Bayerisches Landesamt für
Datenschutzaufsicht

Patch Management im Alltag

Checkliste nach Art. 32 DS-GVO

Stand: 22. Juli 2020

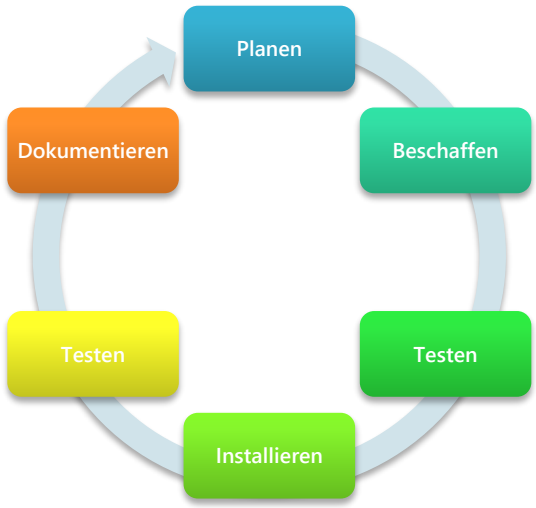
Ziel und Inhalt dieses Papiers

Die vorliegende Handreichung unterstützt vor allem kleine und mittlere Unternehmen dabei, festzustellen, wo und wie ein bedarfsgerechtes Aktualisieren der eingesetzten Softwaresysteme durchzuführen ist. Auch für Freiberufler, Selbstständige und andere Verantwortliche können einige Prüfpunkte dieser Checkliste von Nutzen sein. Das Risiko von Cyberattacken kann bereits durch regelmäßige Sicherheitsupdates erheblich reduziert werden, wenn vorhandene Schwachstellen erfolgreich geschlossen werden. Patch Management beschäftigt sich insbesondere mit dem Beschaffen, dem Testen und dem Einspielen wichtiger Updates für Anwendungen. Patches sind als Korrekturen zu betrachten, um gezielt bekannte Fehler und Schwachstellen zu beheben, die ansonsten den sicheren Betrieb gefährden. Aus datenschutzrechtlicher Sicht besteht nach Art. 32 DS-GVO eine gesetzliche Anforderung, personenbezogene Daten angemessen zu schützen. Verantwortliche müssen demnach Verfahren etablieren, um regelmäßig überprüfen, bewerten und evaluieren zu können, ob die eigenen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung auch tatsächlich wirksam sind. Patch Management spielt folglich eine zentrale Rolle im Sicherheitsumfeld und im Datenschutz. Maßnahmen aus dieser Handreichung zeigen, wie Patch Management in verschiedenen Bereichen einfach gelingen kann. Die aufgeführten Kriterien stellen einen Best-Practice-Ansatz dar und sollen in erster Linie als Einstieg für die wesentlichen Fachbereiche dienen.

Selbst-Check: Patch Management

1 Grundlagen

Das Installieren von Updates stellt zwar den wichtigsten Schritt beim Patch Management dar, bedarf aber noch Unterstützung: Vorhandene Patches müssen bekannt sein, zeitnah beschafft und auf den eigenen Systemen getestet sowie dokumentiert werden.



- **Planen:**
  Ein Plan zum Patch Management ist vorhanden (z. B. Welche Hard- und Software wird eingesetzt? Wer ist wofür zuständig? Welche Prozesse müssen beachtet werden?)
- **Beschaffen:**
  Informationen zu Updates werden gezielt gesucht bzw. Sicherheitshinweise ernst genommen; nur seriöse Quellen werden als Patch-Source genutzt
- **Testen:**
  Patches für kritische Anwendungen werden nicht ungetestet in der Produktivumgebung installiert, sondern erst nach ausreichender Prüfung eingespielt (Testumgebung); nach dem Patch wird der IT-Betrieb auf Funktionalität geprüft
- **Installieren:**
  Das Einspielen von Updates erfolgt kontrolliert, um unnötige Ausfallzeiten im alltäglichen Betrieb zu vermeiden
- **Dokumentieren:**
  Änderungen am System bleiben nachvollziehbar und können so jederzeit nachvollzogen und ggf. nachjustiert werden

>> Weitere Informationen:

www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/bausteine/OPS/OPS_1_1_3_Patch... (BSI)

2 Organisation

Patch Management ist keine Disziplin, die isoliert von anderen Fachbereichen der Organisation behandelt werden kann, da sie sich über alle Systeme und Dienste erstreckt. Eine angemessen Verankerung in den eigenen Organisationsstrukturen ist daher wichtig, um Patches nicht nur rechtzeitig und richtig einzuspielen, sondern auch negative Auswirkungen auf den Betrieb zu vermeiden.

