIP-Netzes der KOM SG. Die zu verwenden QoS Parameter werden dem Partner von der KOM SG zur Verfügung gestellt.
- Die Kommunikation zwischen dem VoIP-Netz und des Partner-Netz (CTI) erfolgt über das KOM SG. Die benötigten Freischaltungen müssen durch den Partner bei der KOM SG beantragt werden.
- Die für die VoIP-Systeme verwendeten Netzwerkports müssen Autosensing und auch die manuelle Einstellung der Übertragungsrate sowie des Duplex Mode unterstützen.

5.6.3 Variante 3: VoIP Kommunikation mittels Enterprise SIP (ESIP) der Swisscom

Alle Partner der Variante 3 telefonieren mittels ESIP. Für die Kommunikation in das öffentliche Telefonnetz wird ein dedizierter SIP-Gateway beim Partner verwendet. Ein dedizierter Router der Swisscom wird beim Partner installiert.
Ergänzend zu den übrigen Vorschriften zum Schutz des Netzwerks müssen im Netzwerk des Partner die folgenden Anforderungen erfüllt sein:

- Die IP-Adressierung des VoIP-Netzes muss zwingend aus dem Adressbereiche der KOM SG erfolgen.
- Für die Einspeisung des VoIP-Netzes zwischen der KOM SG und des Partners wird ein zusätzlicher Netzwerkport eingerichtet. Dieser ist kostenpflichtig.
- Um einen durchgängigen QoS Transport zu gewährleisten, müssen die verwendeten Netzwerkports der VoIP-Systeme den QoS Parametern der KOM SG entsprechen. Ansonsten gilt als Qualitäts-Grenze der Netzwerkport des Voip-Netzes der KOM SG. Die zu verwenden QoS Parameter werden dem Partner von der KOM SG zur Verfügung gestellt.

- Die Kommunikation zwischen dem VoIP-Netz und des Partner-Netz (CTI) erfolgt über das KOM SG. Die benötigten Freischaltungen müssen durch den Partner bei der KOM SG beantragt werden.
- Die für die VoIP-Systeme verwendeten Netzwerkports müssen Autosensing und auch die manuelle Einstellung der Übertragungsrate sowie des Duplex Mode unterstützen.

5.6.4 Variante 4: VoIP Kommunikation mittels Rii-Seez SIP (RSIP) des EW Buchs über das KOMSG

Alle Partner der Variante 4 telefonieren mittels des RSIP. Für die Kommunikation in das öffentliche Telefonnetz wird ein zentraler SIP-Gateway des EW Buchs bzw. des Rii-Seez-Net verwendet.
Ergänzend zu den übrigen Vorschriften zum Schutz des Netzwerks müssen im Netzwerk des Partners die folgenden Anforderungen erfüllt sein:

- Eine logische oder physikalische Trennung zwischen dem Daten- und dem VoIP-Netz. Der Partner muss sicherstellen, dass eine abschliessende Netzwerktrennung zwischen diesen beiden Netzen vorhanden ist.
- Die IP-Adressierung des VoIP-Netzes muss zwingend aus dem Adressbereiche der KOM SG erfolgen.
- Für die Einspeisung des VoIP-Netzes zwischen der KOM SG und des Partners wird ein zusätzlicher Netzwerkport eingerichtet. Dieser ist kostenpflichtig.
- Um einen durchgängigen QoS Transport zu gewährleisten, müssen die verwendeten Netzwerkports der VoIP-Systeme den QoS Parametern der KOM SG entsprechen. Ansonsten gilt als Qualitäts-Grenze der Netzwerkport des Voip-Netzes der KOM SG. Die zu verwenden QoS Parameter werden dem Partner von der KOM SG zur Verfügung gestellt.
- Die Kommunikation zwischen dem VoIP-Netz und des Partner-Netz (CTI) erfolgt über das KOM SG. Die benötigten Freischaltungen müssen durch den Partner bei der KOM SG beantragt werden.
- Die für die VoIP-Systeme verwendeten Netzwerkports müssen Autosensing und auch die manuelle Einstellung der Übertragungsrate sowie des Duplex Mode unterstützen.

