

---

# SAP Security Patch Policy



---

## Inhaltsverzeichnis

---

Inhaltsverzeichnis .....	1
Geltungsbereich.....	1
SAP Security Patch Policy - Überblick .....	1
SAP Security Patch Policy - Regeln.....	3

---

## Geltungsbereich

---

Diese SAP Security Patch Policy gilt ab Inkrafttreten für alle SAP Systeme exklusive den SAP Systemen des CCHH (wie z.B. RD2 und QD2) die durch die TU-Darmstadt verantwortet werden. Dies beinhaltet jegliche Softwarekomponenten die über das SAP Support Portal heruntergeladen werden und innerhalb der TU-Darmstadt genutzt werden. Darunter fallen unter anderem folgende Softwarekomponenten:

- SAP ERP
- SAP NetWeaver Application Server ABAP und JAVA
- SAP Solution Manager
- SAP S/4HANA
- SAP HANA
- SAP Router

Anmerkung: Betriebssystem Patches werden separat betrachtet. Hierzu gibt es ein SLA mit dem HRZ. Die Verantwortung für die Betriebssystem Patches liegt beim HRZ.

---

## SAP Security Patch Policy - Überblick

---

Für die SAP-Systeme der TU Darmstadt gilt entsprechend BSI die „[Standard-Absicherung](#)“. Sofern nicht anders angegeben gilt für die SAP-Systeme die Schutzbedarfskategorie NORMAL.

In Bezug auf die Gefährdungslagen aus [[BSI APP.4.2](#) Seite 2] sind G.2.1 und G.2.2 relevant, diese sind:

- „2.1 Fehlende Berücksichtigung der Sicherheitsempfehlungen von SAP“ im Kontext von Patches und SAP-Sicherheitshinweisen
- „2.2 Fehlendes oder nicht zeitnahes Einspielen von Patches und SAP-Sicherheitshinweisen“  
Insbesondere: „Wenn neue Patches oder SAP-Sicherheitshinweise nicht zeitnah oder gar nicht eingespielt werden, könnten offene Sicherheitslücken von Angreifern ausgenutzt werden. Dadurch

---

könnten Angreifer SAP-ERP Systeme manipulieren. Dann könnten vertrauliche Daten abfließen, Dienste ausfallen oder ganze Geschäftsprozesse stillstehen.“

Um Patches zeitnah innerhalb der SAP Landschaft einspielen zu können müssen Ressourcen und Prozesse durch die beteiligten Einheiten bereitgestellt werden, siehe [[OPS.1.1.3: Patch- und Änderungsmanagement](#)].

In Bezug „APP.4.2.OPS.1.1.3.M15 Regelmäßige Aktualisierung von IT-Systemen und Software (B)“ auf S. 51 wird in den [[Umsetzungshinweisen zu APP4.2](#)] gefordert und empfohlen:

*Grundsätzlich gilt, dass die SAP-Sicherheitshinweise der Priorität 1 (HotNews) und 2 (High) teilweise schwerwiegende Fehler in der Programmierung der SAP-Standardsoftware beheben und deswegen zeitnah bewertet und angewendet werden müssen. Hinweise mit geringerer Priorität können auch über Support-Packages implementiert werden. Da die ausgelieferten Korrekturen oft Abhängigkeiten zum Softwarestand haben und deswegen eine verspätete Umsetzung komplexer wird, sollte mindestens einmal im Jahr ein Support-Package eingespielt werden.*

Das Einspielen der zugehörigen Patches erfordert eine Bewertung, Testaufwände und ggf. eine Downtime der betroffenen SAP-Systeme. Für das Einspielen der jährlichen Support-Package Upgrades sind zusätzliche Testaufwände für die Fachdezernate notwendig und einzuplanen.

Zusätzlich SOLLTEN die Vorgaben und Maßnahmen aus dem SAP Security Baseline Template entsprechend den [[BSI Modul APP.4.2](#)] umgesetzt werden. Der Hersteller SAP hat Anforderungen an seine Kunden in Bezug auf SAP Security Patches in einer FAQ definiert, siehe <https://support.sap.com/en/my-support/knowledge-base/security-notes-news/security-notes-faqs.html>.

Zusammenfassend gilt:

- SAP Security Patches werden nach Priorität / Risiko seitens SAP definiert die sich vom CVSS v3 Base Score ableiten. Die SAP-Einstufungen sind:
  - HotNews (1)
  - Korrekturen mit einer hohen Priorität (2)
  - Korrekturen mit einer mittleren Priorität (3)
  - Korrekturen mit einer niedrigen Priorität (4)
  - Empfehlungen / zusätzliche Informationen (5)
- Patches werden in der Regel am zweiten Dienstag im Monat veröffentlicht (sog. SAP Security Patch Day), Ausnahmen kann es für kritische Security Patches geben
- SAP unterscheidet zwischen „Patch Day Security Notes“ (alle Risiken) und „Support Package Security Notes“ (Risiken: High, Medium, und Low)
- Je nach SAP-Anwendung gibt es unterschiedliche „Maintenance Strategies“ seitens SAP. Diese beschreiben unter anderem, für welche Release-Level Patches bereitgestellt werden. Allgemein gilt die [[24 Monats-Regel](#)]:

„Starting June 11, 2019, for all new SAP Security Notes with high or very high severity we deliver fix for Support Packages shipped within the last 24 months<sup>1</sup> for the versions under Mainstream Maintenance and Extended Maintenance.“ Es gelten die folgenden Abweichungen:

