KOM SG

Sicherheitsvorschriften KOM SG

Datum: 1. Januar 2017
Version: 5.0

In Kraft gesetzt vom Vorstand der KOM SG am 6. Dezember 2016.

St.Gallen, 6. Dezember 2016

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

KOM SG

Inhalt

1	**Einleitung**	**5**
1.1	Ziel und Zweck	5
1.2	Geltungsbereich / Zielpublikum	5
1.3	Organisatorisches Umfeld	5
1.3.1	KOM SG	5
1.3.2	Dienstanbieter und Netzbetreiber	6
1.3.3	Kunde	6
1.4	Bewilligungen	6
1.5	Ausnahmebewilligungen	6
1.6	Koordination	6
2	**Organisatorische Massnahmen**	**6**
2.1	Vorkehrungen der KOM SG	6
2.2	Verantwortung des Kunden	7
2.3	Bewältigung ausserordentlicher Lagen	8
3	**Weisung und Sensibilisierung der Benutzer**	**8**
3.1	Pflichten Verantwortlicher des Kunden	8
3.2	Allgemeine Bestimmungen	9
3.3	Zugangs- und Zugriffsschutz	9
3.4	Gebrauch von E-Mail	9
3.5	Nutzung des Internets	11
3.6	Schutz vor Malware	11
3.7	Mobile Datenträger	11
3.8	Verwendung Fernzugriff	12
3.9	Verhalten bei Sicherheitsvorfällen	12
3.10	Kontrollen, Sanktionen und Disziplinarmassnahmen	12
4	**Schutz im E-Mail Verkehr**	**13**
4.1	Postfach	13
4.2	Mengen- und Grössenbeschränkungen	13
4.3	Globales Adressbuch	13
4.4	Regelbasierte Weiterleitungen	14
4.5	Ausserordentliche Berechtigungen	14

5	**Schutz der Systeme**	**14**
5.1	Grundsätze	14
5.2	Öffentlich zugängliche Systeme	15
5.3	Passwort Richtlinien	15
5.4	Mobile Datenträger	15
5.5	Regelmässige Aktualisierung	16
5.6	Virenschutz	16
5.6.1	Grundsätze	16
5.6.2	Updates der Signaturen	17
5.6.3	Clients	17
5.6.4	Server	17
5.6.5	Ergänzender Schutz für Mailserver	17
5.6.6	Office-Makro Schutz	18
6	**Schutz des Netzwerks**	**18**
6.1	Netzwerkübergänge	18
6.2	Verbindung über Dritt-Carrier	19
6.3	Sichere Netzwerkkomponenten	20
6.4	Schutz der Netzwerkanschlüsse	20
6.5	VPN	21
6.5.1	Externe VPN Zugänge	21
6.5.2	VPN Tunnel für KOM SG Kunden/Standorte	21
6.5.3	VPN Tunnel für Applikationen/Clients	22
6.6	Einsatz von Desktop Sharing Lösungen	22
6.7	Netztrennung durch virtuelle LAN (VLAN)	22
6.7.1	Grundsätze	22
6.7.2	VLAN-Konfigurationen	23
6.8	Drahtlose Netzwerke (Wireless LAN / WLAN)	23
6.8.1	WLAN als öffentliches Netzwerk	23
6.8.2	WLAN als sicheres Netzwerk	24
6.9	Voice over IP (VoIP)	24
6.9.1	Variante 1: VoIP Kommunikation mittels Skyp 4 Business (S4B) über das KOMSG	24
6.9.2	Variante 2: VoIP Kommunikation mittels KOM SG SIP über das KOMSG	24
6.9.3	Variante 3: VoIP Kommunikation mittels Enterprise SIP (ESIP) der Swisscom	25

6.9.4 Variante 4: VoIP Kommunikation mittels Rii-Seez SIP (RSIP) des EW Buchs über das KOM SG 26
6.9.5 Variante 5: VoIP Kommunikation innerhalb des Kundennetzwerks 26

7 Schutz mittels Firewall und IDS/IPS 27
7.1 Grundsätze 27
7.2 Technischer Aufbau 29
7.3 Produkte 30
7.4 Kommunikation 30
7.4.1 Grundsätze 30
7.4.2 Dienste vom internen Netzwerk zum Internet 30
7.4.3 Dienste vom Internet zum internen Netzwerk 30
7.4.4 Netzwerktrennung zwischen dem KOMSG und dem Kundennetzwerk 31
7.4.5 Netzwerktrennung gegenüber Fremdnetzen 31
7.4.6 Testschaltungen 31
7.5 Verwaltung der Firewall-Regeln 31
7.6 Aufzeichnung, Aufbewahrung und Auswertung von Logdaten 31
7.7 System- und Betriebsdokumentation 32
7.8 Prüfung 32

8 Anhang 34
8.1 Glossar 34
9 Checklisten 37

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 Spielregeln im Umgang mit den Dienstleistungen der KOM SG, um innerhalb des KOMSG ein sicheres Umfeld gewährleisten zu können.

1.2 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 Kunde genannt. Alle Vorgaben gelten aber auch für Dienstanbieter und Netzbetreiber, welche 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 Kunden sowie deren IT-Leistungserbringer.

1.3 Organisatorisches Umfeld

1.3.1 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 Kunden 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 Kunden, Dienstanbietern und Netzbetreibern.

1.3.2 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.

1.3.3 Kunde

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

1.4 Bewilligungen

Das Anbieten von eigenen Diensten des Kunden über die Netzwerk-Infrastruktur der KOM SG[1] sowie Kommunikationsverbindungen von Kunden-Netzen zu Stellen ausserhalb des KOMSG (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.

1.5 Ausnahmebewilligungen

Auf Antrag des Kunden entscheidet die Geschäftsstelle der KOM SG über Ausnahmebewilligungen zu diesen Sicherheitsvorschriften. Im Eskalationsfall entscheidet der Vorstand der KOM SG.

Die Ausnahmebewilligungen schwächen das Sicherheitsdispositiv und werden daher mit einer Risikobewertung versehen. Die Geschäftsstelle der KOM SG führt eine gesamthafte Übersicht der Ausnahmebewilligungen. Diese wird für alle KOM SG-Kunden publik gemacht (Vertrauen durch Transparenz).

1.6 Koordination

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

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 Kunden-Netzwerks und an dessen angeschlossenen Systeme sowie der Netzwerke der

[1] z.B. Internet-Zugang für andere KOMSG Kunden

Dienstanbieter und Netzbetreiber. Die Kosten für das Audit werden von der KOM SG getragen. Ausnahmen bilden wiederholte Sicherheitsverletzungen, welche eine Nachprüfung erfordern sowie Zugänge von Dritten zum KOMSG[2].

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 Malware zu reduzieren wird beim Internetzugang der KOM SG bzw. deren Vertragspartner der Datenverkehr analysiert. Die auf das Auffinden von Malware beschränkte Inspektion betrifft den gesamten unverschlüsselten und mit wenigen Ausnahmen auch den verschlüsselten Datenverkehr. Die Inspektion des Datenverkehrs erfolgt datenschutzkonform.

Die KOM SG teilt festgestellte Missbräuche dem Verantwortlichen des Kunden mit. Missbräuchlich ist jede Verwendung der Informatikmittel, die:
a) gegen diese Sicherheitsvorschriften verstösst;
b) gegen andere Bestimmungen der Rechtsordnung verstösst.

2.2 Verantwortung des Kunden

Die Verantwortlichkeiten für die Sicherheit innerhalb der Institutionen müssen geregelt und dokumentiert sein. Jede Institution (Amtsstelle, Gemeinde, öffentlich rechtliche Anstalt, Dritte) hat einen Informatik- oder Sicherheitsverantwortlichen zu benennen und der KOM SG mitzuteilen. Dieser sorgt für die korrekte Umsetzung der vorliegenden Sicherheitsvorschriften.

Werden nicht kunden- oder kantonseigene Informatikmittel zur Aufgabenerfüllung eingesetzt, sind diese gemäss den vorliegenden Sicherheitsbestimmungen zu schützen. Die Kunden sind verpflichtet, die diesbezüglichen Rechte und Pflichten gegenüber den betroffenen Benutzern mittels einer schriftlichen Nutzungsvereinbarung zu regeln.

Es steht dem Kunden frei, die Umsetzung von Teilen oder der Gesamtheit der hier beschriebenen Vorgaben an einen IT-Leistungserbringer zu überbürden. Seitens des Kunden müssen entsprechende vertragliche Regelungen getroffen werden, welche die Einhaltung der Sicherheitsvorschriften von seinem IT-Leistungserbringer verlangen. Diese Weitergabe entbindet den Kunden nicht von der Verantwortung gegenüber der KOM SG.

Im Rahmen seiner Verantwortung ist der Kunde insbesondere für eine regelmässige Prüfung der Konformität seiner Installationen mit diesen Sicherheitsvorschriften besorgt. Die KOM SG stellt dafür entsprechende Checklisten zur Verfügung. Der Kunde ist verpflichtet seine Informationssicherheit mindestens einmal jährlich mit Hilfe dieser Checklisten zu

[2] Siehe Reglement für den Zugang von Dritten zum KOMSG vom 13. September 2007

überprüfen und das Ergebnis der KOM SG mitzuteilen[3]. Die KOM SG wertet diese aus und leitet notwendige Korrekturen oder Sanktionen ein.

2.3 Bewältigung ausserordentlicher Lagen

Der Verantwortliche des Kunden 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 Malware verantwortlich. Sie haben sämtliche ihnen zur Verfügung stehenden Mittel bereitzuhalten und anzuwenden, damit sich zum Beispiel die Malware 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 Kunden 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 Weisung und Sensibilisierung der Benutzer

3.1 Pflichten Verantwortlicher des Kunden

Zur Gewährleistung des sicheren Einsatzes der Informatikmittel müssen alle Benutzer wissen, welche Sicherheitsaspekte sie zu beachten und zu befolgen haben. Dazu hat der Verantwortliche des Kunden sicherzustellen, dass alle Benutzer durch eine Weisung zur Umsetzung von Sicherheitsmassnahmen verpflichtet sind, und wie in den Allgemeinen Geschäftsbedingungen Absatz B. 1 definiert, durch mindestens halbjährlich wiederkehrende Information auf den sicheren Umgang mit Daten und die dazu notwendigen Vorkehrungen hingewiesen werden. Wo immer möglich, sind die Benutzer durch technische Hilfsmittel bei ihrer täglichen Umsetzung der Sicherheitsmassnahmen zu unterstützen.