5.6.5 Variante 5: VoIP Kommunikation mit anderem SIP-Trunk Provider ohne Internetverbindung

Alle Partner der Variante 5 telefonieren mittels anderem SIP-Trunk Provider. Für die Kommunikation in das öffentliche Telefonnetz wird ein dedizierter SIP-Gateway beim Anbieter verwendet. Der Anschluss an den SIP-Gateway erfolgt NICHT über das Internet und der Anschluss ermöglicht keinerlei Verbindungen in das Internet
Ergänzend zu den übrigen Vorschriften zum Schutz des Netzwerks müssen im Netzwerk des Partner die folgenden Anforderungen erfüllt sein:

- Um einen durchgängigen QoS Transport zu gewährleisten, müssen die verwendeten Netzwerkports der VoIP-Systeme den QoS Parametern der KOM SG entsprechen. Ansonsten gilt als Qualitäts-Grenze der Netzwerkport des Voip-Netzes der KOM SG. Die zu verwenden QoS Parameter werden dem Partner von der KOM SG zur Verfügung gestellt.
- Die Kommunikation zwischen dem VoIP-Netz und des Partner-Netz (CTI) erfolgt über das KOM SG. Die benötigten Freischaltungen müssen durch den Partner bei der KOM SG beantragt werden.
- Die für die VoIP-Systeme verwendeten Netzwerkports müssen Autosensing und auch die manuelle Einstellung der Übertragungsrate sowie des Duplex Mode unterstützen.

- Beim Partner muss ein Session Boarder Controller (SBC) eingesetzt werden, auf den der SIP-Trunk terminiert wird.

5.6.6 Variante 6: VoIP Kommunikation innerhalb des Partnernetzwerks

Alle Partner der Variante 6 setzen VoIP für die Kommunikation innerhalb ihres Netzwerkes, nicht aber über das KOMSG ein. Für die Kommunikation über das öffentliche Telefonnetz muss ein VoIP-Gateway im Netzwerk des Partners implementiert sein.
Bei dieser Variante werden private, im KOMSG nicht geroutete IP-Adressen verwendet.
Ergänzend zu den übrigen Vorschriften zum Schutz des Netzwerks müssen im Netzwerk des Partners die folgenden Anforderungen erfüllt sein:

- Die für die VoIP-Systeme verwendeten Netzwerkports müssen Autosensing und auch die manuelle Einstellung der Übertragungsrate sowie des Duplex Mode unterstützen.
- Sollen die Arbeitsplätze bei einem Partner mit nur einem Ethernet-Kabel erschlossen werden, der PC also an das VoIP-Telefon angeschlossen werden können, muss die entsprechende Netzwerkkomponente VLAN-Trunking unterstützen.

6 Schutz in der M365/Azure Cloud

Bevor die Cloudservices von Microsoft genutzt werden, muss der Partner in Zusammenarbeit mit dem zuständigen Datenschutzbeauftragten abklären, welche Daten hochgeladen resp. verarbeitet werden dürfen.

6.1 Authentisierung in Azure Active Directory (AAD)

Folgende Kapitel beschreiben notwendige Konfigurationen, um die Authentisierung zu Azure Active Directory zu schützen. Partner können die ‘Security defaults’ innerhalb von AAD aktivieren oder mittels ‘Conditional Access Policies’ Einschränkungen vornehmen.
Grundsätzlich müssen folgende Punkte bezüglich Authentisierung abgedeckt sein:

- Starke Authentisierung (2-Faktor) für sämtliche User konfigurieren.
- Blockieren von älteren unsicheren Authentisierungsprotokollen (Legacy Authentication).
- Administratoren zu einer starken Authentisierung (2-Faktor) bei jedem Login zwingen.
- Sämtliche Benutzer zu einer starken Authentisierung (2-Faktor) beim Login zwingen, insofern Bedarf besteht (z.B. Login von einem neuen Gerät oder einer anderen Lokation).

