Arbeitsrichtlinie Sicherheitspatches

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Sicherheitspatches
Version	21.0
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	16.10.2019
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	16.10.2019	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 19.0.	Daniel Fürdauer
20.0	04.12.2020	Definition der Tests von Sicherheitspatches geschärft in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 20.0	Daniel Fürdauer
21.0	19.11.2021	Redaktionelle Änderungen, Hervorhebung des proaktivem Patchings.	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

Im Rahmen dieser Arbeitsrichtlinie werden Softwareprodukte und Hardwareressourcen mit Softwareteilen betrachtet, die mit Sicherheitspatches versorgt werden müssen. Ein fehlender oder vernachlässigter Umgang mit Sicherheitspatches führt zu Sicherheitslücken und damit zu möglichen Angriffspunkten. Sicherheitspatches tragen daher maßgeblich zur Wiederherstellung von Verfügbarkeit, Vertraulichkeit, Authentizität und Integrität des jeweiligen Produkts bei.

2. ABGRENZUNG

Ein Patch ist ein generelles Softwareupdate, welches Fehlfunktionen aufgrund von Fehlern in der Entwicklung in einer Software behebt. Fehlerhafte Konfigurationen oder organisatorische Rahmenbedingungen werden nicht betrachtet.
Im Rahmen der Produktpflege ist ein Patch in drei Arten zu unterteilen:

- **Sicherheitspatch**
  Ein Sicherheitspatch behebt eine Schwachstelle im Produkt. Hierunter können Zero Day Exploits, aber auch schon längerfristig bekannte Sicherheitslücken und Schwachstellen zählen.
- **Bug Fix (Funktionaler Patch)**
  Ein Bug Fix behebt aktuelle Fehler in Produkten. Darunter fallen Performance Updates, die Behebung von Fehlern im Programm selbst sowie die Behebung von funktionellen Mängeln.
- **Update (Fähigkeits-Patch)**
  Diese Art von Patches stellen eine Erweiterung, Änderung oder Ergänzung des Produktes dar.

Bei der Bereitstellung von Patches, wird diese Unterteilung nicht von jedem Hersteller berücksichtigt. Ob Patches einzeln zur Verfügung gestellt werden oder eine Bündelung der einzelnen Patches in Release- oder Update-Paketen erfolgt, obliegt dem Hersteller.
Die nachfolgende Richtlinie beschreibt, welche Anforderungen beim Umgang mit Sicherheitspatches zu beachten sind.

3. ALLGEMEINE ANFORDERUNGEN

3.1. Überprüfung des Patch-Stands

Um existierende Produkte auf dem aktuellen Stand zu halten, ist der Ist-Zustand der Produkte regelmäßig mit dem herstellerspezifischen Soll-Zustand abzugleichen. Die Pflege von Produkten mit aktuellen Patches ist unabhängig vom Bekanntwerden von Sicherheitslücken in den betreffenden Systemen sicherzustellen und hat kontinuierlich bzw. während des gesamten Produktlebenszyklus zu erfolgen. Die Pflege von Produkten mit Patches ist proaktiv zu planen und durchzuführen. Eine nachgelagerte Kontrolle kann mittels technischer Lösungen wie einem Schwachstellenmanagement oder organisatorisch erfolgen und ist pro Produkt individuell zu betrachten. Dieser Abgleich verschafft einen aktuellen Überblick über den Patch- und Sicherheitsstand der im Einsatz befindlichen Produkte und deckt offene Sicherheitslücken auf.

3.2. Quellen

Stehen offizielle Sicherheitspatches zur Verfügung, muss die Authentizität und Integrität dieser Patches sichergestellt werden. Als Bezugsquelle von Sicherheitspatches ist grundsätzlich eine vertrauenswürdige Herkunft zu nutzen. Sicherheitspatches zu Produkten sind daher ausschließlich vom Hersteller oder von durch den Hersteller offiziell freigegebene Quellen zu beziehen.

3.3. Kritikalität

Sicherheitspatches dienen der Schließung öffentlich bekannter Sicherheitslücken in Produkten. Mit steigender Kritikalität der offenen Sicherheitslücke steigt gleichzeitig auch die Anforderung auf ein möglichst kurzes Zeitfenster zwischen der Bereitstellung des Patches und dessen Einspielung auf sämtlichen Systemumgebungen. Gleichzeitig ist jedoch zu prüfen und zu testen, ob ein Sicherheitspatch ungewollte Auswirkungen auf das System oder Seiteneffekte auf die Systemlandschaft birgt.
Es müssen technische und organisatorische Möglichkeiten geschaffen werden, um bei aktiven Störungen, Angriffen oder Notfällen kritische Sicherheitspatches unmittelbar einspielen zu können.
Die nachfolgende Tabelle gibt wesentliche Anhaltspunkte zur Bewertung der Kritikalität einer Schwachstelle, die mit dem Sicherheitspatch geschlossen werden soll.

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 Patches

3.4. Umsetzungsfenster

Neben der Kritikalität des Sicherheitspatches ist auch die Erreichbarkeit und Angreifbarkeit der Systeme der VAV bei der Definition eines Zieltermins zu berücksichtigen.
Die nachfolgende Tabelle stellt die umzusetzenden Zeitfenster für die Umsetzung der Sicherheitspatches dar und berücksichtigt dabei neben der Kritikalität der zu schließenden Sicherheitslücke auch die Lokation des betroffenen Systems und die Art der Software.