Die Weisung der Benutzer muss mindestens die folgenden Sicherheitsaspekte und Rahmenbedingungen beinhalten[4]:

[3] Treffen alle der nachfolgenden Kriterien zu, ist der Kunde von dieser Verpflichtung befreit. Kriterien sind: Sämtliche Endsysteme werden innerhalb des APZ betrieben, das lokale Netzwerk ist in Verantwortung des von der KOM SG beauftragten Netzwerkbetreibers, es bestehen keine Übergänge zu Drittnetzen.

[4] Die aufgeführten Sicherheitsmassnahmen beschränken sich auf KOMSG-relevante Aspekte. Ein Beispiel einer umfassenden Weisung ist die kantonale Dienstanweisung über Einsatz und Verwendung von Informatikmitteln.

3.2 Allgemeine Bestimmungen

Geltungsbereich
Die Weisung muss für alle Benutzer im Netzwerk des Kunden gelten.

Nutzung der Informatikmittel
Die Benutzer sind auf die Verantwortung zum gesetzmässigen, zweckmässigen und verhältnismässigen Einsatz von Informatikmitteln aufmerksam zu machen. Die private Nutzung der kundeneigenen Informatikmittel, sowie das Verwenden nicht kundeneigener Informatikmittel am Netzwerk des Kunden sind abschliessend zu regeln.

Handhabung von Informationen
Die Bearbeitung, Speicherung und Weitergabe schützenswerter Daten muss geregelt sein. Unter Berücksichtigung des geltenden Datenschutzgesetzes sind insbesondere die Massnahmen zum korrekten Umgang mit Personendaten sowie die Datenablage und Datensynchronisation mit sogenannten Cloud Services zu definieren.

3.3 Zugangs- und Zugriffsschutz

Schutz der Arbeitsstationen und Netzwerkanschlüsse
Arbeitsstationen und Netzwerkanschlüsse sind durch das Abschliessen der Türe beim Verlassen des Raumes vor unberechtigtem Gebrauch zu schützen. Die Benutzer sind ferner darauf hinzuweisen, dass die Arbeitsstationen beim Verlassen des Arbeitsplatzes gesperrt (Windows Taste + L) werden müssen.

Sicherer Umgang mit Passwörtern
Die Anforderungen an starke Passwörter sind, gestützt auf die technisch erzwungenen Vorgaben der Systeme, zu definieren und kommunizieren. Die Benutzer sind zu instruieren wie starke und einfach merkbare Passwörter erzeugt werden können und wie diese korrekt anzuwenden sind.

Zugang für Dritte
Es sind Verhaltensregeln im Umgang mit nicht autorisierten Personen zu definieren. Dabei sind den Benutzern die Absichten, Möglichkeiten und Vorgehensweisen im Zusammenhang mit Social Engineering aufzuzeigen.

3.4 Gebrauch von E-Mail

Schutz sensitiver Daten
Die Benutzer müssen informiert sein, dass E-Mails beim Versenden über das Internet standardmässig nicht vor unberechtigter Einsicht oder vor Fälschung geschützt sind. Den Benutzern muss klar sein, dass das Versenden von sensitiven Daten in ihrer Verantwortung liegt. Verfügbare technische Hilfsmittel für die sichere Übertragung schützenswerter Daten sind den Benutzern aufzuzeigen. Dabei ist auch der Umgang beim Empfang von verschlüsselten und/oder signierten E-Mails zu berücksichtigen.

Grössenbeschränkung
Der E-Mail-Dienst ist kein Werkzeug um grosse Datenmengen zu streuen/verteilen. Die Benutzer sind darauf hinzuweisen, dass grosse Dateien die innerhalb des gleichen Amtes oder der gleichen Gemeinde zugänglich gemacht werden müssen, auf Datenserver abgelegt werden und als Link in einer E-Mail-Nachricht versendet werden können.

Verteilerlisten
Weil Verteilerlisten und –gruppen wiederum andere Gruppen beinhalten können, sollen nur bekannte Verteiler angewählt und verwendet werden. Es besteht sonst die Möglichkeit, dass eine E-Mail unkontrolliert verbreitet wird.

Globales Adressbuch
Es ist untersagt, das globale Adressbuch zu exportieren und an Dritte weiterzuleiten.

Spam-Mails (unerwünschte Werbemails)
Die Benutzer sind über die persönlichen Vorkehrungen im Zusammenhang mit Spam-Mails zu informieren. Es ist untersagt, SPAM-Mails zu versenden. Es ist ebenso untersagt, SPAM-Mails zu beantworten oder weiterzuleiten. Wird ein Benutzer immer wieder von Spams belästigt, so kann er diese Mails in die so genannte Junk-Mail-Liste seines Mail-Clients aufnehmen. Sollten viele User vom gleichen Spam betroffen sein, so ist beim Informatik- oder Sicherheitsverantwortlichen die zentrale Sperrung zu beantragen[5]. E-Mail-Adressen sollen nur bei vertrauenswürdigen Seiten und im Rahmen der dienstlichen Aufgabenerfüllung auf Internetseiten eingetragen werden.

Befolgen von Warnungen
Warnungen der Informatik- und Sicherheitsverantwortlichen sowie der KOM SG oder seinem Dienstanbieter vor E-Mails mit bestimmten Inhalten (Betreff, Text) sind zu beachten und entsprechende E-Mails sind ohne Öffnen sofort zu löschen.

Outlook Web Access
Beim Outlook Web Access werden die Postfachinhalte verschlüsselt übertragen und sind somit auf dem Übertragungsweg nicht lesbar. Sobald E-Mails und Attachements aus dem Outlook Web Access auf einer lokalen Arbeitsstation abgespeichert werden, sind diese in der Regel nicht mehr verschlüsselt. Die Benutzer müssen über diesen Sachverhalt und den entsprechend umzusetzenden Schutzvorkehrungen informiert sein.

Private E-Mails und E-Mail-Archivierung
Wer die E-Mail-Archivierung abonniert hat, informiert seine Benutzer über die Massnahmen im Zusammenhang mit privaten E-Mails. Diese sind vor der Archivierung zu löschen oder in den Ordner "Keine Archivierung" zu verschieben.

[5] Bezüger des KOMSG Exchange-Dienstes können via Service Desk Ticket die Sperrung bei Abraxas beantragen.

3.5 Nutzung des Internets

Elektronische Medien und Groupware
Elektronische Medien (wie Internet - Radio, Video oder Newsletter) und Groupware (wie Instant Messaging, Foren oder Chatrooms) dürfen nur für dienstliche Zwecke genutzt werden.

Herunterladen und Installieren von Programmen und Programm-Updates
Das selbstständige Herunterladen sowie das Installieren von Programmen und Programm-Updates sind untersagt.

Unzulässige Zugriffe
Unzulässig ist der Zugriff auf Websites mit:
a) erotischem, pornografischem oder sexistischem Inhalt;
b) rassistischem oder gewaltverherrlichendem Inhalt;
c) Inhalten, die sonst wie gegen die guten Sitten verstossen.
Ausgenommen sind Zugriffe, wenn sie zur Erfüllung der dienstlichen Aufgaben notwendig sind.

Private Nutzung
Die private Nutzung des Internets am Arbeitsplatz ist zurückhaltend auszuüben.

3.6 Schutz vor Malware

Grundsätze
Die Schutzmassnahmen dürfen weder ausgeschaltet noch umgangen oder unwirksam gemacht werden. Die Benutzer sind verpflichtet bei Verdachtsfällen ihren Informatik- oder Sicherheitsverantwortlichen umgehend über die Feststellungen zu informieren.

Verdächtige E-Mails
E- Mails von unklarer Herkunft oder mit unüblichen Betreffvermerken sowie suspekte Anhänge und Links dürfen nicht geöffnet werden. Im Zweifelsfall ist die gesamte E-Mail unverzüglich und definitiv im "Posteingang" sowie in den Ordnern "Gelöschte Objekte" und "Gelöschte Elemente wiederherstellen" zu löschen.

3.7 Mobile Datenträger

Schutz sensitiver Daten
Müssen schützenswerte Daten auf mobilen Datenträgern (CDs/DVDs, Memory-Sticks, Notebooks, Tablet-PCs, Smartphones etc.) abgespeichert werden, hat dies jeweils verschlüsselt zu erfolgen. Die Benutzer müssen über die entsprechenden Mittel und das notwendige Wissen zur Handhabung dieser Mittel verfügen.

Smartphones und Tablet-PCs
Bei der Installation von Apps ist Zurückhaltung gefordert. Die Benutzer müssen die bei einem Diebstahl und dem Verlust der Geräte einzuleitenden Massnahmen wie das Remote-Wiping oder das Sperren der SIM-Karte kennen und anwenden können.

3.8 Verwendung Fernzugriff

Zertifikatswarnung
Die Benutzer müssen wissen, dass beim Auftreten einer Zertifikatswarnung die Verbindung zum VPN-Dienst, dem Outlook Web Access (OWA) oder dem Exchange ActiveSync der KOM SG vor Eingabe des Passworts beziehungsweise vor Übermittlung der Zugriffsberechtigung abgebrochen werden muss.

VPN-Zugang
Bei vorhandener Virenmeldung auf einem System ist es untersagt, sich mit diesem über einen Fernzugriff in das KOMSG oder das Netzwerk des Kunden einzubinden.

