1. Hintergrund

Ein „Patch“ stellt aus Endanwendersicht grundsätzlich eine Korrektur einer bereits ausgelieferten Software / von Daten dar. Die Korrektur kann dazu dienen, Sicherheitslücken zu schließen, Fehler zu beheben oder bislang nicht vorhandene Funktionen zu ergänzen.

Im SAP-Kontext werden den Kunden seitens des Herstellers regelmäßig unterschiedliche „Patches“ zur Verfügung gestellt.[1] Zwecks Gewährleistung des unternehmensseitig festgelegten Sicherheitsniveaus und zur Sicherstellung der Datenkonsistenz und der Programmlogik sind in der Regel vor dem „Einspielen“ von Patches eine Reihe von Vorüberlegungen zu treffen. Diese Überlegung gehen von reinen Kosten-Nutzen-Betrachtungen bzw. Kosten-Sicherheit-Abwägungen über zeitliche Planungen („Testaufwand“) bis hin zu generellen Fragestellungen, wie z.B. mit einer bestimmten „Art“ von Patch wie umzugehen ist (s.a. unter Definitionen „SAP-Patch“).

Nicht zuletzt vor dem Hintergrund eines funktionsfähigen SAP-IKS[2] sollte grundsätzlich für jedes SAP-System[3] ein angemessener und funktionierender Patch-Management-Prozess – einschließlich der Bewertung von potentiellen Risiken - eingerichtet sein.

Werden beispielsweise wesentliche sicherheitsrelevante Patches von dem Datenbank-Hersteller nicht installiert, besteht das Risiko, dass Angreifer bekannte Sicherheitsschwachstellen ausnutzen könnten.

Zusammenfassend ist eine Reihe von konzeptionellen Vorüberlegungen für die Umsetzung eines angemessenen und funktionierenden Patch-Managements erforderlich. Mit der vorgelagerten Beschreibung des gewünschten Soll-Zustandes in einem Konzept sind in der Regel auch eine Verbesserung des übergeordneten Patch-Management-Prozesses zur Beschaffung der Patches, zur Durchführung von angemessenen Tests sowie der nachfolgenden Installation der Patches (z.B. Updates oder Sicherheitshinweise) verbunden.

2. Geltungsbereich (Rev.)

Die im Zusammenhang mit dem SAP-Patch-Management-Konzept nachfolgend dargestellten SAP-Soll-Vorgaben sind grundsätzlich für alle Prüfungen des SAP- Patch-Managements in der Diehl-Gruppe – ergänzend zu den bereits vorhandenen Vorgaben - heranzuziehen.

3. Definitionen

Patch	Korrektur einer bereits ausgelieferten Software / von Daten dar.
OSS-Hinweis	Online SAP Support Hinweise. Das OSS ist eine Fehlerdatenbank von SAP, sowie eine Sammlung von Updates und Patches. im OSS sind Millionen Fehler von SAP erfasst, beschrieben und deren Lösung erklärt. Die meisten Fehler werden durch Supportpackages oder Updates bereits im Kundensystem korrigiert sein. Bei jedem OSS-Hinweis ist das betreffende SAP-System aufgeführt und in welchem Release- / Support-Package-Stand der Fehler behoben ist.

[1] S.a. „SAP-Patch-Day-Schedule“ unter https://launchpad.support.sap.com/#/securitynotes (aufgerufen am 9. Mrz. 2018).

[2] Übergeordnetes Risiko: wesentliche sicherheitsrelevante Patches von SAP, Betriebs- und Datenbank-Hersteller sind nicht installiert.

[3] Ein SAP-System besteht grundsätzlich aus drei „Schichten“: Datenbank, Applikation und Präsentation (Schnittstelle zum Benutzer). Weitere Informationen s.a. Unterlage „SAP-Protokollierungs- u. Kontrollkonzept - Soll-Vorgaben“, 3. Definitionen).

