Arbeitsrichtlinie
Schutz vor Schadsoftware

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Schutz vor Schadsoftware
Version	21.0
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	21.10.2019
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	21.10.2019	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 19.0.	Daniel Fürdauer
20.0	04.12.2020	Review ohne inhaltliche Änderungen	Daniel Fürdauer
21.0	22.11.2021	In Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 21.0: Konkretisierung der Kapitel: 1, 3, 3.1, 3.3.1, 3.3.3, 3.4; Neues Kapitel 3.5: Monitoring	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. EINLEITUNG

Diese Richtlinie legt die Anforderungen an den Schutz vor Schadsoftware und das Virenschutzkonzept fest. Wenn immer in dieser Arbeitsrichtlinie von Virenschutz gesprochen wird, ist damit jeglicher Schutz vor Schadsoftware gemeint, sei es proaktiv oder reaktiv.

2. ABGRENZUNG

Die Richtlinie betrachtet nur die Vorgaben für Anwendungen zum Schutz vor Schadsoftware (Virenscanner). Eine Abgrenzung findet weder auf IT-Systemtypen noch auf Schadsoftwaretypen statt.

3. VORGABEN AN DIE KONZEPTION

Es sind angemessene organisatorische und technische Vorkehrungen nach dem Stand der Technik zu treffen. Dazu müssen auch Systeme eingesetzt werden, die in der Lage sind, automatisch im laufenden Betrieb Bedrohungen zu identifizieren, zu vermeiden und Beseitigungsmaßnahmen vorzusehen. Um diesen Schutz entsprechend sicherstellen zu können, sind die folgenden Vorgaben, sofern durch das eingesetzte Produkt umsetzbar, im Rahmen der Konzeption zu berücksichtigen.

3.1. Grundsätzliche Anforderungen

Ein Virenscanner ist grundsätzlich auf allen Client- und Serversystemen (Betriebssystemen) zu installieren. Sollten Ausnahmen von dieser Regel notwendig sein, sind diese mit der Stabstelle Datenschutz und Informationssicherheit abzustimmen und zu dokumentieren. Ausgenommen sind hiervon aktive Netzwerkkomponenten, Embedded Betriebssysteme und Appliances. Da für diese Systeme keine zusätzliche Schutzsoftware installiert werden kann, muss dem Patchmanagement größere Bedeutung beigemessen werden (siehe hierzu auch die Arbeitsrichtlinie Sicherheitspatches).
Schadcode oder Malware dürfen nicht in das Unternehmensnetz eingebracht werden. Ist es trotzdem notwendig, Malware z.B. im Rahmen forensischer Untersuchungen auf Systemen der VAV zu speichern oder testweise auszuführen, so darf dies ausschließlich in isolierten Umgebungen erfolgen. Erkenntnisse solcher Untersuchungen sind der Stabstelle Datenschutz und Informationssicherheit mitzuteilen.
Sicherheitsrelevante Einstellungen sind so zu gestalten, dass eine Veränderung durch den Anwender ausgeschlossen ist.

3.2. Produktauswahl

Es wird empfohlen, bei der Auswahl auf geeignete Produkttestergebnisse von anerkannten Organisationen[1] zurückzugreifen.
Folgende Basisanforderungen sollten die ausgewählten Produkte unterstützen:

[1] Beispiel: AV-Test GmbH (https://www.av-test.org)