Desktop Sharing
Desktop Sharing Lösungen sind nur temporär und nur durch die vom Informatikverantwortlichen bestimmten Benutzern einzusetzen. Diese müssen über Kenntnisse und Anweisungen zur Nutzung von Steuerungs- sowie Kontrollmöglichkeiten des eingesetzten Produktes verfügen. Die Benutzer sind verpflichtet bei Missbrauchsverdacht die Verbindung sofort abzubrechen und den Informatik- oder Sicherheitsverantwortlichen über den Vorfall zu informieren.

3.9 Verhalten bei Sicherheitsvorfällen

Informationswege und Eskalationsstufen
Die Benutzer müssen wissen, wie sie sich beim Auftreten von Sicherheitsvorfällen, zum Beispiel bei einem Verdacht auf Passwortmissbrauch oder einem vermuteten Befall eines Systems durch Malware, zu verhalten haben.

3.10 Kontrollen, Sanktionen und Disziplinarmassnahmen

Information
Hinweise zu den Kontrollmassnahmen und der Meldung von Missbräuchen wie auch den Sanktionen bei Verstössen gegen Sicherheitsvorschriften sind, abgestützt auf die Gegebenheiten des Kunden zu definieren und in der Nutzungsvereinbarung mit den Benutzern konkret zu erwähnen.

Bestätigung
Die Benutzer müssen einmalig pro Version bestätigen, dass sie die sie betreffenden Weisungen verstanden haben und sie mit den Überwachungs- und Disziplinarmassnahmen vertraut sind.

4 Schutz im E-Mail Verkehr

4.1 Postfach

Ein Postfach und dessen Inhalt sind immer einem Benutzer als Inhaber zugeteilt. Standardmässig darf nur der Inhaber des Postfaches auf dieses Zugriffsberechtigung erhalten. Nur der Inhaber des Postfachs darf eine Veränderung der Berechtigungen oder Um- / Weiterleitung veranlassen bzw. anderen Mitarbeitern Berechtigungen auf die verschiedenen Ordner des eigenen Postfaches erteilen.

Auch bei unpersönlichen Postfächern, wie Ressourcen- oder Gruppenpostfächer muss mindestens eine Person oder eine Organisation als Inhaber eingetragen werden. Die Konfiguration der Postfächer ist so vorzunehmen, dass ausschliesslich diese Inhaber Berechtigungen ändern oder Mutationsaufträge auslösen darf.

Der Zugriff auf ein Postfach ist über eine einfache Authentifizierung (Benutzername und Passwort) zu steuern. Als Mindestanforderungen gelten dabei die Passwort Richtlinien gemäss Kapitel 5.3.

4.2 Mengen- und Grössenbeschränkungen

Es ist untersagt über den E-Mail-Dienst grosse Datenmengen zu übermitteln und E-Mails mit grosser Anzahl an Empfängern zu versenden. Demzufolge ist bei der zentralen KOM SG-Maildrehscheibe die maximale Empfängeranzahl pro E-Mail auf 200 Adressaten eingeschränkt. E-Mails über 20 MB werden nicht angenommen und von der zentralen KOM SG-Maildrehscheibe zurückgewiesen.

Auf jedem Mailserver im KOMSG-Verbund muss die maximale Mailgrösse von 20 MB und die maximale Empfängeranzahl pro E-Mail auf 200 Adressaten eingestellt werden.

4.3 Globales Adressbuch

Externe Mailadressen im globalen Adressbuch des KOMSG-Verbundes, sind mit „EXT“ gekennzeichnet. Ein E-Mail, welches 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.

Muss aus einem bestimmten Grund auf einem dezentralen Exchange Server (Server Variante C) eine externe E-Mail-Adresse erfasst werden, so ist diese mit xxxxx EXT entsprechend zu kennzeichnen. Dasselbe gilt für eine Verteilergruppe, in der sich eine solche externe Adresse befindet. Die Verteilergruppe ist mit V-xxxxx EXT zu kennzeichnen.

Externe E-Mail-Adressen sowie Verteilergruppen werden nicht repliziert und sind nur auf demjenigen Server sichtbar, auf dem sie erstellt wurden.

4.4 Regelbasierte Weiterleitungen

Die automatische Weiterleitung von E-Mails von einer Adresse im KOMSG-Verbund auf eine externe Adresse ist bei zentral betriebenen Postfächern unterbunden.

Automatische Weiterleitungen auf externe Postfächer sind auf den dezentralen Exchange-Servern der Kunden ebenfalls technisch zu unterbinden.

4.5 Ausserordentliche Berechtigungen

Ist es notwendig, Änderungen der Berechtigung, wie beispielsweise Zugriffe auf Postfächer oder Weiterleitungen von E-Mails bei Abwesenheiten des Inhabers durchzuführen, so hat dies unter Berücksichtigung der Datenschutzbestimmungen und aufgrund eines schriftlichen Auftrags an die ausführende Stelle zu geschehen.

5 Schutz der Systeme

5.1 Grundsätze

Ein System ist definiert als eine Einheit, die Anwendungen und Operationen ausführt, Daten speichert oder ausgibt und Zugriffsrechte auf ihre Daten regeln kann. Beispiele von Systemen sind Hosts, Server, Clients sowie Multifunktions- und Drucksysteme. Als Clients gelten PCs, Notebooks, Tablet-PCs, IP-Telefone und Smartphones. Explizit nicht unter den Begriff Systeme fallen Firewalls und Netzwerkkomponenten.

Ein System ist genau einem Netzwerk zugeordnet. Ausnahme dieser Regel ist, wenn ein physisches System mehrere logische Systeme beinhaltet. Garantieren die eingesetzten Technologien eine vollständige Trennung zwischen den logischen Systemen und ist sichergestellt, dass jedes logische System nur mit einem bestimmten Netz kommunizieren kann, so darf ein physisches System auch mehreren Netzen zugeordnet werden.

Ein System ist mindestens durch die folgenden Angaben definiert:

- Name des Systems
- Systemverantwortlicher

Damit ein System innerhalb des KOMSG betrieben werden darf bzw. über das KOMSG kommunizieren darf, muss es mindestens die folgenden Anforderungen erfüllen:

- Das System muss auf die Belange der im vorliegenden Dokument definierten Vorgaben und im Beisein eines Kundenverantwortlichen auditierbar sein
- Das System darf keine Erweiterung des Netzwerks zulassen
- Wird das System temporär auch an andere Netzwerke als das KOMSG angeschlossen werden, beispielsweise Notebooks, muss es mit einer aktiven Personal Firewall ausgestattet sein
- Das Serversystem wird bei der Installation gehärtet, das heisst
  - Auf dem System darf nur Software installiert sein, die wirklich benötigt wird
  - Auf dem System sind lediglich notwendige Dienste installiert und aktiviert

5.2 Öffentlich zugängliche Systeme

Öffentlich zugängliche Systeme mit einem Anschluss an das KOMSG, beispielsweise in Bibliotheken, müssen so konfiguriert sein, dass die Benutzer der Systeme nur minimale Rechte haben. Nur die wirklich notwendigen Dienste dürfen installiert sein, es darf für Benutzer nicht möglich sein, zusätzliche Programme zu installieren oder Programme ab mitgebrachten Datenträgern zu starten.

5.3 Passwort Richtlinien

Sämtliche Systeme[6] sind vor Inbetriebnahme so zu konfigurieren, dass für jedes Benutzer- und Administratorenkonto die verwendeten Passwörter mindestens den folgenden Anforderungen entsprechen:

- Länge von mindestens 8 Zeichen
- Passwort muss aus Gross- und Kleinbuchstaben, mindestens einer Zahl und einem Sonderzeichen bestehen
- Maximale Gültigkeit eines Passwortes ist 90 Tage[7]
- Letzte 10 Passwörter dürfen nicht wiederverwendet werden
- Sperrung des Benutzerkontos nach 10-maliger Fehleingabe

Mit technischen Mitteln ist sicherzustellen, dass diese Mindestanforderungen zwingend umgesetzt und durch die Benutzer nicht veränderbar sind.

5.4 Mobile Datenträger

Der Gebrauch von mobilen Datenträgern ist durch technische Hilfsmittel möglichst stark zu schützen. Werden schützenswerte Daten abgespeichert, sind diese auf dem Speichermedium zu verschlüsseln. Beim dienstlichen Einsatz von Smartphones und mobilen Arbeitsstationen (Notebooks, Tablet-PCs) ist der Passwortschutz zwingend.

Der Datenabgleich und die Steuerung der Sicherheitsfunktionen haben bei Smartphones und Tablet-PCs über einen zentralen Zugangspunkt zu erfolgen. Mindestens zu berücksichtigende Einstellungen sind:

- Das Gerätekennwort ist aktiviert, die minimale Kennwortlänge ist 4 Zeichen
- Nach maximal 10 Minuten Inaktivität (ohne Benutzereingabe) wird das Gerät automatisch gesperrt
- Nach maximal 10 fehlerhaften Kennworteingaben werden alle auf dem Gerät enthaltenen Daten gelöscht
- Der Datenabgleich sowie die Speicherkarte und das Datenbackup sind verschlüsselt

Es gilt zu beachten, dass nicht alle Geräte die über den zentralen Zugangspunkt gesteuerten Einstellungen übernehmen, teilweise sogar ignorieren.

[6] Ausgenommen sind Smartphones und Tablet-PCs mit Datenabgleich über zentralen Zugangspunkt
[7] Gilt nicht für technische Accounts sowie Service-Accounts

Die bei einem Diebstahl und dem Verlust der Geräte vorzukehrenden Massnahmen sind zu definieren. Bei Smartphones und Tablet-PCs muss die Möglichkeit zum Löschen der Daten mittels Remote-Wiping vorhanden sein[8].

Bei Synchronisationslösungen über eine spezifische App gelten die Vorgaben sinngemäss auf Ebene dieser App.

Privat beschaffte Geräte unterliegen den gleichen Anforderungen.