Formen von SAP-Patches

Es wird zwischen folgenden **Formen** von Patches unterschieden:

- Security-Patch
- Support-Package
- SAP-Enhancement-Package

Security-Patch

SAP arbeitet im Rahmen eines sog. Security-Response-Prozesses kontinuierlich an der Schließung von Sicherheitslücken oder Schwachstellen, die nach Auslieferung durch eigene oder fremde Tests aufgedeckt werden.

Zur Behebung der aufgedeckten Fehler bzw. zur Schließung der Sicherheitslücken stellt SAP hierzu regelmäßig **Softwarereparaturmaßnahmen** zur Verfügung, die als Patches oder auch Security Patches bezeichnet werden.

Support-Package

Von SAP ausgelieferte Sammlung von Korrekturen zu einem definierten Release-Stand einer SAP-Komponente.

Ein Support-Package enthält in erster Linie

- Software-Korrekturen,
- Rechtliche Änderungen,
- Performanceverbesserungen.

SAP-Enhancement-Package

Ein SAP-Enhancement-Package umfasst typischerweise folgende Inhalte:

- funktionale Erweiterungen
- Branchenspezifische Erweiterungen
- vereinfachte bzw. verbesserte Benutzeroberflächen Enterprise Services

4. Zielsetzung

Mit dem Erstellen eines Patch-Management-Konzepts sind grundsätzlich folgende Zielsetzungen verbunden:

- Sicherstellung der Integrität,
- Sicherstellung der Vertraulichkeit von Daten,
- Sicherstellung der Verfügbarkeit von Daten,
- Verbesserung des übergeordneten Patch-Management-Prozesses.

5. Normative Anforderungsgrundlagen

1. GoBS, GDPdU (bis 2014),
2. GoBD (ab 2014),
3. HGB, KonTraG,
4. Prüfungsstandard des Instituts der Wirtschaftsprüfer in Deutschland e. V. (IDW, PS 330),
5. BDSG a.F. (insbesondere § 31 und Anlage zu § 9 BDSG[4]),
6. Art. 5 Abs. 1f) DSGVO,

[4] Technisch organisatorische Maßnahmen, kurz: TOM‘s

Hier: insbesondere **Art. 5 Abs. 1 Buchstabe f BDSG n.F**., „Integrität und Vertraulichkeit".

7. Datenschutzleitfaden der Deutschsprachige SAP® Anwender-gruppe (DSAG) e. V.

6. Verantwortlichkeiten

Die Verantwortung für die Initiierung, Erstellung und konkrete Ausprägung eines SAP- Patch-Management-Konzepts obliegt regelmäßig dem **IT-Sicherheitsbeauftragten**, der und dem **IT-Leiter.**

Die Verantwortung für die Umsetzung des Konzeptes liegt regelmäßig bei dem zuständigen (System-) **Administrator**.

Die konkreten Verantwortlichkeiten sind mit den eineindeutigen Funktionsnamen im Konzept aufzuführen.

7. Mindestanforderungen

7.1. Vorgabe ist vorhanden

Ein aktuelles, schriftliches und entsprechend freigegebenes, datenschutzkonformes Patch-Management-Konzept liegt für alle SAP-Systeme und alle darin enthaltenen Mandanten vor.

7.2. Formale Kriterien werden erfüllt

Das Berechtigungskonzept erfüllt folgende **formalen Anforderungen** bzw. **Dokumentationsstandards**:

- **Geltungsbereich:** Der **Geltungsbereich** des Patch-Management-Konzeptes muss definiert sein.
- **Review:** Festlegung eines Turnus und der **Verantwortlichkeit** für die regelmäßige Überprüfung des Patch-Management-Konzeptes auf Aktualität und Richtigkeit.
- **Schriftform**: Das Patch-Management-Konzept liegt in **Schriftform** vor.
- **Freigabe**: Das Patch-Management-Konzept ist vom **Dateneigentümer** freigegeben.
- **Aktualität**: Das Patch-Management-Konzept ist **aktuell**.
- **Kommunikation**: Das Patch-Management-Konzept wird an die relevanten Stellen kommuniziert.

