Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.1.3 Patch- und Änderungsmanagement

1. Beschreibung

1.1. Einleitung

Es ist eine große Herausforderung, die in einer Institution eingesetzten Komponenten der Informationstechnik korrekt und zeitnah zu aktualisieren. So zeigt sich in der Praxis, dass vorhandene Sicherheitslücken oder Betriebsstörungen häufig auf mangelhafte oder fehlende Patches und Änderungen zurückzuführen sind. Ein fehlendes oder vernachlässigtes Patch- und Änderungsmanagement führt daher schnell zu möglichen Angriffspunkten.

Aufgabe des Patch- und Änderungsmanagements ist es allgemein, verändernde Eingriffe in Anwendungen, Infrastruktur, Dokumentationen, Prozesse und Verfahren steuer- und kontrollierbar zu gestalten.

1.2. Zielsetzung

In diesem Baustein wird aufgezeigt, wie ein funktionierendes Patchmanagement in einer Institution aufgebaut und wie der entsprechende Prozess kontrolliert und optimiert werden kann.

Über das Patchmanagement hinaus beinhaltet der Baustein jedoch auch einige Kernaspekte eines Änderungsmanagements, die für die Informationssicherheit relevant sind. Mit Änderungsmanagement wird die Aufgabe bezeichnet, Änderungen zu planen und zu steuern.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* ist für den gesamten Informationsverbund anzuwenden.

Die Beschreibungen in diesem Baustein konzentrieren sich auf den IT-Betrieb, und dort insbesondere auf das Patchmanagement, mit dem Software aktualisiert wird (z. B. durch Sicherheitskorrekturen, Service Packs und Hot Fixes). In den einzelnen Bausteinen der Schichten SYS *IT-Systeme* und APP *Anwendungen* finden sich gegebenenfalls spezifischere Anforderungen bezüglich des Patch- und Änderungsmanagements.

Dieser Baustein beinhaltet kein vollständiges Änderungsmanagement, sondern lediglich die Kernaspekte zur Informationssicherheit. In größeren Institutionen ist es sinnvoll, darüber hinaus ein

Änderungsmanagement systematisch zu strukturieren. Hierzu können Standardwerke, wie z. B. der Change-Management-Prozess der „IT Infrastructure Library“ (ITIL), herangezogen werden. Ein solches Änderungsmanagement muss nicht auf die IT beschränkt sein, sondern kann auch Geschäftsprozesse und Fachaufgaben selbst umfassen. Unter Änderung wird in diesem Baustein alles inbegriffen, was damit einhergeht, IT-Komponenten anzupassen, wie z. B. „Changes“, „Patches", „Updates“, „Upgrades“, „Einbau“, „Ausbau“, etc. Software Entwicklung hingegen wird im Baustein CON.8 *Software-Entwicklung* betrachtet.

Anforderungen zu Test und Freigabe von Patches und Software werden in diesem Baustein nicht im Detail behandelt. Sie finden sich im Baustein OPS.1.1.6 *Software-Tests und -Freigaben.*

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* von besonderer Bedeutung.

2.1. Mangelhaft festgelegte Zuständigkeiten

Durch mangelhaft festgelegte, sich überschneidende oder ungeklärte Zuständigkeiten können beispielsweise Änderungsanforderungen langsamer kategorisiert und priorisiert werden. Dadurch kann sich insgesamt die Verteilung von Patches und Änderungen verzögern. Auch wenn Patches und Änderungen vorschnell ohne Testlauf und Berücksichtigung aller (fachlichen) Aspekte freigegeben werden, kann sich das gravierend auf die Sicherheit auswirken.

Im Extremfall können mangelhaft festgelegte Zuständigkeiten die gesamte Institution komplett oder in großem Umfang beeinträchtigen. Störungen im Betrieb wirken sich negativ auf die Verfügbarkeit aus. Werden sicherheitsrelevante Patches nicht oder verspätet verteilt, können die Vertraulichkeit und Integrität gefährdet werden.