5.5 Regelmässige Aktualisierung

Das Patch-Management dient der regelmässigen Aktualisierung der Software, indem die Verbesserungen der Hersteller eingespielt werden. Im Vordergrund stehen Aktualisierungen welche Sicherheitsmängel beheben. Security-Patches müssen laufend, jedoch mindestens wöchentlich auf den Systemen installiert werden. Service Packs sind monatlich, jedoch spätestens ab dem Zeitpunkt wo zusätzliche Sicherheitsfunktionen vorhanden sind oder wo der Hersteller angekündigt hat keine Security-Patches für den bereits installierten Service Pack mehr anzubieten, zu installieren.

Das Patch-Management betrifft Systemprogramme und Anwendungen. Zu berücksichtigen sind insbesondere:

- Betriebssysteme und deren Hilfsprogramme (z.B. Dateimanager, Rechner, etc.)
- Gerätertreiber
- Virenschutz
- Internet-Browser inklusive installierter Erweiterungen (Add-ons, Plugins, etc.)
- Mail-Client
- Office-Umgebung (Word, Excel, etc.)
- PDF-Reader

Ist ein Update nicht möglich (z.B. nicht kompatibel mit anderer installierter Software) müssen entsprechend der Bedrohung geeignete Massnahmen (temporäre Konfigurationsänderungen, Deaktivierung von Diensten bis hin zur Trennung vom Netz) getroffen werden, um Computersysteme und das ganze KOMSG trotzdem ausreichend zu schützen.

5.6 Virenschutz

5.6.1 Grundsätze

Sämtliche Amtsstellen, Gemeinden und sonstigen Institutionen, welche Netzdienste der KOM SG beziehen, haben ihre Systeme mit einem Schutz vor Malware gemäss den nachfolgenden Kapiteln auszurüsten. Dabei müssen alle Clients wie PCs, Notebooks, Tablet-PCs als auch alle Server berücksichtigt sein. Sofern technisch machbar, sind auch IP-Telefone und Smartphones mit einem Virenschutz auszurüsten.

[8] Bezüger des Exchange-Dienstes, Variante A können dies via Service Desk Ticket bei Abraxas veranlassen.

Alle Kunden der KOM SG sind selbst für den Virenschutz verantwortlich und haften in Anlehnung der Allgemeinen Geschäftsbedingungen Absatz H für Schäden, welche durch eine von ihnen verursachte Virenverbreitung entstehen.

5.6.2 Updates der Signaturen

Die zentralen Virenschutzsysteme sowie die Systeme in der DMZ (z.B. Webserver, Mailserver) müssen so konfiguriert werden, dass die regelmässige Abfrage auf dem Server des Herstellers für die neuste Signatur mindestens stündlich vorgenommen wird. Kann das Virenschutzprogramm nicht für ein stündliches Update konfiguriert werden, muss das kürzeste verfügbare Zeitintervall eingestellt werden.

Die Verteilung der neusten Signatur auf Endgeräte innerhalb des Kundennetzwerks muss anschliessend innerhalb des kürzest möglichen Zeitintervalls erfolgen.

Mobile Arbeitsplätze sind so zu konfigurieren, dass sie die Signatur direkt vom Server des Herstellers aktualisieren, sofern sie nicht am Kundennetzwerk angeschlossen sind.

5.6.3 Clients

Das Schutzprogramm gegen Malware muss so konfiguriert werden, dass sämtlicher Datenverkehr auf dem Endgerät überwacht wird. Im Schutzprogramm ist „autoprotect“ und „realtime scan“ zu aktivieren. Sämtliche mobilen Datenträger, wie USB-Medien, CD/DVD etc. müssen vor dem Gebrauch ebenfalls automatisch auf Viren überprüft werden. Einmal pro Monat sind alle Dateien jedes Clients auf Malware zu überprüfen.

Die Benutzerrechte müssen so eingeschränkt werden, dass die Benutzer die Konfiguration des Schutzprogrammes weder verändern noch deaktivieren können.

Das Schutzprogramm muss so konfiguriert werden, dass nach einem Neustart des Clients oder nach einem Loginwechsel des Benutzers der Virenschutz automatisch aktiviert wird.

5.6.4 Server

Das Schutzprogramm muss so konfiguriert werden, dass sämtlicher Datenverkehr auf dem System überwacht wird. Im Schutzprogramm ist „autoprotect“ und „realtime scan“ zu aktivieren. Alle Daten auf den Servern müssen mindestens einmal pro Woche auf das Vorhandensein von Malware überprüft werden.

Das Schutzprogramm muss so konfiguriert werden, dass nach einem Neustart des Servers oder nach einem Loginwechsel des Benutzers/Administrators der Virenschutz automatisch aktiviert wird.

5.6.5 Ergänzender Schutz für Mailserver

Bei Mailservern und -drehscheiben ist nebst dem Schutzprogramm für Fileserver auch ein expliziter Schutz vor Malware, unerwünschter Software und Spams einzusetzen. Dabei müssen alle ein- und ausgehenden E-Mails inklusive deren Anhänge, unabhängig des Absenders, überprüft werden.

Malware in verschlüsselten E-Mails oder Dateien können durch ein Virenschutzprogramm nicht erkannt werden. Sämtliche entschlüsselten E-Mails und Attachements müssen vor Gebrauch auf Malware überprüft werden.

5.6.6 Office-Makro Schutz

Die Microsoft Office Produkte (vornehmlich Word und Excel) müssen so konfiguriert sein, dass Makros nicht automatisch ausgeführt werden können. Der Benutzer muss somit die Makros bewusst aktivieren.

Idealerweise werden Makros allerdings generell deaktiviert, oder nur signierte Makros zugelassen.

6 Schutz des Netzwerks

6.1 Netzwerkübergänge

Das Netzwerk der KOM SG, das KOMSG, wird auch als Verwaltungsnetz bezeichnet. Das KOMSG ist in logische Netze unterteilt. Zentrale Netzwerkübergänge steuern die Kommunikation zwischen den logischen Netzen, zu den verschiedenen Rechenzentren, zu Drittnetzen wie beispielsweise dem bundesweiten Kommunikationsnetz KOMBV/KTV und zum Internet. Von der KOM SG beauftragte Dienstanbieter und Netzbetreiber stellen ihrerseits eine korrekte sowie sichere Umsetzung der zentralen Netzwerkübergänge sicher.

Wird ein Netzwerk transparent (ohne Filtermechanismen) mit dem KOMSG verbunden, entspricht dies einer Erweiterung des Verwaltungsnetzwerks (siehe Abbildung 1 Kunde). Der Kunde ist verpflichtet über keine weiteren Netzwerkübergänge zu verfügen und innerhalb seines Netzwerkes ausschliesslich verwaltungsbezogene Systeme bzw. Systeme mit einem KOMSG entsprechenden Sicherheitsniveau zu betreiben.

Verfügt ein Kunde über einen eigenen Zugang zum Internet oder/und über Netzwerkverbindungen ausserhalb der Verwaltung (z.B. Schulnetz, Spitex, etc.), nachfolgend Fremdnetz genannt, ist das KOMSG vom Netzwerk des Kunden wie auch das Netzwerk vom Kunden zum Internet und den Fremdnetzen zwingend durch eine Firewall abzutrennen (siehe Abbildung 1, LAN Kunde B).

Falls der Kunde einen eigenen Zugang zum Internet hat, muss zwingend eine Firewall zwischen KOMSG und Netzwerk des Kunden implementiert werden. Diese Firewall wird von der KOM SG implementiert und betrieben und regelt ausschliesslich den Verkehr von und zum KOMSG – Netz und kann nicht für andere Zwecke (zum Beispiel direkter Internetzugang) verwendet werden. Die Kosten werden durch den Kunden getragen.

Der Kunde ist verantwortlich für die Installation und den Betrieb einer Firewall zwischen dem Netzwerk des Kunden und dem Internet, sowie allfälligen Fremdnetzen. Nebst den in den nachfolgenden Abschnitten erläuterten Sicherheitsvorkehrungen sind die folgenden Zusatzmassnahmen umzusetzen:

- Die Installation und der Betrieb der Firewall System(e) muss gemäss den Vorgaben in Kapitel 7 erfolgen
- Im Netzwerk des Kunden erfolgt eine physikalische oder logische Netzwerktrennung, die logische Trennung ist mittels VLAN und gemäss Kapitel 6.7 realisiert
- Eine unabsichtliche Kopplung getrennter Netzwerke ist durch Massnahmen wie beispielsweise einer örtlichen Trennung der Netzwerkkomponenten (wo physisch getrennt) oder einer farblichen Unterscheidung der verwendeten Patchkabel (wo physisch oder logisch getrennt) grösstmöglich zu verhindern.
- Der Kunde führt eine Dokumentation aller Netzwerkübergänge in Fremdnetze und kann diese auf Verlangen vorweisen
- Alle Drittnetzverbindungen sind von der KOM SG genehmigen zu lassen

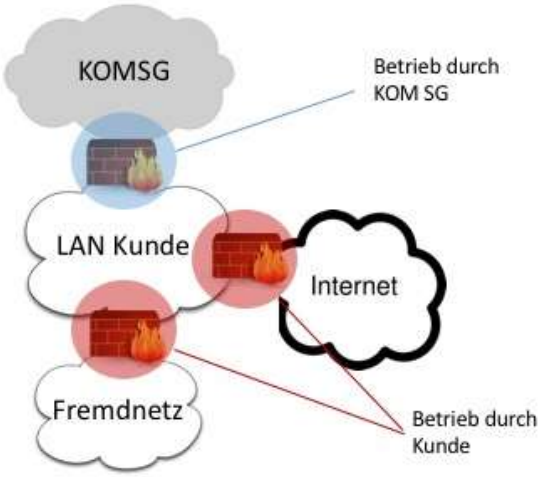

Abbildung 1: Schutz des KOMSG vor fremden Netzwerken mit KOM SG Firewall

6.2 Verbindung über Dritt-Carrier

Werden zwei Teile des KOMSG, beispielsweise zwei Standorte eines Kunden, miteinander durch einen Dritt-Carrier verbunden, so gilt dies nicht als Netzwerkübergang, falls das KOMSG dabei von anderen Netzwerken getrennt bleibt.

