Arbeitsrichtlinie Handhabung technischer Schwachstellen

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Handhabung technischer Schwachstellen
Version	21.0
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	01.12.2020
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
20.0	01.12.2020	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 20.0.	Daniel Fürdauer
21.0	22.11.2021	In Anlehnung an die Anpassungen der entsprechenden Arbeitsrichtlinie der VHV in der Version 21.0: Anpassung der Prozesse zur Priorisierung von Schwachstellen, sowie der Abgrenzung zum Patchmanagement.	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

Aufgrund der hohen Komplexität von IT-Systemen und Softwareprodukten sind Fehler bei der Entwicklung nicht zu vermeiden. Moderne Entwicklungsprozesse unterstützen zwar gezielt bei der Programmierung sicherer Software; dennoch können Schwachstellen von Zeit zu Zeit auftreten. Daher bedarf es geordneter Prozesse und klarer Verantwortlichkeiten zur Erkennung und Behandlung von Schwachstellen, um Sicherheitsrisiken für das Unternehmen zu vermeiden. Die Handhabung von Schwachstellen ist als reaktive Behandlung von Schwachstellen zu implementieren und ersetzt keine proaktiven Regelprozesse wie Patching oder die Härtung von Systemen.

2. GELTUNGSBEREICH

Diese Richtlinie gilt 3 Monate nach dem jeweiligen Änderungsdatum (siehe „Dokumentenhistorie“), frühestens jedoch 2 Jahre nach erstmaliger Freigabe (siehe „Dokumenteneigenschaften“).

3. MANAGEMENT TECHNISCHER SCHWACHSTELLEN

Um auf technische Schwachstellen in IT-Systemen zeitnah reagieren zu können, sind potenzielle Schwachstellen durch Regelprozesse zu identifizieren. , angemessen zu bewerten, nach ihrer Kritikalität zu priorisieren und zu behandeln. Die Ergebnisse sind im Anschluss zu messen.

Durch ein zentrales Schwachstellenmanagement ist das Risiko der Ausnutzung von Schwachstellen zu minimieren.
Weiterhin sind Systemadministratoren und Entwickler dafür verantwortlich, die von ihnen betreuten IT-Systeme und Anwendungen regelmäßig auf offene Schwachstellen und einzuspielende Patches zu überprüfen und diese zu schließen bzw. einzuspielen.

3.1. Schwachstellen-Engineer

Der Schwachstellen-Engineer ist für die Konfiguration des Schwachstellenscanners, die zeitliche Planung, Abstimmung und Ausführung von Scan-Vorgängen verantwortlich.
Hauptaufgaben:

- Konfiguration des Scanners nach den Vorgaben dieser Arbeitsrichtlinie und etwaiger ergänzender Vorgaben des Schwachstellen-Managers.
- Durchführung und Überwachung der Schwachstellenscans.
- Die mit der Schwachstelle verbundenen Risiken sind durch den Schwachstellen-Engineer festzustellen und die erforderlichen Abhilfemaßnahmen zu bestimmen.
- Zeitliche Planung der Schwachstellenbehebung mit den Produktverantwortlichen.
- Erstellung von Berichten über den aktuellen Stand der erkannten Schwachstellen und der Planungen zur Behebung.
- Technische Beratung zur möglichen Behandlung von Schwachstellen.

Nebenaufgaben:

- Ansprechpartner für Performanceprobleme während der Schwachstellenscans.
- Beratung der Produktverantwortlichen

3.2. Schwachstellen-Manager

Der Schwachstellen-Manager ist für die Etablierung einer risikoorientierten Überwachung der IT-Systeme auf Schwachstellen zuständig.
Hauptaufgaben:

- Erstellt Vorgaben zum Umfang, zum Zyklus und zur Tiefe des Scans.
- Berät, falls die Schwachstelle über die bestehenden IT-Servicemanagement Prozesse nicht geschlossen werden kann.
- Der Schwachstellen-Manager berät bei der Ermittlung der Risiken.
- Der Prozess zur Handhabung technischer Schwachstellen wird durch den Schwachstellen-Manager überwacht, um seine Wirksamkeit und Effizienz zu gewährleisten.

Nebenaufgaben:

- Prüft die Möglichkeit einer Risikoakzeptanz und erteilt ggf. notwendige Auflagen.