Das schriftliche Patch-Management-Konzept muss derart verfasst sein, dass es

- verständlich, zuverlässig bzw. verlässlich und richtig sowie überprüfbar und
- „ordnungsgemäß" gemäß den zugrundeliegenden rechtlichen Normen ist. Die Ordnungsmäßigkeit ist gegeben, wenn die
  - Einhaltung gesetzlicher Anforderungen,
  - Gewährleistung der – teilweise gesetzlich geforderten – Nachvollziehbarkeit,
  - Gewährleistung der Datenintegrität,
  - Gewährleistung der Überprüfbarkeit der Wirksamkeit von Datenschutzkontrollmaßnahmen, frühzeitige Erkennung und Beseitigung von potenziellen Schwachstellen, sowie das
  - Erkennen von Verstößen gegen Sicherheitsvorgaben gegeben ist.

7.3. Inhaltliche Mindestvorgaben

1. **Übersicht SAP-Systemlandschaft**, d.h. Übersicht aller eingesetzten SAP-Komponenten
   - Implementierte SAP-Systeme, SAP-Mandanten, SAP-Module,
   - Zugehörige Versionsstände.

2. **Gewichtung** der Komponenten **nach Gefährdungspotential** in Abhängigkeit von der
   - Klassifizierung der Daten (insbesondere Identifizierung von besonders schützenswerten Daten),
   - Bedeutung der Verfügbarkeit einer Anwendung für die Unternehmenseinheit.

3. Definition und **Beschreibung** des **Patch-Management-Prozesses**
   - Festlegung des **Prüfungs-Turnus**
     D.h. Definition des Rhythmus, in dem für die eingesetzten SAP-Softwarekomponenten eine Überprüfung auf neue Schwachstellen erfolgen soll.
     Hinweis: Security Patch-Day jeden 2. Dienstag im Monat.
   - Definition der „**Informationsquellen**“
     Best Practice: Verwendung des SAP Solution Managers beim „System Recommendation“ Prozess
     - Auflistung der Quellen, die für die Überprüfung auf das Vorliegen neuer Schwachstellen heranzuziehen sind (z.B. SAP Marketplace).
     - **Definition** der **„vertrauenswürdigen“ Bezugsquellen** für Software-Updates bzw. Patches D.h. für jede eingesetzte SAP-Komponente muss bekannt sein, wo die Updates bzw. Patches zu beziehen sind.
   - Vorgaben für **Bewertung** neuer **Schwachstellen nach** hiervon ausgehender **Gefährdungslage** („Kritikalität“[5]).
   - **Beschreibung** möglicher **Gegenmaßnahmen** in Abhängigkeit der festgestellten Gefährdungslage und der verfügbaren Möglichkeiten (z.B. Sicherheitsupdate bereits verfügbar?)
   - **Vorgaben** für das **Testen** der Updates bzw. Patches
   - **Vorgaben** für das **Wiederherstellen des ursprünglichen Systemzustandes**

4. **Vorgaben** für die (inhaltliche) **Dokumentation von Änderungen**:

   Hinweis:

   Änderungen sind mindestens mit folgenden Inhalten zu dokumentieren:
   - Änderungsanforderer,
   - betroffenes **SAP-System**
   - betroffener **Mandant**
   - Grund für Änderungsanforderung sowie Ziel, das mit der Änderung verfolgt wird
   - Beurteilung Gefährdungspotential und Priorität
   - Freigabe der Änderungsanforderung
   - Grund bei Ablehnung der Freigabe und Beschreibung der alternativen Gegenmaßnahmen, die zur Beseitigung der Sicherheitslücke stattdessen vorgenommen werden

[5] Eine mögliche Methode zur Bewertung und Klassifizierung von Schwachstellen ist beispielsweise das „Common Vulnerability Scoring System“ (kurz: CVSS, s.a. http:// www.first.org/cvss, aufgerufen am 8. Mrz. 2018).

