Arbeitsrichtlinie Härtung von Systemen und Anwendungen

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern

Version 21.0

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Härtung von Systemen und Anwendungen
Version	21.0
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	16.10.2020
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	16.10.2020	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 19.0.	Daniel Fürdauer
21.0	11.11.2021	Review ohne Änderungen	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

ABKÜRZUNGSVERZEICHNIS

BSI ..... Bundesamt für Sicherheit in der Informationstechnik

CIS ..... Center for Internet Security

NIST ..... National Institute of Standard and Technology

1. EINLEITUNG

Moderne IT-Systeme sind im täglichen Betrieb einer Vielzahl von Gefährdungen ausgesetzt. Oft nutzen erfolgreiche Angriffe bestimmte Fehlkonfigurationen einzelner oder mehrerer Systemkomponenten aus. Ein modernes System hält herstellerseitig Einstellungsmöglichkeiten bereit, die soweit verändert werden können, dass es für einen Angreifer erschwert wird, die aufgestellten Barrieren erfolgreich zu überwinden. Unter einer Härtung, auch „Hardening“ genannt, versteht man die Entfernung aller Softwarebestandteile und Funktionen, die zur Erfüllung der vorgesehenen Aufgabe durch das Programm nicht zwingend notwendig sind, mit dem Ziel, Sicherheitsrisiken zu minimieren. Die nachfolgende Arbeitsrichtlinie beschreibt den Härtungsprozess inklusive der dafür notwendigen Rollen und Verantwortlichkeiten.

2. GELTUNGSBEREICH

Diese Richtlinie findet Anwendung auf Betriebssysteme, Virtualisierungs-Hosts, Datenbanken, Webserver und Middleware-Komponenten sowie branchenunabhängige Standardlösungen wie z. B. Exchange Server oder Microsoft Office. Zusammenfassend werden diese Systeme im Weiteren als „Standardinfrastruktursysteme“ bezeichnet.

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

3. HÄRTUNGSVORGABEN

Die Härtungsvorgaben werden ausschließlich von der Stabstelle Datenschutz und Informationssicherheit festgelegt. Die Vorgaben sind besonders:

- CIS Benchmarks,
- Best Practices (z. B. NIST)
- Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
- Herstellervorgaben.

Die Härtung muss durch den IT-Betrieb erfolgen.

3.1. Neueinführung von Standardinfrastruktursystemen

3.1.1. Existierende Härtungsstandards

Die Neueinführung von Standardinfrastruktursystemen darf ausschließlich durch den IT-Betrieb erfolgen. Der IT-Betrieb hat sicherzustellen, dass neue Standardinfrastruktursysteme ausschließlich gehärtet ausgeliefert werden, wobei die Härtung bis zum ersten fachlichen Test erfolgt sein muss.
Für die Standardinfrastruktursysteme sind in aller Regel Best Practices für die Härtung der Systeme verfügbar. Die Stabstelle Datenschutz und Informationssicherheit stellt dem IT-Betrieb entsprechende Härtungsvorgaben zur Verfügung. Der IT-Betrieb muss die in diesen technischen Vorgaben beschriebenen Sicherheitsparameter so vollständig wie möglich umsetzen.
Die Praxis zeigt, dass bedingt durch unternehmensspezifische und funktionale Anforderungen nicht immer alle Sicherheitsparameter umgesetzt werden können. In diesem Fall hat der IT-Betrieb die Nichtumsetzbarkeit nachvollziehbar zu begründen und etwaige risikominimierende Maßnahmen zu dokumentieren. Die Stabstelle Datenschutz und Informationssicherheit bewertet im Anschluss das verbleibende Restrisiko, das sich in der Abweichung zur Härtungsempfehlung begründet. Basierend auf der Höhe des Restrisikos kann eine Risikoübernahme durch den Risikoverantwortlichen erfolgen.

Daran anschließend teilt der IT-Betrieb die abgestimmte VAV-Standardkonfiguration (auch "Golden-Image" genannt), dem Schwachstellenengineer mit. Dieser pflegt die nicht umsetzbaren Sicherheitsparameter als genehmigte Ausnahmen in das neu zu erstellende Scan-Profil ein, um bei zukünftigen Scans nicht notwendige Schwachstellenwarnungen (sog. „False Positives“) zu vermeiden. Abschließend veranlasst der IT-Betrieb einen Scan mit dem Schwachstellenscanner auf das neue VAV-Standardsystem. Somit werden die Umsetzung und die Richtigkeit der Ausnahmen im Scan-Profil final geprüft. Der Schwachstellenengineer teilt diesen Schwachstellenbericht dem Auftraggeber des IT-Betriebs und der Stabstelle Datenschutz und Informationssicherheit mit.

3.1.2. Keine existierenden Härtungsstandards

Sollten für eine Anwendung keine Härtungsvorgaben veröffentlicht sein, sind die Sicherheitsparameter bzw. Einstellungen von dem IT-Betrieb gemeinsam mit der Stabstelle Datenschutz und Informationssicherheit einzustellen und diese zu dokumentieren.
Basierend auf der Risikobewertung wird durch die Stabstelle Datenschutz und Informationssicherheit die weitere Vorgehensweise mit der Linie bzw. dem Projekt abgestimmt und festgelegt. Eine Produktivsetzung ist vor der Umsetzung der vereinbarten Maßnahmen nicht zu empfehlen.
Hinsichtlich der Risikobewertung gelten die unter 3.1.1 gemachten Ausführungen.

3.2. Änderungen an Standardinfrastruktursystemen

Im Rahmen der regulären Anforderung von IT-Systemen liefert der IT-Betrieb gehärtete VAV-Standardsysteme aus. Diese sind nach den Vorgaben in Kapitel 3.1 abgesichert.
Auf den Standardinfrastruktursystemen werden neue Anwendungen installiert und konfiguriert. Unter Umständen müssen durch die Installation der neuen Softwarebestandteile oder besonderer funktionaler Anforderungen Sicherheitseinstellungen auf den Standardinfrastruktursystemen geändert werden, um die Zielfunktionalität zu erreichen. Diese Änderungen sind durch den IT-Betrieb als (Sammel-)Change zu dokumentieren.
Mit dem Ende der Umsetzungsphase veranlasst der IT-Betrieb einen Systemscan mit dem VAV-Schwachstellenscanner. Sofern sich im Report Abweichungen von der Konfiguration der ausgelieferten Standardinfrastruktursysteme ergeben, ist der Ergebnisbericht der Stabstelle Datenschutz und Informationssicherheit zu übermitteln. Basierend auf diesem Bericht bewertet die Stabstelle Datenschutz und Informationssicherheit die aus den Abweichungen vom Standardinfrastruktursystem resultierenden Risiken und stimmt mit der Linie bzw. dem Projekt die weitere Vorgehensweise ab.