- ☐ Patch Management ist fester Bestandteil der IT-Organisation
- ☐ Eigene Zuständigkeiten und Verantwortlichkeiten in der IT-Organisation sind definiert und kommuniziert (z. B. Wer patcht was? Wer kümmert sich um die Recherche von Schwachstellen?)

- ☐ Der Datenschutzbeauftragte versteht die Überprüfung der Wirksamkeit des Patch Managements als Teil seiner Kontrolltätigkeit
- ☐ Der IT-Sicherheitsverantwortliche (sofern vorhanden) erstellt die Patch Management-Regelungen oder ist zumindest dabei eingebunden
- ☐ Der Zeitaufwand für das Suchen, Testen und Einspielen von Patches wird im Alltag berücksichtigt (zeitliche Ressourcen)
- ☐ Ausreichende personelle und finanzielle Ressourcen zum Patchen stehen zur Verfügung (insbesondere bei Notfall-Patches)
- ☐ Eigene Systemlandschaft ist dokumentiert (Netzpläne)
- ☐ Überblick über die IT-Assets (sämtliche Hardware und Software) ist vorhanden (Inventarliste)
- ☐ Konzept zum Patch Management existiert (u. a. Update-Plan, Übersicht der eingesetzten Software und Versionsstände)
- ☐ Regelungen bestehen, wie Patches im Zweifel priorisiert werden (insb. auf Grundlage der damit verbundenen Risiken bei Nichteinspielung, z. B. aufgrund der Einstufung durch Hersteller oder CERT-Bund)
- ☐ Strukturen sind vorhanden, um die Auswirkungen von fehlerhaften Updates abzufedern (Ausfallsicherheit, redundante Systeme, Testumgebungen, Wiederherstellungsoptionen)
- ☐ Negative Auswirkungen von Patches, wie z. B. unbeabsichtigte Störungen der Systeme, Geschäftsprozesse und Datenstrukturen, werden aufgearbeitet und analysiert
- ☐ Vorbereitungen für geschäftskritische Anwendungen bei einer nicht patchbaren Sicherheitslücke werden getroffen (z. B. Planspiel für Zero Day Exploit)
- ☐ Änderungen durch Patches werden intern kommuniziert (ggf. Ausfallzeiten wegen Update, neue Funktionen)
- ☐ Bei neuer Hard- und Software sind Test- und Abnahmeverfahren etabliert

>> Weitere Informationen:

www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Schulung/OnlinekursITGrundschutz2018/... (BSI)

3 Informationsgewinnung

Ohne zeitnahe Kenntnis einer Sicherheitslücke besteht die Gefahr, dass Cyberkriminelle diese ausnutzen und sich Zugang zu Unternehmensdaten verschaffen. Es ist daher im eigenen Interesse zu gewährleisten, dass wesentliche Informationen zu Sicherheitslücken aktiv gesucht und wahrgenommen werden.

- ☐ Regelmäßige Auswertung und Dokumentation von Informationen zu Sicherheitslücken der eingesetzten Software wie Betriebssysteme, Office-Software, Fachanwendungen und Geräteumgebung (z. B. durch E-Mail-Newsletter, Herstellerveröffentlichungen, Fachmedien, Branchenplattformen, Sicherheitswarnungen)
- ☐ Bewertungssysteme für Schwachstellen sind bekannt und bei Bedarf werden ergänzende Informationen zur Schwere der jeweiligen Lücke eingeholt (wie z. B. CWSS, CVSS)
- ☐ Es wird geprüft, an welcher Stelle Auto-Update-Funktionen zur Verfügung stehen, um diese dann in Betracht zu ziehen
- ☐ Vollautomatischen Update-Mechanismen wird nicht blind vertraut, sondern diese werden überprüft und passend konfiguriert – jedoch werden diese grundsätzlich zur Nutzung bevorzugt
- ☐ Richtige Bezugsquellen werden ausgewählt – z. B. nicht auf Fake-Patches hereinfallen, die auf fremden Websites angeboten werden (Vertrauenswürdigkeit der Bezugsquelle prüfen, gerade bei Programmen ohne Auto-Update)
- ☐ Integrität und Authentizität von Softwarepaketen werden sichergestellt (etwa Prüfsumme, digitale Signatur)
- ☐ Verträge mit Anbietern werden geprüft (In welchem Zyklus sind diese verpflichtet, Updates bereitzustellen? Laufen womöglich Support-Verträge aus?)
- ☐ Eingespielte Abläufe: Nach Kenntnis der Verfügbarkeit eines wichtigen Sicherheitspatches finden unverzüglich die weiteren Schritte statt (insb. die zeitnahe Einspielung des Updates)