4. IDENTIFIZIEREN

Um IT-Systeme vor Sicherheitslücken zu schützen, sind diese IT-Systeme vollständig zu erfassen und regelmäßig mit herstellerspezifischen Soll-Zuständen, Best-Practice (z. B. CIS-Benchmark) und gegen bekanntgewordene Sicherheitslücken zu überprüfen. Um eine ganzheitliche Identifizierung von Sicherheitslücken durchzuführen, ist diese zeitnah, wirksam, systematisch und reproduzierbar durchzuführen und sollte mittels technischer Lösungen erfolgen, um eine ganzheitliche Identifizierung von Sicherheitslücken sicherzustellen.

4.1. Auslöser

Die Durchführung eines Schwachstellen-Scans ist aufgrund verschiedener Auslöser notwendig.

4.1.1. Inbetriebnahme eines neuen Systems

Vor der produktiven Inbetriebnahme eines neuen IT-Systems sind Schwachstellen-Scans durchzuführen.

4.1.2. Wesentliche Änderungen am System

Werden an einem IT-System wesentliche Änderungen vorgenommen (z.B. Versionswechsel der Anwendung), ist das IT-System auf potenzielle neue Schwachstellen zu scannen.

4.1.3. Regelmäßiger Scan

Um den sich ständig ändernden Angriffsszenarien und neu bekannt gewordenen Schwachstellen entgegenzuwirken, sind durch den Schwachstellen-Manager regelmäßige und risikoorientierte[1]

[1] Risikoorientiert berücksichtigt z.B. Faktoren wie durchgeführte Risikoanalysen, aufgetretene Sicherheitsvorfälle und geschäftskritische Prozesse, etc.

Überprüfungen auf Schwachstellen aller Systeme zu planen und vom Schwachstellen Engineer durchzuführen.

4.1.4. Wiederholung eines Scans

Zumindest bei Schwachstellen der Kritikalität „critical“ (siehe unter 5.1) wird empfohlen, die Wirksamkeit der Maßnahme durch einen erneuten Scan zu verifizieren.

5. BEWERTEN

Sicherheitslücken sämtlicher IT-Systeme sind einschließlich der Betrachtung von Schwachstellen, Fehlkonfigurationen und anderen Sicherheitsindikatoren zu bewerten.

5.1. Bewertung von Schwachstellen

Die Bewertung von Schwachstellen orientiert sich an der potenziell möglichen Auswirkung, welche aus der gefundenen Schwachstelle resultiert. Die Festlegung der Bewertung ergibt sich aus der mit dem Schwachstellen-Scanner ermittelten Kritikalität und kann vom Schwachstellen-Engineer, zusammen mit dem Schwachstellen-Manager und unter Zuhilfenahme weiterer Informationen individuell angepasst werden.
Die nachfolgende Tabelle legt Kriterien für die Bewertung der Kritikalität einzelner Schwachstellen fest:

KRITIKALITÄT	BESCHREIBUNG
Critical	**Exploit-Code ist öffentlich verfügbar und / oder die Schwachstelle wird aktiv ausgenutzt** • Schwachstelle kann ohne oder mit geringer Authentifizierung ausgenutzt werden • Fernzugriff • Einschleusen und Ausführen von Code möglich • Zugriff auf vertrauliche Daten • Möglichkeit Daten zu manipulieren, zu zerstören oder das System offline zu nehmen • Beeinträchtigung weiterer Systeme
High	**Aktuelle Exploits und / oder Angriffe sind nicht bekannt, aber möglich** • Schwachstelle kann ohne oder mit geringer Authentifizierung ausgenutzt werden • Fernzugriff • Einschleusen und Ausführen von Code möglich • Zugriff auf vertrauliche Daten • Möglichkeit Daten zu manipulieren, zu zerstören oder das System Offline zu nehmen • Beeinträchtigung weiterer Systeme
Medium	**Ausnutzen der Schwachstelle mit moderatem Fachwissen möglich** • Fernzugriff, mit oder ohne Authentifizierung • Teilweise Zugriff auf interne Daten, Daten können zerstört werden

Low	**Ausnutzen der Schwachstelle nur mit Experten oder Insiderwissen möglich** • Lokale Schwachstellen • Benötigt eine Authentifizierung • Möglicher Zugriff auf interne Daten • Keine Möglichkeit Daten zu manipulieren und / oder zu löschen

Tabelle 1: Kritikalität von Schwachstellen

Die Kritikalität einer einzelnen Schwachstelle baut grundsätzlich auf dem CVSS (Common Vulnerability Scoring System) auf. In diesem Score wird folgende Metriken betrachtet: Angriffsvektor, Angriffskomplexität, benötigte Berechtigungen, Benutzerinteraktion, Auswirkung, Vertraulichkeit, Integrität und die Verfügbarkeit.
Um ein reelles und aktuelles Lagebild von einer Schwachstelle zu erlangen, sind bei der Bewertung einer Schwachstelle neben dem CVSS auch Umstände wie bestehende Exploits und Malwarekits, das Alter der Schwachstelle und die aktuellen Bedrohungslage zu dieser Schwachstelle mit zu bewerten.

