

Template

OPS.1.1.3 Patch- und Änderungsmanagement

Herausgeber:

Handwerkskammer Rheinhessen
Dagobertstraße 2
55116 Mainz

Telefon: (06131) 9992 - 61
Telefax: (06131) 9992 - 861
E-Mail: j.schueler@hwk.de

Webseite: www.it-sicherheitsbotschafter.de

Stand: Juni. 2020

Baustein: Patch- und Änderungsmanagement (OPS.1.1.3)

Bausteine	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19
OPS.1.1.3 Patch- und Änderungsmanagement	X	X	X																

Sicherheitslücken und Neuerungen in Programmen erfordern zeitnahe Anpassungen und Aktualisierungen der Software. Ein fehlendes oder vernachlässigtes Patchmanagement führt zu Lücken in der Sicherheit einzelner Komponenten und damit zu möglichen Angriffspunkten. Aufgabe des Patchmanagements ist es allgemein, verändernde Eingriffe in Anwendungen, Infrastruktur, Dokumentationen, Prozessen und Verfahren steuer- und kontrollierbar zu gestalten.

OPS.1.1.3.A1 Konzept für das Patch- und Änderungsmanagement

Das Unternehmen hat ein Patchmanagement entwickelt und dokumentiert. Updates werden vom IT-Verantwortlichen geplant und nach Feierabend durchgeführt. Die Verfügbarkeit mobiler Geräte wird bei der Planung berücksichtigt.

Updates der Branchensoftware werden vom Dienstleister im Rahmen eines Wartungsvertrages durchgeführt. Der Patch-Level der auf der IT-Infrastruktur (Server, Clients, mobile Geräte) installierten Software wird über ein Softwaretool (SUMO) ermittelt. Die Verfügbarkeit von Updates wird regelmäßig überprüft.

Vor der Installation aller Updates wird als Rückfall-Lösung eine Sicherung auf ein externes Speichermedium durchgeführt. Die Installation der Updates wird in den Bemerkungen der Sicherung dokumentiert.

OPS.1.1.3.A2 Festlegung der Verantwortlichkeiten

Der IT-Dienstleister ist für das Patch-Management des Betriebssystems, der Anwendungen und der IT-Infrastruktur (Router, Switch etc.) verantwortlich. Die Verantwortung für das Patch-Management der Branchensoftware liegt beim IT-Dienstleister.

OPS.1.1.3.A3 Konfiguration von Autoupdate-Mechanismen

Updates des Betriebssystems werden zunächst automatisch heruntergeladen. Um Unterbrechungszeiten zu reduzieren wurden für Windows-Updates Nutzungszeiten festgelegt. In diesem Zeitraum werden keine Neustarts ausgeführt. Bei der Beschaffung neuer Komponenten werden die Update-Mechanismen überprüft und dokumentiert.

Prüfung: Patch- und Änderungsmanagement

Leitfragen	Ja	Nein	Prüfen
Gibt es einen Verantwortlichen für Sicherheits-Updates?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Werden Sicherheits-Updates regelmäßig eingespielt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Werden Windows-Updates zentral vorgenommen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sind Benutzer verpflichtet, Sicherheits- und Windows-Updates selbst durchzuführen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Wird die Durchführung der Software-Updates regelmäßig überprüft?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Werden Updates für Anwendungsprogramme getestet, bevor sie für die allgemeine Verwendung freigegeben werden?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Wurden alle Benutzer darauf hingewiesen, dass Programme aus dem Internet nur nach ausdrücklicher Genehmigung des Systemverwalters heruntergeladen und installiert werden dürfen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ist es den Benutzern ausdrücklich untersagt worden, eigene Programme auf den Firmen-PCs zu installieren?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>