>> Weitere Informationen:

cert-bund.de (CERT Bund)

cwe.mitre.org/cwss/cwss_v1.0.1.html (CWSS)

nvd.nist.gov/vuln-metrics/cvss (CVSS)

www.cvedetails.com (CVE Details)

4 Betriebssysteme (Clients)

Betriebssysteme auf den Arbeitsplätzen sind aufgrund ihres täglichen Einsatzes aktuell zu halten. Werden veraltete, nicht mehr vom Hersteller unterstützte Versionen eingesetzt, besteht die Gefahr zahlreicher nicht zu schließender Sicherheitslücken.

- ☐ Ausschließlicher Einsatz von Desktop-Betriebssystemen, für die der Hersteller/Maintainer beim Bekanntwerden von Schwachstellen Sicherheitsupdates zur Verfügung stellt
- ☐ Automatische Updates der Desktop-Betriebssysteme (direkt vom Hersteller oder durch zentrale Verteilung)
- ☐ Für Microsoft Windows werden die gängigen Funktionen verwendet (Windows Update, Gruppenrichtlinien, WSUS)
- ☐ Bei größerer Anzahl von Clients wird geprüft, ob ein weiteres Software-Tool zum Patchen hilfreich sein kann (unterstützende Software)
- ☐ Vor der Patch-Installation: Auswirkungen des Patches in Testumgebung prüfen, bevor Roll-Out auf alle Clients stattfindet (Funktioniert die Patch-Installation?)
- ☐ Den Ausroll-Prozess des Patches bei Bedarf in mehreren Stufen in Betracht ziehen und Bildung von Client-Gruppen, um mögliche Fehler durch den Patch in der ersten Gruppe frühzeitig zu erkennen
- ☐ Nach der Patch-Installation: Test der Auswirkungen auf die Produktivumgebung (Laufen die Clients wie gewünscht? Funktionieren alle Anwendungen noch?)

5 Software (Arbeitsplätze)

Schwachstellen in Browsern oder anderen häufig genutzten Programmen aus dem Betriebsalltag gehören zu den Haupteinfallstoren bei Cyberattacken. Die regelmäßige Pflege des täglichen Werkzeugs an einem Bildschirmarbeitsplatz der Mitarbeiter gehört deshalb zu den Kernaufgaben der IT-Abteilung.

- ☐ Geregelter Prozess für Updates, auch von Basiskomponenten wie z. B. Java, PDF-Reader, ZIP-Programm
- ☐ Verzicht auf den Einsatz unsicherer Produkte wie z. B. Flash

- ☐ Auto-Update-Funktionen für nicht-kritische Anwendungen werden genutzt, wenn die damit verbundenen Risiken als tolerabel eingestuft werden können
- ☐ Geregelter Prozess für Updates der Browser besteht (Empfehlung: Automatisch, sofern möglich)
- ☐ Browsererweiterungen werden beim Patchen nicht vergessen (Add-Ons, Plugins, Themes, Toolbars etc.)
- ☐ Office-Anwendungen bleiben sicher konfiguriert und aktuell (insbesondere Vorsicht bei Makros und nachladenden Inhalten)

>> Weitere Informationen:

www.allianz-fuer-cybersicherheit.de/ACS/DE/Angebote/... (Allianz für Cybersicherheit)

6 Webauftritt (Homepage)

Viele Cyberattacken sind gerade dann erfolgreich, wenn Websites stiefmütterlich gepflegt und nach der Ersteinrichtung keine weiteren Sicherheitsupdates eingespielt werden. Die zwangsläufig öffentliche Erreichbarkeit der Website bedeutet ein hohes Maß an Verantwortung hinsichtlich eines sicheren Betriebs.