6. PRIORISIEREN

Eine Priorisierung der Schwachstellen bzw. der Behandlung offener Schwachstellen sollte risikoorientiert erfolgen. Das Risiko, welches durch eine Schwachstelle ausgelöst wird, ist grundsätzlich im Kontext des betroffenen IT-Systems zu sehen. Um dies gewährleisten zu können, sind IT-Systeme in Prioritätsklassen einzuteilen. Hierbei sind IT-Systeme zu priorisieren, welche in Geschäftsprozesse eingebunden sind, die einen hohen Schutzbedarf aufweisen.
Gefährdungen werden im Kontext beurteilt, um Behebungsmaßnahmen anhand der IT-System-Priorität, Bedrohungskontext und Schweregrad der Sicherheitslücken zu priorisieren.

6.1. Risikoorientierte Priorisierung von Schwachstellen

Die nachfolgende Tabelle stellt die umzusetzenden Zeitfenster für die Schließung der Schwachstelle dar und berücksichtigt dabei neben der Kritikalität der zu schließenden Schwachstelle auch die Lokation des betroffenen Systems und die Art der Software.

KRITIKALITÄT FÜR VAV	LOKATION DES SYSTEMS	SOFTWARETYP	ZEITFENSTER FÜR PATCHUMSETZUNG	AUSNAHME
Critical	Alle	Alle	Innerhalb **48 Stunden**	**Einmalig möglich** (durch Risikoverantwortlichen in Abstimmung mit Stabstelle Datenschutz & Informationssicherheit)
Low, Medium, High	DMZ	Betriebssystem (Windows, Linux etc.)	**5-mal jährlich** aber mindestens alle 90 Tage	
		Anwendungen (Web-, Applikationsserver etc.)		

		Hardware (iOS, Firmware etc.)		
	LAN (internes Netz)	Betriebssystem (Windows, Linux etc.)	**4-mal jährlich** aber mindestens alle 120 Tage	**Einmalig möglich** (durch Risikoverantwortlichen)
		Anwendungen (Datenbanken, Fach-, Clientanwendungen etc.)		
		Hardware (iOS, Firmware etc.)		

Tabelle 2: Umsetzungsfristen von Schwachstellen

Sollten bei einem initialen Schwachstellenscan eine Vielzahl von Sicherheitslücken erkannt werden, kann die Überschreitung der Behebungsfristen akzeptabel sein. Die Behebung hat dabei nach der Kritikalität priorisiert zu erfolgen.

6.2. Priorisieren von Maßnahmen

Sofern innerhalb einer Kritikalitätsstufe mehrere Schwachstellen oder mehrere von Schwachstellen betroffene IT-Systeme vorliegen, ist wie folgt vorzugehen:

- IT-Systeme die durch die Summierung von einzelnen Schwachstellen ein überproportional hohes Risiko darstellen
- Schwachstellen, welche eine hohe Kritikalität aufweisen
- Lösungen, die bei der Umsetzung eine signifikante Reduktion des Gesamtrisikos darstellen

Die Stabstelle Datenschutz und Informationssicherheit ist im Bedarfsfall bei der Priorisierung beratend hinzuzuziehen. Sofern eine Schwachstelle nicht innerhalb der festgelegten Zeiten geschlossen werden kann, ist dies der Stabstelle Datenschutz und Informationssicherheit unverzüglich mitzuteilen. Risiken, die durch den Aufschub der Schwachstellenbehandlung entstehen, sind im Risikobehandlungsplan aufzunehmen. Die Möglichkeit zur ad-hoc Berichterstattung an die Geschäftsleitung bleibt hiervon unberührt.

7. BEHANDELN

Im Rahmen der Behandlung von Schwachstellen ist zu ermitteln, welche Lösung sich zur Behebung einer Schwachstelle (am sinnvollsten) umzusetzen lässt.