2.2. Mangelhafte Kommunikation beim Änderungsmanagement

Wenn das Patch- und Änderungsmanagement innerhalb der Institution wenig akzeptiert wird oder die beteiligten Personen mangelhaft kommunizieren, kann das dazu führen, dass Änderungsanforderungen verzögert bearbeitet werden oder über eine Änderungsanforderung falsch entschieden wird. Dadurch kann das Sicherheitsniveau insgesamt verringert und der IT-Betrieb ernsthaft gestört werden. In jedem Fall wird bei mangelhafter Kommunikation der Änderungsprozess ineffizient, da zu viel Zeit und Ressourcen investiert werden müssen. Dies wirkt sich negativ auf die Reaktionsfähigkeit der Institution aus und kann im Extremfall dazu führen, dass Sicherheitslücken entstehen oder wichtige Ziele der Institution nicht erreicht werden.

2.3. Mangelhafte Berücksichtigung von Geschäftsprozessen und Fachaufgaben

Ungeeignete Änderungen können unter anderem den reibungslosen Ablauf der Geschäftsprozesse oder Fachaufgaben beeinträchtigen oder gar dazu führen, dass die beteiligten IT-Systeme komplett ausfallen. Auch ein noch so umfangreiches Testverfahren kann nicht vollkommen ausschließen, dass sich eine Änderung im späteren Produktivbetrieb als fehlerhaft erweist.

Wird im Änderungsprozess die Auswirkung, Kategorie oder Priorität einer eingereichten Änderungsanforderung hinsichtlich der Geschäftsprozesse beziehungsweise Fachaufgaben falsch eingeschätzt, kann sich das angestrebte Sicherheitsniveau verringern. Solche Fehleinschätzungen treten überwiegend auf, wenn sich die für die IT zuständigen Personen und die zuständigen Fachabteilungen nicht ausreichend abstimmen.

2.4. Unzureichende Ressourcen beim Patch- und Änderungsmanagement

Für ein wirkungsvolles Patch- und Änderungsmanagement sind angemessene personelle, zeitliche und finanzielle Ressourcen erforderlich. Sind diese nicht vorhanden, könnten beispielsweise die notwendigen Rollen mit ungeeigneten Personen besetzt werden. Auch können so keine Schnittstellen für bestimmte Informationen geschaffen werden, beispielsweise zwischen der IT und den entsprechenden Ansprechpartnern und Ansprechpartnerinnen in den Fachbereichen. Auch die erforderlichen Kapazitäten für die Infrastruktur der Test- und Verteilungsumgebungen könnten nicht bereitgestellt werden. Können die personellen, zeitlichen und finanziellen Mängel im Regelbetrieb häufig noch ausgeglichen werden, zeigen sie sich unter hohem Zeitdruck umso deutlicher, beispielsweise wenn Notfallpatches eingespielt werden müssen.

2.5. Probleme bei der automatisierten Verteilung von Patches und Änderungen

Häufig werden Patches und Änderungen nicht manuell, sondern zentral softwareunterstützt verteilt. Wird eine solche Software benutzt, können fehlerhafte Patches und Änderungen automatisiert im gesamten Informationsverbund verteilt werden, wodurch große Sicherheitsprobleme entstehen können. Besonders gravierend ist es, wenn auf vielen IT-Systemen gleichzeitig Software installiert wird, die Sicherheitslücken enthält.

Treten nur vereinzelte Fehler auf, lassen sie sich oft per Hand beheben. Problematisch wird es aber, wenn IT-Systeme über einen längeren Zeitraum nicht erreichbar sind. Ein Beispiel sind Mitarbeitende im Außendienst, die ihre IT-Systeme nur selten und unregelmäßig an das LAN der Institution anschließen. Wenn das Werkzeug so konfiguriert wird, dass die Aktualisierungen nur innerhalb eines bestimmten Zeitraums verteilt werden, und dann nicht alle IT-Systeme erreichbar sind, können diese IT-Systeme nicht aktualisiert werden.

2.6. Mangelhafte Wiederherstellungsoptionen beim Patch- und Änderungsmanagement

Wenn Patches oder Änderungen verteilt werden, ohne dass eine Wiederherstellungsoption vorgesehen ist, oder wenn die Wiederherstellungsroutinen der eingesetzten Software nicht oder nicht angemessen wirken, kann fehlerhaft aktualisierte Software nicht zeitnah korrigiert werden. Dadurch können wichtige IT-Systeme ausfallen und hohe Folgeschäden entstehen. Neben dem Verlust der Daten sind vor allem die Verfügbarkeit und Integrität der Daten und der betroffenen IT-Systeme gefährdet.