ANFORDERUNG	BESCHREIBUNG
Zentrale Administration	Das Produkt besitzt eine zentrale Managementkonsole für die Konfiguration und Verwaltung der Funktionen. Die Etablierung eines Berechtigungskonzepts für verschiedene Rollen muss möglich sein. Die Anbindung an eine zentrale Benutzerverwaltung sollte möglich sein.
Remoteinstallation und Updatemanagement	Die unbeaufsichtigte automatische Installation der Virenscanner von Arbeitsplatz- und Serversystemen sollte über das Netzwerk möglich sein. Sofern Verfahren zur Installation aus der Ferne und automatisiert erfolgen, sollten Integritätskontrollen der ausgerollten Softwarepakete erfolgen. Nur Softwarepakete von der Herstellerseite dürfen installiert werden. Dies betrifft auch Updates der Virenscanner für alle Module, sowie die Updates der Virensignaturen. Integritäts- und Authentizitätskontrollen für Updates der Virensignaturen müssen vom Produkt unterstützt werden.
Integritätstest	Das Produkt sollte Integritätstests der eigenen Services, Daten und Programme sowie Bibliotheken enthalten. Weiterhin sollte es in der Lage sein, ein unerwartetes Verhalten von laufenden Prozessen zu erkennen.
Selbsttest	Das Produkt muss Änderungen an seinen Konfigurationseinstellungen auf Plausibilität prüfen können. Änderungen an der Konfiguration sind zu protokollieren.
IPv6-Fähigkeit	Eine Kompatibilität gemäß RIPE-554 (Internet Protocol Version 6) sollte gewährleistet sein.
Prüfungen auf Schadsoftware	Das Produkt muss über unterschiedliche Überprüfungsmethoden verfügen. Folgende Überprüfungsmethoden sollte das Produkt umfassen: Standardüberprüfungen, individualisierte Überprüfung durch den Benutzer, Schnellprüfung und vollständige Überprüfung. Die Überprüfung des Systems muss dabei automatisiert (zeitgesteuert), manuell und bei Zugriff (engl. „on-access“) erfolgen können.
Prüfung von Daten	Die Überprüfung von Daten muss alle gängigen Dateisysteme und Dateiformate umfassen. Weiterhin muss die Funktionalität der Überprüfung von komprimierten Archivdateien gegeben sein. Das Werkzeug soll gängige Archive, z. B. ZIP, TAR, … automatisch entpacken und die darin enthaltenen Dateien prüfen können. Dieses sollte auch bei Archiven mit einer Verschachtelungstiefe von mindestens 16 Archiven möglich sein. Bei kennwortverschlüsselten Archiven sollte die Möglichkeit bestehen, diese Archive aussteuern zu können. Zumindest muss das Ereignis in den Protokolldateien festgehalten werden.
Prüfung von Quellen	Die Überprüfung verschiedenster Quellen eines Systems muss gewährleistet sein. Dazu zählen insbesondere das Dateisystem, USB-Verbindungen, Internet-Verbindungen (inklusive Browser-Schutz), lokale Mailboxen, Downloads via http(s), Remote File-Systeme und sonstige Schnittstellen zur Nutzung von Wechselmedien.

ANFORDERUNG	BESCHREIBUNG
Herstellerunterstützung	Der Hersteller muss Sicherheits- und Signaturupdates regelmäßig, mindestens täglich automatisiert bereitstellen. Der Hersteller muss einen angemessenen Support bieten.
Mobiler Einsatz **(gilt nur für Produkte zum Schutz von Schadsoftware von Arbeitsplatzsystemen)**	Der Schutz vor Schadsoftware im mobilen Einsatz von Arbeitsplatzsystemen muss gewährleistet werden können. Die Funktionsweise des Produkts muss auch dann weiterhin gegeben sein, wenn ein Client nicht mehr mit dem Netzwerk verbunden ist. Die sich im mobilen Einsatz befindlichen Systeme müssen direkt mit Updates für die Virensignaturen des Herstellers versorgt werden können.

Tabelle 1: Anforderungen an Leistungsfunktionalitäten

3.3. Virenschutzarchitektur

Die einzusetzende Gesamtlösung für den Schutz vor Schadsoftware muss einen modularen Ansatz verfolgen und somit Produkte für den Schutz vor Schadsoftware für spezielle Umgebungen zur Verfügung stellen. Hierbei sind verschiedene Produkte für

- Schutz vor Schadsoftware für den Internetverkehr (DNS und Firewall),
- Schutz vor Schadsoftware für E-Mail am Mailgateway und
- Schutz vor Schadsoftware für alle Server- und Clientsysteme, auch virtuelle Systeme

einzusetzen.
Für die einzelnen Module sollten jeweils unterschiedliche Produkte von unterschiedlichen Herstellern eingesetzt werden, um die Erkennungsrate zu steigern und somit den Schutz zu erhöhen.

3.3.1. Schutz mobiler Arbeitsplatzsysteme

Für mobile Arbeitsplatzsysteme ist sicherzustellen, dass die Funktions- und Wirkungsweise des Schutzes vor Schadsoftware im mobilen Einsatz gewährleistet bleibt und nicht umgangen beziehungsweise deaktiviert werden kann. Es ist sicherzustellen, dass die Erkennung einer Schadsoftware auf einem mobilen System an die zentrale Managementkonsole gemeldet wird. Ist dies im mobilen Einsatz nicht möglich, muss die Meldung spätestens dann erfolgen, wenn sich das mobile System wieder mit dem Netzwerk der VAV verbindet. Wird eine Schadsoftware jedoch nicht eliminiert, so darf das System nicht an das VHV Netz gekoppelt werden, es sei denn, ein sicheres Quarantänenetzwerk ist hierfür bereitgestellt.
Weiterhin gilt für Smartphone- und Tablet-Geräte die folgende Vorgabe: Sofern ein realistisches Angriffsszenario für die Geräte besteht, ist ein entsprechender Schutz vor Schadsoftware gemäß den Vorgaben dieser Richtlinie direkt auf den Geräten zu etablieren. Werden iOS basierende Geräte betrieben, muss aktuell kein direkt auf den Geräten etablierter Schutz vor Schadsoftware sichergestellt werden. Ein angemessener Schutz wird dann innerhalb des Netzwerks der VAV sichergestellt.