Die Trennung kann wie folgt erreicht werden:

- Der Dritt-Carrier stellt die Abgeschlossenheit des Netzwerkes durch geeignete Mittel sicher, beispielsweise durch den Einsatz von MPLS-VPNs, einem optischen Wellenlängenmultiplexverfahren wie DWDM (Dense Wavelength Division Multiplex), einer direkten Fiber- oder Mietleitung.

- Die Verbindung wird durch einen VPN-Tunnel über das Internet aufgebaut, sie ist entsprechend zu authentisieren und zu verschlüsseln.

Verbindungen zwischen mehreren Standorten eines Kunden durch einen Dritt-Carrier sind der KOM SG vor Inbetriebnahme mitzuteilen.

6.3 Sichere Netzwerkkomponenten

Die Netzwerkkomponenten (Switch, WLAN, Router, Firewall) müssen so installiert werden, dass der physische Zugang nur für Berechtigte möglich ist. Der unberechtigte logische Zugriff zu den Netzwerkkomponenten ist durch folgende Massnahmen wirksam zu verhindern:

- Komplexe Passwörter mit mindestens 12 Zeichen
- Keine Standard Passwörter und SNMP-Einstellungen
- Kein Einsatz von SNMP Version 1, nach Möglichkeit SNMP Version 3 mit aktivierten Sicherheitsmechanismen verwenden
- Einschränken der darauf zugreifenden Endgeräte, entweder durch die Konfiguration von Filterlisten (auch Access Lists genannt) oder durch das Verwenden eines dedizierten Management-VLANs
- Bei WLAN-AccessPoints und Firewall Systemen erfolgt der logische Zugriff ausschliesslich vom internen Netzwerk her
- Verwenden von sicheren Kommunikationsprotokolle wie ssh oder https, deaktivieren unsicherer Protokolle wie telnet oder http
- Wo IPv6 nicht eingesetzt wird, ist das Protokoll mitsamt seinen Diensten zu deaktivieren.

Die Firmware/Software der Netzwerkkomponenten ist regelmässig zu aktualisieren. Im Vordergrund stehen dabei Aktualisierungen welche Sicherheitsmängel beheben. Diese sind spätestens einen Monat nach Herausgabe durch den Hersteller zu installieren.

Ergänzende Sicherheitsfunktionen zum Schutz vor Netzwerkangriffen sind, wo von den Netzwerkkomponenten unterstützt, zu implementieren. Beispiele sind die Einschränkung der Anzahl erlaubten MAC-Adressen pro Port zur Verhinderung von MAC-Flooding sowie MAC-Spoofing Attacken und herstellerbezogene Konfigurationen zum Schutze der DHCP-Server oder dem Verhindern von ARP-Spoofing Attacken (benutzt für man-in-the-middle Attacken).

Falls Konfigurations-Dateien einzelner Systeme extern abgelegt werden, so müssen diese vor unberechtigter Veränderung wirksam geschützt werden.

6.4 Schutz der Netzwerkanschlüsse

Aktive Netzwerkanschlüsse sollen nur vorhanden sein, wo diese benutzt werden. Nicht dauernd benutzte Anschlüsse sind auf ein Minimum zu reduzieren und unbenutzte Netzwerkanschlüsse sind zu deaktivieren. Wo sich Netzwerkanschlüsse ausserhalb kontrollierter Räumlichkeiten befinden, sind diese mindestens mit der Konfiguration eines MAC-Filters, besser mit der Implementation einer Netzwerkauthentifikation basierend auf 802.1x vor unberechtigtem Zugang zu schützen. Die Konfiguration muss vorsehen, dass beim

Anschluss von fremden Systemen entweder der Netzwerkanschluss oder der Datenfluss automatisch gesperrt wird.

6.5 VPN

6.5.1 Externe VPN Zugänge

Ein VPN-Zugang zum KOMSG und dem Netzwerk des Kunden wird grundsätzlich durch die KOM SG bzw. deren Vertragspartner[9] angeboten. Hat der Kunde das Bedürfnis eine eigene Lösung zu betreiben müssen dabei die folgenden Grundsätze befolgt werden:

- Es wird ein VPN Produkt mit aktueller Technologie, basierend auf IPSec oder SSL, verwendet. Der VPN Tunnel muss auf der Firewall oder einem dedizierten System in der DMZ des Kunden terminiert werden.
- Bei aktivem VPN-Zugang ist das anrufende System vor unberechtigtem Zugriff aus dem Internet und den Fremdnetzen geschützt (kein split tunneling).
- Im Fall eines VPN-Zugangs durch einen Benutzer muss für den Aufbau eines VPN-Tunnels eine Zwei-Faktor Authentisierung eingesetzt werden. Die benutzten Berechtigungsnachweise (Benutzername/Passwort, Zertifikat, etc.) sind eindeutig dem Benutzer zugeordnet.
- Im Fall eines VPN-Zugangs durch ein System muss sich für den Aufbau des VPN-Tunnels ein Prozess (z. B. im Batchbetrieb) authentifizieren. Die benutzten Berechtigungsnachweise sind eindeutig nur diesem Prozess resp. dem anrufenden System zugeordnet.
- Die für den Aufbau eines VPN-Tunnels benötigten Berechtigungsnachweise sind nur mit grossem Aufwand zu erraten und auf den dezentralen Systemen vor unberechtigtem Zugang geschützt.
- Die authentifizierte Kommunikation wird durch die Firewall bzw. dem dedizierten System in der DMZ nach einer definierten Lebensdauer, maximal acht Stunden, terminiert.
- Die Rechte und Pflichten der Benutzer sind mittels einer Nutzungsvereinbarung geregelt, siehe auch organisatorische Massnahmen Kapitel 2.2.

6.5.2 VPN Tunnel für KOM SG Kunden/Standorte

Grundsätzlich sind direkte VPN Tunnels innerhalb des KOM SG verboten, wenn sie dem Zweck dienen Verbindungen zwischen einzelnen Kunden oder zwischen Kunden und internen oder externen Rechenzentren aufzubauen. Vor allem wenn der Tunnel dazu dient die gesamte Kommunikation eines KOM SG-Kunden 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 Kunden benötigt.

[9] Zum heutigen Zeitpunkt ist dies die Abraxas Informatik AG

Die Gründe für ein Verbot der oben erwähnten VPN Tunnels sind wie folgt:

- Die meisten Tunneltechnologien verschlüsseln die komplette Kommunikation. Somit ist die Kommunikation innerhalb des Tunnels für das KOM SG nicht ersichtlich und kann somit von den eingesetzten Sicherheits-Netzkomponenten (Firewalls, Security-Monitoring, etc.) nicht analysiert werden.
- Das bestehende Routingkonzept der KOM SG und SIK wird nicht eingehalten oder wird ausgehebelt. Dies kann im Betreib und bei Störungen zu Problemen bei der Störungsbehebung führen.
- Beim Kunden muss zusätzlich Hardware (Router, Firewall) installiert werden. Dies setzt ein gewisses Knowhow des Kunden voraus.
- Das KOM SG Netzwerk muss unter Umständen angepasst werden (Bandbreite).

6.5.3 VPN Tunnel für Applikationen/Clients

VPN Tunnels welche zur Verschlüsselung einzelner Applikationen dienen (z.B. https, Sftp, etc.) oder Applikationen welche zur Verschlüsselung der gesamten Kommunikation eines einzelnen Clients dienen (VPN Client, Anyconnect, etc.) sind indes erlaubt.

6.6 Einsatz von Desktop Sharing Lösungen

Fernzugriffe über Desktop Sharing Produkte sind in jedem Fall mit starker Authentifikation, sicherem Kommunikationsprotokoll und vom Dateneigentümer kontrolliert einzusetzen. Als kontrolliert gilt: die Applikation bzw. dessen Dienst ist nur aktiv wenn benötigt und die Steuerungs- sowie Kontrollmöglichkeiten des eingesetzten Produktes werden beim Verbindungsaufbau wie auch während dem laufenden Fernzugriff vollumfänglich genutzt.

6.7 Netztrennung durch virtuelle LAN (VLAN)

6.7.1 Grundsätze

Die Trennung von verschiedenen Netzen muss nicht zwingend physikalisch erfolgen. Durch den Einsatz von virtuellen LANs (VLANs) kann eine logische Trennung erreicht werden.

Die Trennung von Netzwerken mittels VLAN soll jedoch nur in einer verantwortbaren Umgebung verwendet werden. Das heisst innerhalb eines Netzwerkes, welches durch den Kunden oder dessen IT-Leistungserbringer betrieben wird. Die Übergänge von einem VLAN zu einem anderen müssen durch den Einsatz eines Routers, allenfalls mit Filterfunktionen, gezielt und wo gewünscht geschaffen werden. Verfügen die logisch getrennten Netze über unterschiedliche Sicherheitsniveaus (z.B. Verwaltungsnetz vs. Schulnetz) ist durch den Einsatz eines Firewall Systems und unter Berücksichtigung der in Kapitel 7 definierten Vorgaben, eine strikte Netzwerktrennung zu erreichen.

6.7.2 VLAN-Konfigurationen

Werden virtuelle LANs eingesetzt, sind an den betroffenen Netzwerkkomponenten die folgenden Konfigurationen vorzunehmen bzw. zu berücksichtigen:

- 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.
- Für Trunkports werden dedizierte VLAN IDs eingesetzt.
- Allenfalls vorhandene Protokolle wie VTP zur automatischen Konfiguration von VLANs sind ausgeschaltet (bzw. mode transparent) oder wenn benötigt sind VTP-Passwörter konfiguriert.

Unterstützt eine Netzwerkkomponente nicht alle notwendigen Konfigurationsmöglichkeiten, darf diese nur ausserhalb einer VLAN-Umgebung eingesetzt werden.