4. Vorgaben für die (inhaltliche) **Dokumentation von Änderungen** (Forts.)

- **Datum** und **Uhrzeit** der Einspielung des Updates bzw. Patches
- **Person**, die das Update bzw. Patch eingespielt hat
- **Evaluation**:
  - Datum der Durchführung
  - Person, die die Evaluation durchgeführt hat
  - Ergebnis der Evaluation

5. Definition von **Verantwortlichkeiten** für die

- Überprüfung auf Vorliegen neuer Schwachstellen
- Bewertung der Gefährdungslage
- Freigabe der Einspielung bzw. NICHT-Einspielung von Patches
  D.h. Definition, wer berechtigt ist, zu entscheiden, ob ein Patch eingespielt wird oder nicht.
- Umsetzung der freigegebenen Änderungen
- Durchführung der Evaluation

6. Vorgehensweise beim **Einspielen** der **Enhancement Packages**

Erstellen einer konzeptionellen Vorgehensweise im Umgang mit Enhancement Packages und der Aktivierung von Business Functions,

- Klare und dokumentierte Vorgehensweise und Verantwortung für Betreiber und Anwender,
- Sachgemäße Einführung und Produktivsetzung,
- Nachweisbare Entscheidungsfindung beim Änderungsmanagement und eine ordnungsmäßige Freigabe zur Aktivierung von Business Functions,
- Differenzierte Beurteilung bei mehreren Kunden auf einem Mandanten
- Definition von Verantwortlichkeiten für den Support nach der Aktivierung
- Überprüfen ob eine Abhängigkeit zu SAP-Add-On eines fremden Anbieters besteht
- Es gibt ein Sandboxsystem für das Testen und Auswirkungsanalyse
- Restriktive Vergabe der Berechtigungen für das Switch Framework

Die Verantwortlichen sollten die grundsätzliche **Vorgehensstrategie** festgelegt haben, wie Enhancement Packages bzw. Business Functions installiert und aktiviert werden.

Dabei ist **sicherzustellen,** dass

- alle verfügbaren Business Functions nach Bedarf installiert werden,
- ein separates Testsystem besteht, das als Sandbox-System wieder „plattgemacht“ werden kann,
- ein Änderungsmanagement für neue Business Functions geregelt ist,
- Zuständigkeiten und Verantwortliche für jeweiligen Aufgaben definieren.

6. Vorgehensweise beim **Einspielen** der **Enhancement Packages** (Forts.)

Darüber hinaus sollten **Dokumentationsregelungen** für folgende Gruppierungen bestehen:

- Projekte – Mitlaufende Prüfung von EHP-Projekten
- Betreiber – Strategie, Konzept, Vorgehensweise, Change-Management, Support
- Anwender – Testqualität, Einführungsvorgehen, Betriebsdokumentation

7. Weitere Überlegungen

Einsatz von zentralisierten Lösungen zur gezielten und mehrstufigen Ausrollung von Updates oder manuelle Pflege der eigenen IT-Systeme.

7. Reports, Transaktionen und Tabellen

Bei den nachfolgend nicht abschließend aufgeführten (SAP-) Reports, Transaktionen und Tabellen ist zwischen folgenden inhaltlichen Zielstellungen zu unterscheiden:

- Vornehmen von Einstellungen bzw. Aktivitäten im Zusammenhang mit der Durchführung des Patch-Management-Prozesses,
- Kontrolle bzw. Überwachung und Auswertung von Informationen zum Patch-Management-Prozess.

Report, Transaktion, Tabelle	Beschreibung
SPAM	Aufruf des Support-Package-Managers
SNOTE	Einspielen / Anzeige von OSS-Hinweisen (OSS-Notes) verwendet werden.
SFW5	Switch Framework; zentrale Schaltstelle für Business Functions um sich Beschreibungen, Release Informationen und Testkataloge anzeigen zu lassne.
CVERS	Enthält Release-Stände der im System vorhandenen Softwarekomponenten

♦ ♦ ♦