6.1.1 Sicherung der Authentisierung mittels Security Defaults

Die Security Defaults bieten eine simple Lösung, um sämtliche oberhalb definierter Anforderungen abzudecken. Wenn die Security Defaults aktiviert werden, können keine Conditional Access Policies erstellt werden.

Im Anhang, Kapitel 2.4.1, sind die technischen Details sowie Links dokumentiert.

6.1.2 Sicherung der Authentisierung mittels Conditional Access policy

Conditional Access kann dazu verwendet werden, um den Zugriff auf AAD mit mehr Feinheiten als den Security Defaults zu konfigurieren. Ausnahmen, Regelungen und Scope muss manuell konfiguriert werden. Der Partner sollte Conditional Access nur dann einsetzen, wenn entsprechendes Know-How bezüglich AAD resp. Conditional Access besteht.

Im Anhang, Kapitel 2.4.2, sind die technischen Details sowie Links dokumentiert.

6.2 Endpoint Sicherheit mittels M365 Cloud

Falls die Endgeräte mittels AAD verwaltet werden, können benötigte Konfigurationen aus dem Kapitel 3.2 (Schutz von Clients) auch mittels M365 Cloud umgesetzt werden als Alternative zu den Gruppenrichtlinien.

Im Anhang, Kapitel 2.4.3, sind die technischen Details sowie Links dokumentiert.

6.3 Mail Routing – Sicherheit im E-Mail Verkehr

Standardmässig werden sämtliche E-Mails via Abraxas versendet/empfangen. Nutzt ein Partner ausschliesslich M365, um Mails zu empfangen und zu versenden, ohne dass diese via Abraxas geroutet werden, gelten folgende Mindestanforderungen:

- Eingehende E-Mails müssen durch eine Sandbox analysiert werden
- Die Anforderungen an die Sandbox-Lösung entsprechen den Parameter aus Kapitel 7.3.

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

- Safe Attachments
- Safe Links

Im Anhang, Kapitel 2.4.4, sind die technischen Details sowie Links dokumentiert.

6.4 Allgemeine Vorkehrungen

Einige Grundsätze, die beachtet werden müssen, sind nachfolgend aufgelistet.

6.4.1 Consent Grant (Enterprise Application)

Benutzer können standardmässig Applikationen mit Anbindung zu AAD Berechtigungen erteilen, um auf Informationen derer Profile zuzugreifen. So kann beispielsweise eine Kalender-App Zugriff auf die Kalenderinhalte des entsprechenden Benutzers anfragen.

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.

Im Anhang, Kapitel 2.4.5.1, sind die technischen Details sowie Links dokumentiert.

6.4.2 Notfall Account (Break-Glass Account)

Um den Zugang zu AAD sicherzustellen, kann es sinnvoll sein sogenannte ‚break-glass‘ Accounts zu erstellen. Dieser Account wird nie im täglichen Gebrauch genutzt, sondern ist lediglich für den Notfall zu konfigurieren.
Diese Accounts sollen mit den höchsten Berechtigungen (Global Admin) ausgestattet werden und keine 2-Faktor Authentisierung nutzen, die vom Mobilfunk oder Internet-Services Dritter abhängig ist. Wenn beispielsweise der Mobilfunk gestört ist und daher keine Authentisierung mittels 2-Faktor möglich ist, stellt ein solcher Account den Zugriff sicher. Zudem sollten diese Accounts nicht in eine On-Premise Umgebung synchronisiert werden resp. nur in der Cloud existieren.
Für diese Accounts gelten folgende Empfehlungen:

- Sehr langes (20+ Stellen) und komplexes Passwort.
- Das Passwort wird nur verschlüsselt abgelegt (z.B. in einem Passwortmanager) oder physisch sicher aufbewahrt (z.B. Safe).
- Wenn möglich 2-Faktor aktiviert, jedoch NICHT via Mobilfunk (z.B. FIDO oder (T)OTP Verfahren, die offline funktionieren).
- Nutzung nur im Notfall, keine tägliche Nutzung
- Alarmierung für Nutzung einrichten (Benachrichtigung, wenn dieser Account genutzt wird)

7 Schutz im E-Mail Verkehr (On-Premise Exchange oder Exchange Online)

7.1 Mengen – und Grössenbeschränkung

Auf jedem Mailserver im KOMSG-Verbund muss die maximale Attachmentgrösse von 20 MB und die maximale Empfängeranzahl pro E-Mail auf 200 Adressaten eingestellt werden.
Für Partner, die M365 ohne Anbindung an den KOMSG-Verbund nutzen gilt diese Einschränkung nicht.