6.8 Drahtlose Netzwerke (Wireless LAN / WLAN)

Grundsätzlich darf im KOMSG ein WLAN als öffentliches Netzwerk oder als eingeschränktes, sicheres Netzwerk betrieben werden. Der Einsatz dieser beiden Varianten unterscheidet sich in den Sicherheitsmassnahmen und ist in den WLAN-Implementationen dementsprechend zu berücksichtigen.

6.8.1 WLAN als öffentliches Netzwerk

Wird ein WLAN als öffentliches Netzwerk betrieben, hat grundsätzlich jedermann Zugriff auf das Netzwerk. Zu beachten sind dabei jedoch die gesetzlichen Rahmenbedingungen. Wird beispielsweise als Dienstleistung ein öffentlicher Internetzugang zur Verfügung gestellt, ist man im rechtlichen Sinn ein Fernmeldedienstanbieter. Währendem auf eine Verschlüsselung des WLANs verzichtet werden kann, muss in diesem Fall die Rückverfolgbarkeit der Benutzeraktivitäten sichergestellt werden. Der Kunde ist verpflichtet die gesetzlichen Rahmenbedingungen basierend auf dem Einsatzzweck seines öffentlichen WLANs abzuklären und entsprechende Massnahmen vollumfänglich umzusetzen.

Beim Betrieb eines öffentlichen WLANs sind zudem die folgenden Massnahmen umzusetzen:

- Das WLAN ist durch eine Firewall vom restlichen Netzwerk abgetrennt, direkte Zugriffe auf interne Netzwerke müssen unterbunden sein.
- Die Firewall erlaubt nur den Zugriff mit den nötigsten Diensten ins Internet und allenfalls auf einzelne Systeme in der DMZ.
- Die Benutzer müssen informiert werden, dass die Daten nicht oder nur schwach verschlüsselt sind und die übermittelten Informationen damit von anderen Personen gelesen werden können.

Soll vom öffentlichen WLAN auf Daten innerhalb dem Kundennetzwerk oder dem KOMSG zugegriffen werden, müssen diese Zugriffe über den VPN-Zugang erfolgen. Dabei gelten die in Kapitel 6.5 beschriebenen Bedingungen.

6.8.2 WLAN als sicheres Netzwerk

Damit vom WLAN direkt auf Daten innerhalb dem Kundennetzwerk oder dem KOMSG zugegriffen werden darf, müssen die folgenden Bedingungen erfüllt sein:

- Es wird eine gegenseitige Authentisierung eingesetzt. Die Benutzer müssen sich für den Zugriff auf das WLAN stark authentisieren (SecureID oder Zertifikat)[10].
- Die Daten werden auf der Luftstrecke mit einem heute als sicher geltenden Algorithmus verschlüsselt[11].
- Die Benutzerverwaltung des WLAN wird kontinuierlich gepflegt. Es ist sicherzustellen, dass austretende Mitarbeiter keinen Zugriff mehr auf das WLAN erhalten.

6.9 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.

6.9.1 Variante 1: VoIP Kommunikation mittels Skyp 4 Business (S4B) über das KOMSG

Alle Kunden 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 Kunden die folgenden Anforderungen erfüllt sein:

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

6.9.2 Variante 2: VoIP Kommunikation mittels KOM SG SIP über das KOMSG

Alle Kunden 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 Kunden die folgenden Anforderungen erfüllt sein:

- Eine logische oder physikalische Trennung zwischen dem Daten- und dem VoIP-Netz. Der Kunde 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.

---

[10] Diese Anforderungen werden nebst einer Lösung basierend auf SecureID heute von den Protokollen EAP-TLS (aktuell beschrieben im RFC 5216), EAP-SIM (aktuell beschrieben im RFC 4186) und LEAP (Cisco-proprietär) erfüllt.

[11] Aktuell wird dies durch 802.11i / WPA2, in welchem die Verschlüsselung mittels Advanced Encryption Standard (AES) realisiert wird, erfüllt.

- Für die Einspeisung des VoIP-Netzes zwischen der KOM SG und des Kunden 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 Kunden von der KOM SG zur Verfügung gestellt.
- Die Kommunikation zwischen dem VoIP-Netz und des Kunden-Netz (CTI) erfolgt über das KOM SG. Die benötigten Freischaltungen müssen durch den Kunden bei der KOM SG beantragt werden.
- Das Netzwerk muss geswitched sein und eine Übertragungsrate von mindestens 100 Mb/s full duplex unterstützen.
- Die für die VoIP-Systeme verwendeten Netzwerkports müssen Autosensing und auch die manuelle Einstellung der Übertragungsrate sowie des Duplex Mode unterstützen.

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

Alle Kunden der Variante 3 telefonieren mittels ESIP. Für die Kommunikation in das öffentliche Telefonnetz wird ein dedizierter SIP-Gateway beim Kunden verwendet. Ein dedizierter Router der Swisscom wird beim Kunden installiert.

Ergänzend zu den übrigen Vorschriften zum Schutz des Netzwerks müssen im Netzwerk des Kunden die folgenden Anforderungen erfüllt sein:

- Eine logische oder physikalische Trennung zwischen dem Daten- und dem VoIP-Netz. Der Kunde 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 Kunden 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 Kunden von der KOM SG zur Verfügung gestellt.
- Die Kommunikation zwischen dem VoIP-Netz und des Kunden-Netz (CTI) erfolgt über das KOM SG. Die benötigten Freischaltungen müssen durch den Kunden bei der KOM SG beantragt werden.
- Das Netzwerk muss geswitched sein und eine Übertragungsrate von mindestens 100 Mb/s full duplex unterstützen.
- Die für die VoIP-Systeme verwendeten Netzwerkports müssen Autosensing und auch die manuelle Einstellung der Übertragungsrate sowie des Duplex Mode unterstützen.

6.9.4 Variante 4: VoIP Kommunikation mittels Rii-Seez SIP (RSIP) des EW Buchs über das KOM SG

Alle Kunden 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 Kunden die folgenden Anforderungen erfüllt sein:

- Eine logische oder physikalische Trennung zwischen dem Daten- und dem VoIP-Netz. Der Kunde 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 Kunden 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 Kunden von der KOM SG zur Verfügung gestellt.
- Die Kommunikation zwischen dem VoIP-Netz und des Kunden-Netz (CTI) erfolgt über das KOM SG. Die benötigten Freischaltungen müssen durch den Kunden bei der KOM SG beantragt werden.
- Das Netzwerk muss geswitched sein und eine Übertragungsrate von mindestens 100 Mb/s full duplex unterstützen.
- Die für die VoIP-Systeme verwendeten Netzwerkports müssen Autosensing und auch die manuelle Einstellung der Übertragungsrate sowie des Duplex Mode unterstützen.

6.9.5 Variante 5: VoIP Kommunikation innerhalb des Kundennetzwerks

Alle Kunden der Variante 5 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 Kunden 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 Kunden die folgenden Anforderungen erfüllt sein:

- Eine logische oder physikalische Trennung zwischen dem Daten- und dem VoIP-Netz.
- Das Netzwerk muss geswitched sein und eine Übertragungsrate von mindestens 100 Mb/s full duplex unterstützen.
- 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 Kunden mit nur einem Ethernet-Kabel erschlossen werden, der PC also an das VoIP-Telefon angeschlossen werden können, muss die entsprechende Netzwerkkomponente VLAN-Trunking unterstützen.
- Wird eine Kommunikation zwischen dem VoIP-Netz und des Kunden-Netz (CTI) gewünscht, muss durch den Kunden eine Verbindung zwischen den beiden Netzen geschaffen werden. Wird dies gemacht, muss aus Sicherheitsgründen gegenüber dem KOM SG ein sicherer Übergang gemäss Kapitel 6.1 geschaffen werden.

7 Schutz mittels Firewall und IDS/IPS

7.1 Grundsätze

Der Zugang zum Internet wird grundsätzlich durch die KOM SG bzw. deren Vertragspartner[12] angeboten. Verfügt ein Kunde über einen eigenen Zugang zum Internet oder/und über Netzwerkverbindungen ausserhalb der Verwaltung, so ist wie in Kapitel 6.1 beschrieben, das KOMSG vom Netzwerk des Kunden wie auch das Netzwerk vom Kunden zum Internet und den Fremdnetzen zwingend durch eine Firewall abzutrennen. Die Firewall zischen dem KOMSG- und dem Kundenetz wird von der KOM SG implementiert und betrieben. Die Kosten werden durch den Kunden getragen.

Den Kunden wird demzufolge die Möglichkeit geboten eigene Verbindungen aus ihrem Netz auf externe Dienste, wie beispielsweise das Internet einzurichten. „LAN Kunde B“ in der Abbildung 2 stellt diese Situation dar:

[12] Zum heutigen Zeitpunkt ist dies die Abraxas Informatik AG

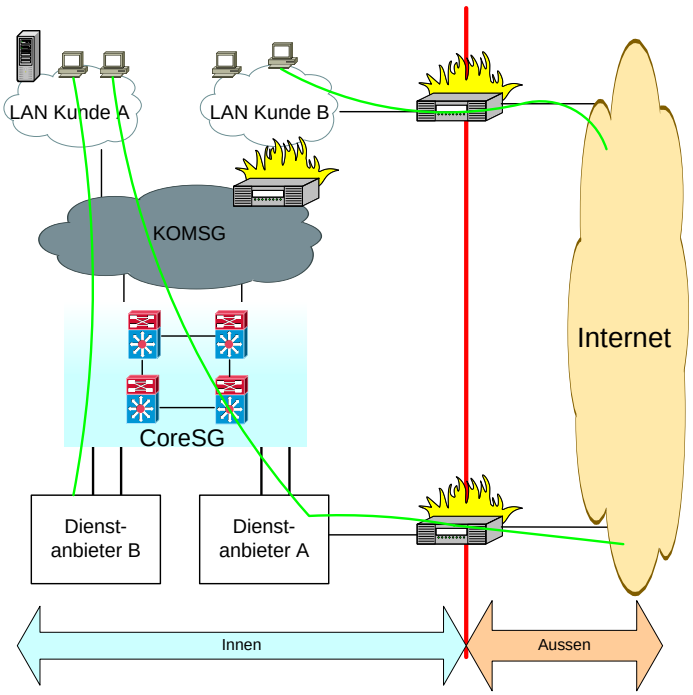

Abbildung 2: Firewall-Übersicht

Eine Firewall bietet in ihrer grundsätzlichen Funktion keinen Schutz vor Protokoll-Missbrauch oder applikatorischen Fehlern. Demzufolge ist als zusätzliche Schutzmassnahme die Analyse des Datenverkehrs bis und mit der Anwendungsebene empfohlen. Systeme welche solche Analysen durchführen sind zentrale Virenschutz-Gateways, Intrusion Detection- und Prevention-Lösungen, Application Layer Firewalls bzw. Application Gateways.