- ☐ Insbesondere Content Management Systeme (CMS) und Shop-Systeme sind auf dem neuesten Security Patch Level zu halten; aufgrund der weiten Verbreitung sind diese ein beliebtes Angriffsziel (z. B. WordPress, Joomla, Magento)
- ☐ Für Datenbanken werden zusätzliche Sicherheitsmaßnahmen getroffen (bspw. weiterer Zugangsschutz: IP-Adressraum definieren, Mehr-Faktor-Authentifizierung für Admins, Firewall konfigurieren)
- ☐ Eingebundene Plugins bleiben ebenso im Blickfeld (z. B. können WordPress-Plugins zum Einfallstor werden)
- ☐ Themes von CMS und Shop-Baukästen sind bei Bedarf zu aktualisieren
- ☐ Drittinhalte (Skripte etc.) dürfen nicht vergessen werden, da dadurch unbemerkt Schadcode ausgeliefert werden kann
- ☐ Schwachstellen-Scanner können genutzt werden, um mögliche eigene Verwundbarkeiten von außen selbst zu erkennen

>> Weitere Informationen:

owasp.org/www-community/Vulnerability_Scanning_Tools (OWASP)

7 Server

Alle an das Internet angebundenen Systeme sind grundsätzlich im Fokus von Cyberattacken. Auch Server, deren Aufgabe nicht die Zurverfügungstellung von Webdiensten darstellt, sind vor unbefugten Zugriffen zu schützen.

- ☐ Die Serverlandschaft wird hinsichtlich Patch-Level und Schwachstellen regelmäßig geprüft (z. B. mittels Schwachstellen-Scanner)
- ☐ Installation der Server-Updates auf Test-Servern; insbesondere bei kritischen Servern eigene Testumgebung
- ☐ Geregelter Prozess zum zeitnahen Einspielen von Sicherheitsupdates der Server besteht (meist ohnehin elementares Betriebssystem-Feature)
- ☐ Kontrolle durch die Administratoren, ob auf den Servern befindliche Applikationen noch funktionsfähig sind (laufendes Monitoring)
- ☐ Es wird geprüft, ob Patch Management Tools angeboten werden und helfen können, gezielt Security Patches auf Servern automatisiert nach Freigabe zu installieren
- ☐ Für Microsoft Windows wird der Dienst Microsoft Windows Server Update Services (WSUS) genutzt
- ☐ Ungesicherte Systeme (mit klaffender Lücke und nicht verfügbarem Patch) werden als Notfallmaßnahme anderweitig abgesichert (z. B. Web Application Firewall, Virtual Patching)

8 Sicherheitskomponenten

Ein geregeltes Patch Management sorgt dafür, dass Programme aktuell bleiben. Für den ausreichenden Schutz vor Schadcode dagegen sorgen Sicherheitskomponenten wie Viren-Scanner und Firewalls. Folglich ist es wichtig, auch diese stets aktuell zu halten.

- ☐ Übersicht wird vorgehalten, welche Security Komponenten eingesetzt werden
- ☐ Es ist definiert, wie Virenscanner aktuelle Virendefinitionen erhalten (z. B. tägliche automatische Aktualisierung der Signaturen)
- ☐ Automatische Benachrichtigungen an die IT-Administration bei Verdacht auf unbefugte Verarbeitungen und zentrale Erfassung von Alarmmeldungen
- ☐ Einsatz von Endpoint Protection auf Arbeitsplatzrechnern bei Bedarf berücksichtigen
- ☐ Klare Anweisungen an Beschäftigte zum Umgang mit Alarmmeldungen

9 Mobilgeräte

Nicht nur durch Außendiensttätigkeiten, wie z. B. den Vertrieb, sondern auch aufgrund einer gesteigerten Nachfrage an Homeoffice-Möglichkeiten für Mitarbeiter ist das Patchen bei mobilen Endgeräten wichtiger denn je.

- ☐ Mobile Device Management ist etabliert (Übersicht, welches Gerät in welcher Version im Einsatz ist)
- ☐ Gewährleistung einer regelmäßigen Anbindung mobiler Endgeräte an die Verteilung von Patches
- ☐ Information der Mitarbeiter zum sicheren Umgang mit mobilen Endgeräten (insbesondere Smartphones und Notebooks)
- ☐ Klare Regelungen zum Umgang mit privaten Geräten (keine Einbindung unsicherer Privatgeräte ins Unternehmensnetz)

>> Weitere Informationen:

www.lda.bayern.de/de/checklisten.html (BayLDA)

Aktuelle Version zum Download:

www.lda.bayern.de/checkliste_patch_mgmt

Herausgeber und Kontakt:

Bayerisches Landesamt für Datenschutzaufsicht
(BayLDA) | Promenade 18 | 91522 Ansbach
www.lda.bayern.de | Tel.: 0981 180093-100
poststelle@lda.bayern.de