Arbeitsrichtlinie Kommunikationssicherheit

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Kommunikationssicherheit
Version	21.0
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	09.12.2019
Verabschiedet durch	Daniel Fürdauer (Informationssicherheitsbeauftragter)
Klassifikation	Intern
Verantwortlicher Verantwortliche Abteilung	Daniel Fürdauer Datenschutz und Informationssicherheit
Fachlicher Ansprechpartner	Daniel Fürdauer (daniel.fuerdauer@vav.at)
Letztes Review	November 2021

Dokumentenhistorie

Version	Datum	Beschreibung der Änderung	Ersteller
19.0	09.12.2019	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 19.0.	Daniel Fürdauer
20.0	04.12.2020	Redaktionelle Änderungen und Möglichkeit der Berücksichtigung von Services bei der Gestaltung von Netzsegmenten ergänzt (Kap 3.1).	Daniel Fürdauer
21.0	22.11.2021	Ergänzung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 19.0: Reglementierter Internetzugang auch außerhalb vom VAV Netzwerk	Daniel Fürdauer

Hinweis zur Schreibweise

Die verwendete männliche Sprachform dient der leichteren Lesbarkeit und meint immer alle Geschlechter (m/w/d). Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

INHALTSVERZEICHNIS

1. ZIELSETZUNG

Zur Gewährleistung einer sicheren Kommunikation ist es wichtig, angemessene Vorkehrungen zum Schutz von Informationen in Netzwerken und den unterstützenden informationsverarbeitenden Einrichtungen zu ergreifen. Ziel ist es dabei, die Sicherheit der Informationen in Netzwerken und den Schutz vernetzter Dienste vor unbefugten Zugriff zu gewährleisten.

2. ADRESSATEN

Diese Richtlinie richtet sich an die Verantwortlichen und Betreiber von Netzinfrastrukturen und Kommunikationsdiensten.

3. INTERNES NETZWERK

Netzwerke müssen angemessen verwaltet und gesteuert werden, um Informationen in Systemen und Anwendungen zu schützen. Dabei sind klare Verantwortlichkeiten und Verfahren für die Verwaltung der Netzwerktechnik zu definieren.
Kommen im internen Netzwerk dynamische Routingprotokolle zum Einsatz, dürfen diese nur mit einer Authentisierung verwendet werden.

3.1. Planung und Konzeption von Netzwerken

Um die Verfügbarkeit zu gewährleisten, ist eine resiliente Architektur aufzubauen. Ein solches Netzwerkdesign wird umso wichtiger, je zentraler die Infrastruktur implementiert wird.
Die Vertraulichkeit des Netzwerks ist u. a. durch eine Segmentierung und Abgrenzung unterschiedlicher Netzsegmente sicherzustellen. Netzsegmente müssen auf Grundlage des Schutzbedarfs oder der Art des Services voneinander abgegrenzt werden. Die Berechtigungen zu einzelnen Netzsegmenten ist durch ein Berechtigungskonzept zu regeln. Die Vergabe von Rechten hat stets zweckgebunden und nach dem Minimalprinzip zu erfolgen.

3.2. Segmentierung von Netzwerken

Die Segmentierung von Netzwerken verfolgt das Ziel, den Angriffsvektor zu minimieren und daraus resultierende Risiken einzudämmen. Dabei sind einzelne Netzsegmente so zu gestalten, dass sie folgende Anforderungen erfüllen:

- Für jedes Netzsegment muss festgelegt werden, inwieweit es als vertrauenswürdig eingestuft werden kann. Netze, die nicht vertrauenswürdig sind, sind als „untrusted“ zu behandeln und entsprechend abzusichern Ein Netzsegment ist als „untrusted“ zu betrachten, wenn die alleinige Hoheit der VAV in einem Netzsegment nicht sichergestellt werden kann. Dies trifft grundsätzlich auf Netzsegmente zu, die aus dem Internet oder einem nicht VAV Netzsegment zugreifbar sind.
- Client-, Server und Infrastruktur-Netze sind zu separieren.
- Managementsegmente für administrative Umgebungen sind einzurichten.
- Technische Lösungen (z.B. LAN, Storage, UC und VoIP) sind voneinander zu trennen.
- Segmentierung von zentralen Infrastrukturdiensten.
- Webanwendungen sind in gesonderten Netzsegmenten zu betreiben.
- Netzzugänge zu unsicheren (nicht VAV) Netzwerken sind in einem dafür erstellten Netzsegment zu terminieren.