- Maintenance Strategy for SAP BW/4 HANA: see [SAP Note 2347382](#)
- Maintenance Strategy for SAP Analytics BI Suite: see [SAP Note 2771848](#)

- 
- *Maintenance Strategy for SAP BW/4 HANA: see [SAP Note 2347382](#)*
  - *Maintenance Strategy for SAP Analytics BI Suite: see [SAP Note 2771848](#)*
  - *Maintenance Strategy for SAP GUI for Windows and SAP GUI for Java: see [SAP Note 147519](#)*
  - *Maintenance Strategy for SAP Kernel: see [SAP Note 787302](#)*
  - *Maintenance Strategy for SAP HANA: see documents for [HANA1](#) and [HANA2](#) or [SAP Notes 2021789](#) and [2378962](#)*
  - *Maintenance Strategy for SAP Business Client for Desktop: see [SAP Note 2302074](#)*
  - *Maintenance Strategy for SAP Business One and SAP Business One, version for SAP HANA®: see [SAP Note 3209797](#)*

Demzufolge müssen z.B. ABAP-Systeme auf einem Support Package Release Stand sein, der nicht älter als 24 Monate ist, um zu garantieren, dass Security Patches mit hohem oder sehr hohem Risiko ohne ein SP-Upgrade eingespielt werden können. Für ein SP-Upgrade sind üblicherweise erhebliche Testaufwände notwendig, die die Fachdezernate mit involvieren.

Zusätzlich hat die SAP mit dem SAP Security Baseline Template eine Herstellervorgabe ähnlich den BSI-Anforderungen zum SAP Security Patch Prozess beim Kunden empfohlen. Dort heißt es:

- „2.2.2.1.1 b) SAP Security Notes must be reviewed timely and implemented timely – if not decided and documented otherwise in the review.“

---

## **SAP Security Patch Policy - Regeln**

---

Die folgenden Regeln gelten für das Einspielen von SAP Sicherheitshinweisen die von SAP im Support Portal veröffentlicht werden:

- [SAPSECPOL-1] Um Security Notes zeitnah einspielen zu können MÜSSEN diese monatlich bewertet werden. Es gibt weder in den BSI APP 4.2 / OPS.1.1.5 Vorgaben, noch bei SAP eine Definition von „zeitnah“. Für die TU-Darmstadt gilt, dass die Erstbewertung durch das Team der SAP Basis/SAP Anwendungen innerhalb von 2 Wochen nach Veröffentlichung erfolgen SOLL.
- [SAPSECPOL-2] Security Notes vom Typ „Hot News“ und „Hoher“ Priorität SOLLTEN innerhalb von 4 Wochen in Produktion installiert sein.
- [SAPSECPOL-3] Hinweise mit geringerer Priorität können auch über Support-Packages implementiert werden. Dies impliziert eine Risikoakzeptanz für die Hinweise die bei der Bewertung entsprechend klassifiziert wurden.
- [SAPSECPOL-4] Support Packages SOLLTEN mindestens einmal jährlich entsprechend der SAP Maintenance Strategy aktualisiert werden.
- [SAPSECPOL-5] Für das Einspielen von Sicherheitshinweisen die als kritisch für die TU Darmstadt bewertet wurden können kurzfristig Downtimes und Wartungsfenster durch die Gruppe SAP-Anwendungen festgelegt werden (Notfall-Patch-Prozess).
- [SAPSECPOL-6] SAP-Datenbanken die auf SAP HANA basieren unterliegen den gleichen oben genannten Zeitlichen- und Prozess-Vorgaben. Für MSSQL sind die Herstellervorgaben und ggf. zusätzliche Hinweise von SAP zu beachten.

Die Prozessdokumentation befindet sich im [TU Signavio Process Collaboration Hub](#).

---

Entsprechend der SAP-Empfehlung (12-Monats-Regel), erfolgt ein Software-Update der gesamten SAP-Systemlandschaft, wie z.B. SP-Stacks, Kernel, Datenbank mindestens einmal im Jahr. Für das SAP ERP System erfolgt dies in Abstimmung mit dem CCHH-Hochschulverbund.

Die SAP-Sicherheitshinweise werden automatisiert über die [Onapsis Plattform](#) detektiert. Die Hinweise werden innerhalb von 2 Wochen durch die Gruppe SAP Anwendungen bewertet. SAP-Sicherheitshinweise mit der Prio „sehr hoch und hoch“ (CVSS v3 7-10) sollen innerhalb von 4 Wochen eingespielt werden.

Entsprechend den Best Practices der SAP-Community, werden die SAP-Sicherheitshinweise ohne oder nur mit reduzierten Tests in die Landschaften in 2 Phasen eingespielt: als erstes in die DEV/QAS Systeme und zeitlich versetzt in die PROD-Systeme. Für die DEV/QAS-Systeme werden diese an jedem dritten Freitag im Monat und für die PROD-Systeme an jedem ersten Freitag des Monats im Rahmen der Systemwartung eingespielt.

Das Einspielen der Security Patches erfordert ggf. Testaufwände und nutzt die bestehenden Changemanagement Prozesse (Entwicklung, QA, dann Produktion). Diese Vorgabe impliziert eine Risikoakzeptanz für die potentielle Verwundbarkeit durch den fehlenden Security Patch bis zur Installation des zugehörigen Patches entsprechend der zu vor genannten Prioritäten.

Die Server Betriebssystem Patches werden vom HRZ (Systembetrieb) entsprechend dem [Operation Level Agreement \(OLA\)](#) verantwortet.