Kann nicht garantiert werden, dass im Netzwerk des Kunden alle Systeme über einen aktiven und aktuellen Virenschutz verfügen, sind die übertragenen Daten im Firewall System oder einem anderen vorgelagerten System auf Malware zu überprüfen.

Wo IPv6 nicht benötigt wird, ist der komplette IPv6-Datenverkehr zu blockieren.

7.2 Technischer Aufbau

Abbildung 3 zeigt die Skizze eines typischen Firewall Systems. Die folgenden Beschreibungen beziehen sich auf die hier aufgeführten Elemente.

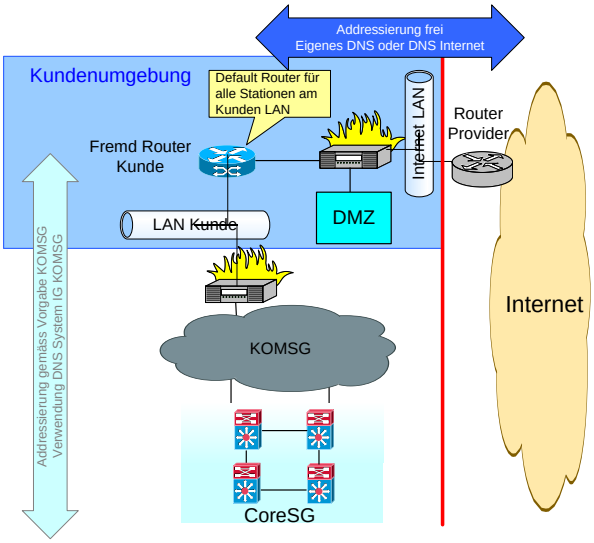

Abbildung 3: Aufbau eines Firewall-Systems

Die Anbindung an externe Netze insbesondere an das Internet erfolgt über ein Firewall System. Innerhalb der Übergangszone von und zum Internet wird eine so genannte „demilitarisierte Zone“ (DMZ) aufgebaut, welche alle Dienste beherbergt, die von aussen erreichbar sind.

Die Firewall bzw. der vorgeschaltete Router fungiert als Standard Gateway der Endgeräte im Netzwerk des Kunden. Das Firewall System (bzw. der vorgeschaltete Router) ist für die Network Address Translation (NAT) zwischen den Drittnetzen und dem Netzwerk des Kunden resp. dem KOMSG besorgt.

Das Firewall System ist auch dafür besorgt, dass die Namens-Auflösung korrekt geschieht. Zu diesem Zweck muss es einen DNS-Dienst anbieten, welcher sicherstellt, dass interne Dienste über die internen Netze erreicht werden, und dass externe Dienste über die Firewall geführt werden („Splitting DNS“).

Der Betreiber muss für einen sicheren Betrieb der Firewall Systeme besorgt sein. Insbesondere muss er gewährleisten, dass die Betriebs- und Wartungsarbeiten die Sicherheit der Netzwerke nicht gefährden (Zugangskontrolle, Authentisierung). Dies ist durch entsprechend zu erstellende Betriebsvorschriften zu unterstützen und sicherzustellen.

7.3 Produkte

Es sind ausschliesslich Firewall Produkte einzusetzen, welche mindestens eine dynamische Paketfiltertechnik (so genanntes Stateful Packet Inspection) bieten. Reine Paketfilter sind aufgrund der oftmals komplex zu konfigurierenden Filterlisten nicht erlaubt.

Es ist sicherzustellen, dass die Unterstützung und die Wartung der eingesetzten Produkte während deren Verwendungsdauer gewährleistet sind. Ferner muss der Betreiber der Firewall Systeme nachweisen können, dass er über genügend betriebliche Erfahrung mit dem eingesetzten Produkt verfügt, und dass er im Fall von technischen Problemen kompetente Ansprechpartner des Herstellers kontaktieren kann.

7.4 Kommunikation

7.4.1 Grundsätze

Das Netzwerk des Kunden darf keine Verbindung in Fremdnetze haben, welche nicht über ein Firewall System abgewickelt wird.

Die Firewall Systeme werden restriktiv aufgesetzt, das heisst: „alles, was nicht ausdrücklich erlaubt ist, ist verboten“. Dies bedeutet, es dürfen nur die notwendigen Endgeräte und Dienste (Netzwerkprotokoll) bzw. Kommunikationsbeziehungen freigeschalten sein. Die Firewall Systeme verfügen jeweils über eine letzte und abschliessende Verbotsregel (alle Netze, Systeme und Dienste / deny all).

7.4.2 Dienste vom internen Netzwerk zum Internet

Für alle Systeme im Netzwerk des Kunden kann der Zugang zu gängigen Diensten (Netzwerkprotokolle) im Internet geöffnet werden. Diese gängigen Dienste sind: http, https, smtp, dns, ntp.

Unter der Voraussetzung, dass der Zugang auf bestimmte Systeme im Netzwerk des Kunden eingeschränkt wird, ist die Freischaltung weiterer Dienste (Netzwerkprotokolle) zum Internet erlaubt.

7.4.3 Dienste vom Internet zum internen Netzwerk

Falls interne Dienste von aussen (Internet und Fremdnetze) erreichbar sein sollen, so muss das Firewall System so aufgebaut sein, dass die Sicherheit der internen Systeme durch die Verwendung der Dienste nicht gefährdet ist.

Als Mindestanforderung muss der Datenverkehr über spezifische Systeme in der DMZ (z.B. Webserver, reverse Proxies, VPN-Gateway, etc.) geführt werden. Diese Systeme müssen durch das Firewall System vor unberechtigtem Zugriff aus dem Internet geschützt sein. Das System selbst darf nur auf dedizierte Systeme und Dienste im internen Netzwerk des Kunden zugreifen können.
Die spezifischen Systeme in der DMZ sind zwingend mit den im Kapitel 5 beschriebenen Sicherheitsanforderungen auszustatten. Hervorzuheben sind hierbei das regelmässige

und schnelle Aktualisieren der Software, die Gewährleistung eines aktiven und aktuellen Virenschutzes sowie dem Härten des Systems.

7.4.4 Netzwerktrennung zwischen dem KOMSG und dem Kundennetzwerk

Der Übergang zwischen dem KOMSG und dem Netzwerk des Kunden muss auf der Firewall so konfiguriert sein, dass ein- wie auch ausgehend nur die notwendigen Dienste und Systeme für die netzwerkübergreifende Kommunikation freigeschaltet sind. Hat der Kunde einen direkten Internetzugang, muss eine Firewall zwischen KOMSG und internem Netzwerk implementiert werden. Diese Firewall wird von der KOM SG implementiert und betrieben. Die Kosten werden durch den Kunden getragen.

7.4.5 Netzwerktrennung gegenüber Fremdnetzen

Um eine klare Grenze zwischen den Systemen, welche dem Sicherheitsniveau des KOMSG entsprechen und den Systemen in Fremdnetzen sicherzustellen, muss eine strikte Netzwerktrennung vorliegen.

Eine strikte Netzwerktrennung liegt vor, wenn es sich um vereinzelte Kommunikationsverbindungen handelt und diese auf einzelne Endgeräte (IP-Adresse) und Dienste (Netzwerkprotokoll) eingeschränkt sind. Dabei ist es unbedeutend, ob die Netzwerkverbindung über physisch oder logisch getrennte Netzwerke führt.

7.4.6 Testschaltungen

Für Testzwecke können einzelne Sicherheitsvorkehrungen verändert bzw. deaktiviert werden. Dies aber nur unter den folgenden Voraussetzungen:

- Die Veränderungen bzw. Deaktivierungen sind zeitlich begrenzt und werden nach Abschluss der Arbeiten wieder restlos entfernt. Nach Möglichkeit durch zeitlich limitierte und automatisch korrigierende Regeleinträge.
- Die speziellen Konfigurationen werden vollständig dokumentiert und inklusive zeitlichem Ablauf protokolliert.
- Während der Zeit mit reduziertem Schutz werden die Überwachungsaktivitäten angemessen verstärkt (z.B. vollständige Log-Überwachung).
- Test-Schaltungen müssen der KOM SG gemeldet werden.

7.5 Verwaltung der Firewall-Regeln

Firewall-Regeländerungen sind einem formalen Prozess zu unterwerfen, dieser muss nachvollziehbar und die Regeln müssen dokumentiert sein. Der Betreiber der Firewall Systeme muss ein Vetorecht für Regeländerungen haben, wenn berechtigte Zweifel an der Aufrechterhaltung der Informatiksicherheit bestehen.

7.6 Aufzeichnung, Aufbewahrung und Auswertung von Logdaten

In den Log-Protokollen sind sämtliche sicherheitsrelevante Vorfälle aufzuzeichnen um künftige Untersuchungen und die Überwachung der Zugangskontrolle zu ermöglichen.

Es ist sicherzustellen, dass die Logdaten auch nach Ausfall des Firewall Systems noch vorhanden sind. Die Log-Protokolle sind vor unberechtigten Zugriffen zu schützen und müssen mindestens 3 Monate aufbewahrt werden.