Netzsegmente sind nach dem aktuellen Stand der Technik voneinander zu separieren. Die Umsetzung der Separierung hat mindestens auf Basis von Quell- und Zieladresse sowie von Netzwerkpaketen,-protokollen und -diensten zu erfolgen. Übergänge zwischen den Netzsegmenten sind nach dem Prinzip von Whitelists zu erstellen. Die Whitelists sind zweckgebunden und nach dem Minimalprinzip zu gestalten. Der Datenaustausch zwischen Netzsegmenten erfolgt ausschließlich über die definierten und kontrollierten Netzübergänge (z.B. Firewalls). Unkontrollierte Netzübergänge und Zugriffe von unterschiedlichen Netzsegmenten sind technisch und organisatorisch zu unterbinden.

3.3. Gastzugänge

Ein Gastzugang soll Besuchern und externen Mitarbeitern den Internetzugang ermöglichen. Hierbei sind zusätzliche Anforderungen zu beachten:

- Gäste-WLANs und Gäste-LANs müssen von VAV internen Netzen separiert werden. Dies ist mindestens mithilfe einer logischen Trennung durchzuführen.
- Der Gastzugang darf nur Verbindungen Richtung Internet zur Verfügung stellen. Der Zugang zum internen VAV Netz ist zu unterbinden.
- Der Zugang zum Internet sollte transparent erfolgen (kein Proxy etc.).

3.4. Dokumentation

Zur Gewährleistung einer angemessenen Dokumentation ist ein Netzwerktopographieplan, der die physische Struktur des Netzwerks darstellt und ein Netzwerktopologieplan, der die logische Struktur des Netzwerks abbildet, zu erstellen.
Der Netzwerktopographieplan muss mindestens die folgenden Aspekte beinhalten:

- Die räumliche Anordnung der Netzwerkkomponenten und
- die topographische Anbindung der Netzkomponenten.

Der Netzwerktopologie-Plan muss mindestens die folgenden Aspekte beinhalten:

- Die Segmentierung des Netzwerks.
- Die Netz- und IP-Adresse der abgebildeten Netzwerksegmente und Netzkomponenten.
- Die Netzkomponenten, die zur Bildung der Segmente verwendet werden.

An Netzübergängen sind zudem alle Kommunikationspartner und -dienste inklusive der Richtung der Kommunikation zu dokumentieren und nachzuhalten (dies kann beispielsweise über Firewallregelwerke geschehen).

4. DRAHTLOSNETZWERKE

Drahtlose, lokale Netze (WLAN) sind im Vergleich zu kabelgebundenen Netzwerken zusätzlichen Gefährdungen ausgesetzt. Daher sind bei einem Betreib von WLAN-Umgebungen weitere Maßnahmen zu treffen:

- Bei der Planung, Konzeption und dem Aufbau von Drahtlosnetzwerken sind internationale Standards nach dem Stand der Technik zu verwenden.
- Es dürfen nur autorisierte WLAN-Clients eine Verbindung zum WLAN herstellen. Dies ist über eine sichere Authentifizierung sicherzustellen. Werden in diesem Umfeld Zertifikate eingesetzt, sind diese regelmäßig zu erneuern. Hierbei zu gewährleisten, dass die Authentisierung des IT-Systems und des Users gesondert erfolgen.
- Bei WLAN-Netzen ist sicherzustellen, dass der Inhalt des Datenstroms vor unbefugter Kenntnisnahme geschützt ist. Dies ist in Drahtlosnetzwerken grundsätzlich durch eine Verschlüsselung des Datenstroms zu gewährleisten. Die hierbei eingesetzte Verschlüsselungsmethode muss dem Stand der Technik gerecht werden.
- Durch die fehlende physischen Zugriffssteuerung auf WLAN-Netze ist der Angriffsvektor auf Drahtlosnetzwerke durch anderweitige Maßnahmen zu kompensieren. Auf Grundlage dieser Anforderung ist die Ausleuchtung des WLAN auf die Räumlichkeiten der VAV zu beschränken.
- WLAN-Netze sind durch eine SSID zu identifizieren. Eine direkte Ableitung des SSID Namens auf das Unternehmen, den Betreiber, das Netzwerk oder den Verwendungszweck ist zu vermeiden.
- Eine nicht genehmigte Erweiterung von Netzwerken ist zu unterbinden. Es sind Maßnahmen zu implementieren, die das Einbinden von Repeatern oder den Aufbau von Network Bridges verhindern.