3.3.2. Schutz am Mail-Gateway

Sämtliche Dateien, die mit Schadsoftware behaftet, ausführbar (inklusive Makros) und per Kennwort verschlüsselt sind, sind durch das E-Mail-Gateway in Quarantäne zu verschieben. Sofern E-Mails aufgrund der genannten Restriktionen abgewiesen wurden, sollten sowohl Absender als auch Empfänger automatisiert benachrichtigt werden.
Eine manuelle Überprüfung auf schadhafte Programme oder Programmteile ist nur durch qualifiziertes Personal nach einem Incident Request erlaubt. Die Überprüfung muss in einer gesicherten Umgebung stattfinden, um eine eventuelle Ausbreitung des Virus zu verhindern.

3.3.3. Schutz für den Internetverkehr (DNS und Firewall)

Im Folgenden sind die Vorgaben definiert, die ausschließlich für den Schutz vor Schadsoftware für den Internetverkehr gelten.
Es wird ein DNS-Filtering-System (Blue Shield Umbrella) eingesetzt, sodass Schadsoftware bereits vor der Firewall blockiert wird. Die Domains werden mit künstlicher Intelligenz, predictive und evolutionären Algorithmen analysiert und es wird insbesondere vor Advanced Malware, Ransomware, Botnets, Command & Control, Phishing, Cryptp Mining und Zero Day Exploits geschützt.
Die Firewall (Sonicwall) verfügt zusätzlich zu den normalen Firewall-Funktionen über Advanced Threat Protection, Intrusion Prevention, Malware-Schutz, Anwendungsidentifizierung und Filterung von Webinhalten.

3.4. Quarantänezone

Für jedes einzelne Modul ist eine Quarantänezone zu etablieren, (mit Ausnahme am Firewallsystem), welche die folgenden Vorgaben umsetzt:

- Die Quarantänezone muss ein abgeschotteter Bereich eines IT-Systems sein, mit dem nicht ohne weiteres ein Datenaustausch stattfinden kann.
- Die Quarantänezone ist je nach Schutzbedarf des zugehörigen IT-Systems logisch oder physisch von restlichen Bestandteilen des IT-Systems zu separieren.
- Die Daten innerhalb der Quarantänezone sollten so durch den Virenscanner verschlüsselt werden, dass eine Ausführung und ein Wirken der Schadsoftware ausgeschlossen sind.
- Bei Arbeitsplatzsystemen ist ein Zugriff durch Benutzer auf die Quarantänezone zu unterbinden.
- Ein Wiederherstellen von Dateien aus der Quarantänezone muss für den Fall von fälschlicherweise erkannten Softwarebestandteilen gewährleistet sein.
- In der Quarantänezone sollten Funktionen zur risikofreien Analyse von Dateien gewährleistet werden.

3.5. Monitoring

Der oder die verantwortlichen IT-Mitarbeiter müssen täglich auf neue Virenmeldungen prüfen. Ausgenommen hiervon ist der Virenschutz am Mailgateway, da erkannte schadhafte Anhänge nicht zugestellt werden. Im Falle eines Trojaners ist die Stabstelle Datenschutz und Informationssicherheit unverzüglich zu unterrichten.

3.6. Betriebskonzept Malwareschutz

Die Betriebskonzepte für Proxyserver, Mailgateway, Client- und Serversysteme müssen vom IT-Betrieb vor Inbetriebnahme erstellt werden. Folgende Punkte sind in den Konzepten zu berücksichtigen:

- Wie wird ein Befall mit Malware gemeldet, erkannt und welche Aktionen werden eingeleitet
- Wann und auf welche Weise werden die Virenschutzdefinitionen aktualisiert
- Wann und auf welche Weise wird das Programm selbst aktualisiert
- Welche Aktivitäten werden ergriffen, wenn eine Aktualisierung des Programms oder der Virenschutzdefinitionen nicht vollständig durchgeführt wurde
- Wer welche Rechte auf der Scan Engine hat
- Welche Reports wann erstellt werden und wer die Empfänger sind
- Welche Systeme aus welchem Grund nicht oder nur teilweise gescannt werden können
- Wie die Funktionsfähigkeit überwacht wird und Ausfälle behandelt werden

Ebenso gehört in das Betriebskonzept, wer für die einzelnen Punkte verantwortlich ist. Dies können eine einzelne Person oder eine Gruppe sein. Bei einer einzelnen Person muss eine Vertretung sichergestellt werden.
Sofern genehmigte Sonderregelungen mit der Stabstelle Datenschutz und Informationssicherheit abgestimmt sind und die Ausnahmen auf Dauer Bestand haben sollen, sind diese im Betriebskonzept mit zu berücksichtigen.