7.1. Behandlung von technischen Schwachstellen

Nach der Feststellung unbehandelter und offener technischer Schwachstellen sind zeitnah angemessene Abhilfemaßnahmen zu ergreifen. Die mit der Schwachstelle verbundenen Risiken sind

durch den Schwachstellen Engineer in Verbindung mit dem eingesetzten Tool festzustellen und die erforderlichen Abhilfemaßnahmen zu bestimmen. Der Schwachstellen Manager berät bei der Ermittlung der Risiken.
Sämtliche Maßnahmen sind über die Regelprozesse der Änderungssteuerung (Incident-, Change- und Problemmanagement) vom Schwachstellen Engineer anzustoßen.
Alle durchgeführten Aktivitäten, Bewertungen und Schwachstellen sowie die Maßnahmenplanung sind zu dokumentieren.
Der Prozess zur Handhabung technischer Schwachstellen wird durch den Schwachstellen Manager überwacht, um seine Wirksamkeit und Effizienz zu gewährleisten.
Die Behandlung von Schwachstellen muss ggf. für jede Schwachstelle sowie für jedes Informationssystem individuell zu gestalten sein.
Zur Behandlung von Schwachstellen stehen grundsätzlich mehrere Möglichkeiten zur Verfügung, wobei eine dauerhafte Behandlung einer temporären Behandlung vorzuziehen ist:

7.1.1. Einspielen von Sicherheitspatches

Stellt der Hersteller eines Softwareprodukts zur Behebung einer Sicherheitslücke ein Sicherheitspatch zur Verfügung, so ist dieser zeitnah entsprechend den Vorgaben der Arbeitsrichtlinie Sicherheitspatches einzuspielen. Die Definition „zeitnah“ richtet sich nach der Tabelle oben.
Für selbst entwickelte Softwareprodukte ist zu prüfen, wie schnell die Sicherheitslücke durch eine eigene Entwicklung geschlossen werden kann. Hierbei ist ebenfalls die Kritikalität der Schwachstelle zu berücksichtigen.

7.1.2. Konfiguration der betroffenen Informationssysteme

Bei Konfigurationsfehlern sollten die bestehenden Konfigurationen auf Basis der Vorgaben in der "Arbeitsrichtlinie Härtung" und aufgrund von Best-Practice-Empfehlungen berichtigt werden. In manchen Fällen stellt der Hersteller, falls aktuell keine Patche verfügbar sind, sogenannte „Workarounds“ bereit. Hierbei handelt es sich um kurzfristige Konfigurationsänderungen, welche die Schwachstelle temporär beheben oder die Auswirkung abmildern. Keinesfalls dürfen diese „Workarounds“ als endgültige Lösung betrachtet werden. Nach spätestens 90 Tagen muss eine erneute Überprüfung stattfinden und verfügbare Patches eingespielt werden.

7.1.3. Virtuelles Patching

„Virtuelles Patching“ stellt eine schnell durchzuführende Möglichkeit dar, um bei noch ausstehenden Patchen Angriffe abzuwehren und das gefährdete IT-System abzuschirmen. Angriffe werden während des Transports abgefangen, so dass bösartiger Datenverkehr nicht mehr die eigentliche Anwendung erreicht. Der eigentliche Quellcode des IT-Systems selbst wird dabei nicht geändert, das Ausnutzen der Schwachstelle wird jedoch verhindert. Nach spätestens 90 Tagen muss eine erneute Überprüfung stattfinden und verfügbare Patches eingespielt werden.

7.1.4. Zugangsbeschränkung

Für aktuell gefährdete IT-Systeme kann der Zugang temporär beschränkt werden. Durch den verkleinerten Personenkreis, welcher Zugang zu den betroffenen IT-Systemen hat, kann sich auch die Eintrittswahrscheinlichkeit der Ausnutzung der Schwachstelle reduzieren. Betroffene IT-Systeme können beispielsweise in Insellösungen betrieben werden.

7.1.5. Abschalten von Funktionen

Es muss grundsätzlich überlegt werden, in wie weit Funktionen wie Services oder Dienste abgeschaltet werden können. Das gilt insbesondere für Betriebssysteme und Softwareprodukte mit einem großen Funktionsumfang. In vielen Fällen handelt es sich hierbei um Standardfunktionen, die bei der Installation mit installiert werden.

7.2. Sonstige risikominimierende Maßnahmen

Auch ein kurzfristiger und temporärer Wechsel eines Softwareprodukts kann als risikominimierende, alternative Maßnahme gelten.

8. MESSEN

Um auf Entwicklungen aktiv reagieren zu können, sind Schwachstellen und daraus resultierende Risiken regelmäßig zu messen und zu kommunizieren, um die Risikoreduzierung voranzutreiben.