7.2 Automatische Weiterleitungen

Automatische Weiterleitungen an externe Postfächer sind auf den Exchange Server technisch unterbunden worden.

7.3 Eigene Sandbox Lösung

Die kantonale Infrastruktur nutzt eine standardisierte Sandboxlösung um Mitarbeitende vor schädlichen Emails und deren Anhängen, Links etc. zu schützen.
Betreiber eigener Infrastrukturen müssen durch Ihre Sandboxlösung mindestens folgende Anforderungen abdecken.

7.3.1 Schutz vor bekannter Malware

Die Sandboxlösung muss:

- Malware durch bekannte Pattern erkennen. Moderne Malware-Pattern sind so implementiert, dass ganze Malware-Familien mit einem Pattern erkannt werden.
- Code Analyse durchführen, um unerwünschte Mechanismen in ausführbaren Dateien und Office Dokumenten zu erkennen
- Blockieren von E-Mails, die bekannten Malware Weblinks enthalten (anbinden von herstellerbezogener Malware URL-Listen wie auch externe Listen)
- Blockieren von E-Mail Anhängen, die Malware Weblinks enthalten
- Einpflegen von eignen Black/Whitelists, um umgehend auf einen Angriff reagieren zu können
- Umschreiben von unbekannten Weblinks während der Übermittlung des E-Mails, so dass beim Klick auf die URL erneut eine Prüfung über die Sandbox stattfindet. Dadurch kann Malware erkannt werden, die bei der Übermittlung des E-Mails noch nicht aktiv war.

7.3.2 Schutz vor unbekannter Malware

Um auch aktuell unbekannte Malware zu entdecken, muss die Sandboxlösung mindestens folgende Funktionalität aufweisen:

- Code Analyse in ausführbaren Dateien und Office Dokumenten (MS Office, PDF, ...) durchführen, um unerwünschte und gefährliche Mechanismen zu erkennen
- Ausführen von Makros in E-Mails oder Anhängen, um das Verhalten auf dem System und im Netzwerk zu analysieren (z.B. in einer virtuellen Umgebung)
- Ausführbare Dateien in einer abgeschotteten Umgebung ausführen und das Verhalten auf dem System wie auch im Netzwerk analysieren. Verifikation der Zugriffe ins Internet (Zugriff auf Malware URLs).
- Ausführen von Dateien, die über Weblinks heruntergeladen werden, Analyse des Verhaltens auf dem System wie auch im Netzwerk

7.4 Schutz vor E-Mail Spoofing

Auf den Exchange Server (oder in Exchange Online, falls M365 verwendet wird) wurden entsprechende Transport-Rules definiert, um Emails, die von ausserhalb der Organisation versendet werden und die Domäne des Partners verwenden, blockiert werden/ in Quarantäne verschoben werden.
Durch diese Konfiguration wird verhindert, dass externe Sender gefälschte Mails mit Absenderadressen, welche die Domäne des Partners imitieren, an Mitarbeitende des Partners versenden können.

7.5 Globales Adressbuch

Externe Mailadressen im globalen Adressbuch des KOMSG-Verbundes, sind mit „EXT“ gekennzeichnet. Ein E-Mail, die an eine Adresse aus dem globalen Adressbuch gesendet wird, die nicht als extern gekennzeichnet ist, verlässt den KOMSG-Verbund nur bei einer Bearbeitung über den Outlook Web Access oder aufgrund einer Datensynchronisation mit mobilen Clients.