5. EXTERNE SCHNITTSTELLEN

Erfolgt eine technische Kommunikation zwischen einem internen Netzwerk zu einem externen Netzwerk, das nicht unter der Kontrolle der VAV steht, müssen folgende Anforderungen erfüllt sein:

- Informationen müssen nach dem derzeitigen Stand der Technik über sichere Protokolle übertragen werden.
- Verbindungen zu externen Netzen sind nach dem Stand der Technik angemessen zu verschlüsseln und zu authentisieren.
- Der Internetzugang sowie sämtliche Schnittstellen zum Netzwerk der VAV sind zu reglementieren und zu überwachen; hierzu sind geeignete technische Maßnahmen zu treffen. Ebenso sind alle weiteren Datenflüsse durch geeignete Strukturen zu reglementieren.
- Die Kommunikationsverbindungen sind bis auf die minimalen benötigten technischen Voraussetzungen einzuschränken.
- Im Falle eines Versagens der eingesetzten Sicherheitsgateways muss sichergestellt werden, dass während dieser Zeit keine eingehenden oder ausgehenden Netzwerkverbindungen hergestellt werden können.
- Ein unkontrollierter Verbindungsaufbau zu externen Netzen ist technisch zu unterbinden.

5.1. Demilitarisierte Netzwerkzonen

Netzwerke, in denen die alleinige Hoheit der VAV nicht sichergestellt werden kann, sind besonders zu sichern. An dieser Stelle ist eine Netzsegmentierung nicht ausreichend. Daher gelten für diese Netzwerkzonen weitere Sicherheitsanforderungen:

- Anbindungen externer Schnittstellen und nach extern erbrachten Services sind im Rahmen einer demilitarisierten Netzwerkezone (DMZ) von internen Netzsegmenten abzugrenzen. Die Übergänge der DMZ-Segmente sind mittels geeigneter technischer Maßnahmen gegeneinander abzusichern.
- Netzübergänge dürfen ausschließlich über die dafür vorgesehenen Sicherheitsgateways erfolgen. Keine anderen Dienste oder Anwendungen dürfen zur Verfügung gestellt werden. Ein administrativer Zugriff auf Sicherheitsgateways darf ausschließlich über sichere Netzsegmente, sichere Konsolen, verschlüsselte Verbindungen oder dedizierte Netzwerke erfolgen.
- Anpassungen von Regelsätzen auf den Sicherheitsgateways müssen nach dem Whitelisting-Verfahren sowie nach Minimalanforderungen erfolgen. Der ausschließliche Einsatz von Blacklists ist nicht ausreichend.
- Eine Datenhaltung innerhalb der DMZ ist zu vermeiden.

5.2. Internetzugriff

Der Zugriff aus VAV internen Netzwerken auf das Internet zur Nutzung von externen Webdiensten birgt Risiken für die Informationssicherheit. Der Zugriff auf externe, nicht vertrauenswürdige Netze (wie z. B. das Internet) ist daher strikt zu reglementieren und zu überwachen.