KRITIKALITÄT FÜR VAV	LOKATION DES SYSTEMS	SOFTWARETYP	ZEITFENSTER FÜR PATCHUMSETZUNG	AUSNAHME / RISIKOÜBERNAHME
Critical	Alle	Alle	Innerhalb **48 h**	**Nicht möglich**
Low, Medium, High	DMZ	Betriebssystem (Windows, Linux etc.)	**5-mal jährlich** aber mindestens alle 90 Tage	**Einmalig möglich** (durch Risikoverantwortlichen in Abstimmung mit der Stabstelle Datenschutz und Informationssicherheit)
		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 Sicherheitspatches

Unter bestimmten Umständen kann es notwendig sein, dass die Umsetzung eines Sicherheitspatch-Zyklus nicht fristgerecht durchgeführt werden kann oder soll. Dieser Aufschub der Umsetzung kann einmalig, also bis zur Fristerreichung des Folgetermins, gewährt werden. Zum Zeitpunkt des folgenden Umsetzungszeitfensters müssen die aufgeschobenen, sowie auch die hinzugekommenen Sicherheitspatches eingespielt werden. Die Entscheidung, einen Sicherheitspatch nicht innerhalb der festgelegten Zeiten einzuspielen, bedarf einer Risikoübernahme durch den Risikoverantwortlichen entsprechend der Risikoübernahmeprozesse (siehe hierzu auch die Konzernrichtlinie Informationssicherheit).

3.5. Test

Im Gegensatz zu Funktionalen- und Fähigkeitspatches, sowie Release Updates, haben Sicherheitspatches in der Regel keine Auswirkungen auf den Anwendungsbetrieb. Da der Fokus ausschließlich auf dem Schließen offener Sicherheitslücken und Schwachstellen liegt.

Um negative Seiteneffekte auf das Produkt selbst, Schnittstellen und Geschäftsprozesse abwägen und abfangen zu können, sind Sicherheitspatches zu testen. Dieser Umstand ist der Dynamik, Individualität und Komplexität der IT-Landschaft geschuldet.
Sollte sich im Rahmen der Tests herausstellen, dass das Einspielen des Patches ein größeres Problem darstellt, als die zu patchende Sicherheitslücke selbst birgt, ist das Patchen so lange zurück zu halten bis diese Herausforderung gelöst ist.
Grundsätzlich sind Sicherheitspatches, im Rahmen zur Aufrechterhaltung der Qualität der eingesetzten Produkte, entsprechend der Prozesse Patch- und Changemanagement einzuspielen.

3.6. Dokumentation

In jedem Fall muss dokumentiert werden, wann, von wem und aus welchem Anlass Sicherheitspatches eingespielt wurden. Aus der Dokumentation muss sich der aktuelle Patchlevel des Systems jederzeit und schnell ermitteln lassen, um beim Bekanntwerden von Schwachstellen schnell Klarheit darüber zu erhalten, ob das System dadurch gefährdet ist.

3.7. Datensicherung und Rollback-Konzept

Vor der Installation eines Patches sollte stets eine Datensicherung, ein Snapshot oder eine gleichwertige Sicherung des Systems erstellt werden, die es bei Problemen ermöglicht, den vorherigen Zustand wiederherzustellen. Dies gilt insbesondere dann, wenn ausführliche Tests aus Zeitgründen oder mangels eines geeigneten Testsystems nicht durchgeführt werden können.
Des Weiteren ist ein Rollback-Konzept zu implementieren, das es ermöglicht, flexibel auf Herausforderungen während laufender Updates reagieren zu können.

3.8. Keine Installation eines Sicherheitspatches

Treten im Rahmen von Tests oder durch andere Abhängigkeiten schwerwiegende Probleme auf, die das Einspielen eines Sicherheitspatches verhindern, so muss das Risiko einer daraus resultierenden offenen Sicherheitslücke durch adäquate Maßnahmen auf ein akzeptables Maß reduziert werden. Hierbei sind sowohl der Verhinderungsgrund selbst, dass daraus resultierende Schadenpotenzial und die risikominimierenden Maßnahmen zu dokumentieren.
Risikominimierende Maßnahmen können beispielsweise sein:

- Abschaltung von Diensten, Funktionen und Produkten, die von der Schwachstelle betroffen sind,
- Segmentierung der Schwachstelle mittels Firewall, Benutzerrechten oder Netzsegmenten,
- Einrichtung einer erhöhten Überwachung und Definition von möglichen Gegenmaßnahmen im Falle von Unregelmäßigkeiten oder
- organisatorische Maßnahmen wie Schulungen oder Sensibilisierungen der Mitarbeiter.

Die Maßnahmen müssen so beschaffen sein, dass sie zu einer Minimierung des Schadenpotenzials führen und einen adäquaten Ersatz, zu dem nicht eingespielten Sicherheitspatch bilden.
Dabei ist zu beachten, dass sich einzelne aus Sicherheitslücken entstehende Schwachstellen gegenseitig addieren können und die Gefährdung der IT-Landschaft somit weiter zunehmen kann.