Die Logdaten sind mindestens einmal pro Woche zu analysieren. Die Analyse kann entweder automatisch oder manuell erfolgen. Bei einer automatischen Analyse muss ein automatisches Warnsystem eingebunden werden.
Falls die Auswertung der Logdaten und allfällig weitergehende Analysen einen Angriff bestätigen, sowie keine wirksamen Gegenmassnahmen zur Verfügung stehen, so muss der Verantwortliche des Kunden die Verbindung zum Internet oder zum Fremdnetz sofort deaktivieren. Anschliessend ist gemäss Kapitel 2.3 (Bewältigung ausserordentlicher Lagen) vorzugehen.

7.7 System- und Betriebsdokumentation

Die Systemdokumentation der Firewall muss mindestens beinhalten:

- Detailspezifikation der Installation, Sichtbarkeit der verschiedenen Netzwerkzonen
- Konfiguration der Netzwerk-, Routing- und NAT-Einstellungen
- Konfiguriertes Regelset inklusive Testschaltungen
- Zeitsynchronisations- und Log-Einstellungen
- Produktspezifische Einstellungsmöglichkeiten

Die Betriebsdokumentation der Firewall muss mindestens beinhalten:

- Anträge, Bewilligungen und die Ausführung von Regeländerungen
- Sämtliche Änderungen am Firewall System insgesamt
- Alle Veränderungen der Netzwerkumgebung (Netzwerkzonen, Router)
- Auswertung der Logdaten

Die gesamte Dokumentation muss aktuell und innerhalb einer Stunde verfügbar sein. Der Zugriff darf ausschliesslich für Berechtigte des Kunden sowie dessen allfälligen IT-Leistungserbinger möglich sein. Die KOM SG kann Einsicht in die Dokumentation verlangen.

7.8 Prüfung

Die Firewall Systeme sind regelmässig, mindestens aber einmal pro Jahr, durch den Kunden oder durch ihn Beauftragte zu überprüfen. Die Kosten der Prüfung werden durch den Kunden getragen. Die Prüfung muss die folgenden Bereiche umfassen:

- Konformität mit den Sicherheitsvorschriften
- Aktualität und Korrektheit der Regeleinträge
- Korrekte Installation und Funktion insgesamt
- Vollständigkeit der Dokumentation

Die Prüfung ist zu dokumentieren. Der Prüfbericht muss mindestens die folgenden Themeninhalte berücksichtigen:

- Geprüfte Bereiche
- Resultate

- Massnahmen aufgrund der Prüfungen

Die KOM SG kann Einsicht in die Prüfungsdokumentationen verlangen.

8 Anhang

8.1 Glossar

Begriff	Bedeutung
Application Gateway	Ein Application Gateway ist ein System, auf dem für jede unterstützte Anwendung ein spezielles Programm Verbindungsanforderungen von Benutzerprozessen entgegennimmt, die Autorisierungen dieser Prozesse prüft, im positiven Fall Verbindungen aufbaut, unterhält und später auch wieder abbaut. Ein solches Programm, das im Wesentlichen als Stellvertreter und Vermittler zwischen Benutzerprozess und Server tritt, wird auch als Proxy-Server bezeichnet.
Application Layer Firewall	Siehe auch Begriff Firewall. Eine Application Layer Firewall berücksichtigt zusätzlich zu den reinen Verkehrsdaten wie Quelle, Ziel und Dienst noch den Inhalt der Netzwerkpakete bis und mit der Anwendungsschicht (OSI Layer 7, Application Layer).
Desktop Sharing	Desktop Sharing Lösungen ermöglichen die Übermittlung von Bildschirminhalten sowie die Fernsteuerung entfernter Systeme über ein Netzwerk, wie beispielsweise dem Internet. Im Unterschied zu konventionellen Lösungen initiieren Desktop Sharing Produkte den Fernzugriff vom internen Netzwerk aus.
DMZ	DMZ ist die Abkürzung für Demilitarisierte Zone. Der Ausdruck stammt aus dem militärischen Sprachgebrauch und bezeichnet eine Sicherheitszone zwischen Kampfgebieten. Im Informatikumfeld ist es eine Netzwerkzone für öffentlich zugängliche Internet-Dienste. Es ist das Netzwerk zwischen dem geschützten internen Netzwerk und dem ungeschützten externen Netzwerk.
Firewall	Schutzmechanismus in Form von Hard und Software, welcher den Datenfluss zwischen zwei Netzsegmenten kontrolliert und diesen bei Verstoss gegen definierte Regeln unterbindet.
Hoax	Eine „Ente“, also eine Falschmeldung, oft über angebliche Malware. Ein Hoax richtet nur insofern Schaden an, wenn der Benutzer der Aufforderung in der Falschmeldung folgt und indem er durch die Bitte um Weiterversand Ressourcen beansprucht (Ablage auf Mail-System, Bandbreite beim Weiterversand).

Intrusion Detection, Intrusion-Prevention	Intrusion Detection- und Prevention-Lösungen (IDS, IPS) dienen zur Erkennung von Angriffen, die gegen ein Computersystem oder Kommunikationsnetzwerk gerichtet sind. IDS- und IPS-Systeme können eine Firewall ergänzen oder auch direkt auf dem zu überwachenden Computersystem aktiv sein und so die Sicherheit von Netzwerken erhöhen.
IP-Telefonie	IP-Telefonie (kurz für Internet-Protokoll-Telefonie), auch Internet-Telefonie oder Voice over IP (kurz VoIP) genannt, ist das Telefonieren über Computernetzwerke, welche nach Internet-Standards aufgebaut sind. Dabei werden die für Telefonie typischen Informationen, d. h. Sprache und Steuerinformationen über ein auch für Datenübertragung nutzbares Netz übertragen. Bei den Gesprächsteilnehmern können sowohl Computer, auf IP-Telefonie spezialisierte Telefonendgeräte, als auch über spezielle Adapter angeschlossene klassische Telefone die Verbindung herstellen.
Makro (Microsoft Office)	Ein Makro ist in der Softwareentwicklung eine zusammengefasste Folge von Anweisungen, um diese anstelle von Einzelanweisungen, mit nur einem Aufruf ausführen zu können. Makros können beim Öffnen von Microsoft Office Dateien automatisch ausgeführt werden. Dabei können im Hintergrund Viren installiert werden.
Malware	Sammelbegriff für Viren, Trojaner, Würmer und Hoax. Generell versteht man darunter Software, welche schädliche Funktionen ausführt.
Remote Wiping	Sicheres Löschen von Daten aus der Ferne. Siehe Wiping.
Reverse Proxy	Ein Proxy bezeichnet ein System, das zwischen einem Server und einem Client postiert wird. Er arbeitet als Vermittler, der auf der einen Seite Anfragen entgegennimmt, um dann über seine eigene Adresse eine Verbindung zur anderen Seite herzustellen. Ein Reverse Proxy tritt als vermeintliches Zielsystem, meist gegenüber Anfragen aus dem Internet, in Erscheinung und verbirgt so dem Client die wahre Adresse des Zielsystems.
Social Engineering	Durch das Ausnutzen der Hilfsbereitschaft, Gutgläubigkeit oder Unsicherheit von Personen, gelangen Angreifer an vertrauliche Informationen oder verleiten die Opfer zur Ausführung bestimmter Aktionen. Da die technischen Schutzmassnahmen immer aufwändiger und dadurch auch schwieriger zu überwinden werden, erfreut sich Social Engineering zunehmender Beliebtheit.

Spam-Mail	Als Spam werden unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten bezeichnet, die dem Empfänger unverlangt zugestellt werden und häufig werbenden Inhalt haben.
Trojaner	Trojaner sind Programme, die neben scheinbar nützlichen auch schädliche Funktionen enthalten. Trojaner dienen primär dazu ein Computersystem via Fernzugriff zu kontrollieren.
Tunneling	Ein Verfahren, bei dem Datenpakete von einem Protokoll mit Hilfe eines anderen Protokolls übertragen werden. Oft werden dabei die ursprünglichen Daten auch verschlüsselt.
Virtual Private Network	Ein Verfahren, bei dem Datenpakete von einem Protokoll mit Hilfe eines anderen Protokolls übertragen werden. Oft werden dabei die ursprünglichen Daten auch verschlüsselt.
Virus	Viren sind Programmteile, die eine zerstörerische Wirkung auf Daten oder auf ein bestimmtes Computersystem haben können. Normalerweise benötigt ein Virus eine Aktion des Benutzers um aktiviert zu werden. Beispielsweise werden Mail-Anhänge geöffnet, Files auf den Server kopiert oder eine Fremd-CD in das System eingelesen. Somit hat der Virus die Möglichkeit sich zu verbreiten.
VLAN	Ein Virtual Local Area Network (VLAN) ist ein logisches Teilnetz innerhalb eines gesamten physischen Netzwerks. Es kann sich über einen oder mehrere Switches hinweg ausdehnen.
VoIP	Siehe IP-Telefonie
VPN	Siehe Virtual Private Network
Wiping	Sicheres Löschen von Daten durch mehrmaliges Überschreiben mit speziellen Bit-Mustern oder Zufallsdaten. Dadurch soll gewährleistet werden, dass die gelöschten Daten nicht mehr durch forensische Analyse von Datenträgern rekonstruiert werden können.
Wurm	Würmer sind wie Viren, haben jedoch die Möglichkeit, einmal aktiviert, sich auf andere Computersysteme zu verbreiten. Im Gegensatz zu den Viren nutzen Würmer Sicherheitslücken von Computersystemen aus. Beispielweise können Würmer sich innerhalb eines Netzwerkes verbreiten und eine ganze Gruppe von Computersystemen infizieren.

9 Checklisten

Die Checklisten der KOM SG dienen zur Überprüfung der Einhaltung der vorliegenden Sicherheitsvorschriften. Sie werden von der KOM SG, von beauftragten Auditoren sowie für die jährliche Überprüfung durch den Kunden eingesetzt.