- Ein nicht authentifizierter Zugriff in oder aus dem Netzwerk der VAV ist grundsätzlich abzuweisen bzw. zu unterbinden. Die Kommunikationsverbindungen sind jederzeit zweifelsfrei einer handelnden natürlichen Person zuzuordnen.
- Ein(e) Kommunikation / Datenaustausch ist grundsätzlich zu protokollieren.
- Um Gefährdungen für die Vertraulichkeit, Integrität und Authentizität einzugrenzen, sollten sämtliche externe Kommunikationsverbindungen verschlüsselt erfolgen.
- Der Datenaustausch zwischen VAV und externen, nicht vertrauenswürdigen Netzen ist auf Schadsoftware zu überprüfen. Der Zugriff und die Bereitstellung unerwünschter Inhalte ist zu unterbinden.
- Proxy-Server, ebenso wie andere IT-Systeme, die für die direkte Kommunikation zum oder vom Internet konzipiert sind, müssen in einer demilitarisierten Zone (DMZ) aufgestellt werden.
- Der Internetzugriff von VAV IT-Systemen ist auch dann zu reglementieren und zu steuern, wenn sich VAV IT-Systeme in Netzwerken befinden, die nicht unter der Kontrolle der VAV stehen (z. B. im Homeoffice).

Ein(e) Kommunikation/Datenaustausch ist grundsätzlich zu protokollieren, hier sind mindestens folgende Informationen zu erfassen:

- Benutzerkennung
- Quell- und Ziel-Adresse
- Zeitstempel
- Genutzte Protokolle
- Sicherheitsrelevante Auffälligkeiten (abgelehnte Anfragen)

Das zur Reglementierung und Überwachung eingesetzte IT-System, das den Zugriff auf das Internet bereitstellt, ist durch seinen Einsatzzweck einem großen Angriffsvektor ausgesetzt. Um diesem Angriffsvektor entgegenzuwirken, sind im Rahmen der Konfiguration und des Betriebs dieser IT-Systeme folgende Anforderungen zu erfüllen:

- Der administrative Zugriff ist vom zu reglementierenden Datenstrom zu trennen (das Management hat über ein Out-of-band Netzwerk zu erfolgen).
- Administrative Accounts sind auf ein Minimum zu beschränken.
- Regelwerke sind nach einem Whitelisting-Verfahren zu implementieren.
- Content Filter sind auf einem aktuellen Stand zu halten und es ist ein Prozess zu implementieren dies zu gewährleisten.

5.3. Externe Netzzugriffe

Erfolgt ein Zugriff auf das interne Netzwerk über externe Netze, beispielsweise über ein VPN (Virtual Private Network), ist dieser Zugriff besonders zu schützen. Bei der Planung und Umsetzung solcher Zugriffe ist folgendes zu beachten:

- Der Zugriff auf interne Netzwerke ist zusätzlich zu authentisieren und zu verschlüsseln. Die technische Umsetzung muss nach dem Stand der Technik erfolgen. Die Übertragung der verwendeten Konfigurationen und Schlüssel auf andere IT-Systeme, zum Beispiel auf private Smartphones oder PCs, ist nicht gestattet.
- Für den Aufbau von externen Netzzugriffen sind ausschließlich Hard- und Softwarekomponenten zu verwenden, die durch den IT-Betrieb implementiert wurden. Änderungen an der Konfiguration dieser Komponenten sind ausschließlich durch qualifiziertes IT-Personal zulässig
- Der Zugriff auf interne Netzwerke von außen ist über einen Berechtigungsprozess zu steuern.
- Nicht mehr benötigte User-Zugänge sind umgehend zu entfernen.
- Die Nutzung dieser Zugriffe hat ausschließlich zweckgebunden zu erfolgen. Eine erweiterte Nutzung ist technisch zu unterbinden.
- Eine Verbindungssession ist zeitlich zu begrenzen und ist automatisiert zu trennen.
- Der Zugriff über externe Netzwerke auf das interne Netzwerk der VAV ist zu protokollieren.

5.4. Datenübertragung

- Bei einer Übertragung von Daten an Dritte sind im Vorfeld Vereinbarungen bezüglich eines sicheren Transfers zu regeln und umzusetzen.
- Eine Datenübertragung über externe Netze hat grundsätzlich verschlüsselt zu erfolgen.
- Werden Daten und Informationen über externe Netzwerke übertragen, sind die Integrität und Vertraulichkeit sicherzustellen. Hierzu sind technische Maßnahmen nach dem Stand der Technik zu wählen.