2.7. Fehleinschätzung der Relevanz von Patches und Änderungen

Werden Änderungen falsch priorisiert, könnten beispielsweise zuerst unwichtige Patches installiert werden. Wichtige Patches hingegen werden dann zu spät installiert. Sicherheitslücken bleiben so länger bestehen. Das Patch- und Änderungsmanagement wird oft durch softwarebasierte Werkzeuge unterstützt. Auch diese Werkzeuge können Softwarefehler enthalten und dadurch unzureichende oder fehlerhafte Angaben über eine Änderung machen. Werden die Angaben, die ein solches Tool über eine Änderung macht, nicht überprüft und auf Plausibilität getestet, kann die tatsächliche von der angenommenen Umsetzung von Änderungen abweichen.

2.8. Manipulation von Daten und Werkzeugen beim Änderungsmanagement

Das Patch- und Änderungsmanagement agiert oft von zentraler Stelle aus. Aufgrund seiner exponierten Stellung ist es besonders gefährdet. Wenn es bei einem Angriff gelingen sollte, die beteiligten Server zu übernehmen, könnten über diesen zentralen Punkt manipulierte Softwareversionen gleichzeitig auf eine Vielzahl von IT-Systemen verteilt werden. Oft entstehen weitere Angriffspunkte dadurch, dass diese IT-Systeme von externen Partnerinstitutionen betrieben werden (Outsourcing). Es könnte auch Wartungszugänge geben, die ermöglichen, auf den zentralen Server zur Verteilung von Änderungen zuzugreifen. Auch diese könnten für Angriffe genutzt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.1.3 *Patch- und Änderungsmanagement* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.1.3.A1 Konzept für das Patch- und Änderungsmanagement (B) [Fachverantwortliche]

Wenn IT-Komponenten, Software oder Konfigurationsdaten geändert werden, MUSS es dafür Vorgaben geben, die auch Sicherheitsaspekte berücksichtigen. Diese MÜSSEN in einem Konzept für das Patch- und Änderungsmanagement festgehalten und befolgt werden. Alle Patches und Änderungen MÜSSEN geeignet geplant, genehmigt und dokumentiert werden. Patches und Änderungen SOLLTEN vorab geeignet getestet werden (siehe hierzu auch OPS.1.1.6 *Software-Tests und Freigaben*). Wenn Patches installiert und Änderungen durchgeführt werden, MÜSSEN Rückfall-Lösungen vorhanden sein. Bei größeren Änderungen MUSS zudem der oder die ISB beteiligt sein. Insgesamt MUSS sichergestellt werden, dass das angestrebte Sicherheitsniveau während und nach den Änderungen erhalten bleibt. Insbesondere SOLLTEN auch die gewünschten Sicherheitseinstellungen erhalten bleiben.

OPS.1.1.3.A2 Festlegung der Zuständigkeiten (B)

Für alle Organisationsbereiche MÜSSEN Zuständige für das Patch- und Änderungsmanagement festgelegt werden. Die definierten Zuständigkeiten MÜSSEN sich auch im Berechtigungskonzept widerspiegeln.

OPS.1.1.3.A3 Konfiguration von Autoupdate-Mechanismen (B)

Innerhalb der Strategie zum Patch- und Änderungsmanagement MUSS definiert werden, wie mit integrierten Update-Mechanismen (Autoupdate) der eingesetzten Software umzugehen ist. Insbesondere MUSS festgelegt werden, wie diese Mechanismen abgesichert und passend konfiguriert werden. Außerdem SOLLTEN neue Komponenten daraufhin überprüft werden, welche Update-Mechanismen sie haben.

OPS.1.1.3.A15 Regelmäßige Aktualisierung von IT-Systemen und Software (B)

IT-Systeme und Software SOLLTEN regelmäßig aktualisiert werden.

Grundsätzlich SOLLTEN Patches zeitnah nach Veröffentlichung eingespielt werden. Basierend auf dem Konzept für das Patch- und Änderungsmanagement MÜSSEN Patches zeitnah nach Veröffentlichung bewertet und entsprechend priorisiert werden. Für die Bewertung SOLLTE geprüft werden, ob es zu diesem Patch bekannte Schwachstellen gibt. Es MUSS entschieden werden, ob der Patch eingespielt werden soll. Wenn ein Patch eingespielt wird, SOLLTE kontrolliert werden, ob dieser auf allen relevanten Systemen zeitnah erfolgreich eingespielt wurde. Wenn ein Patch nicht eingespielt wird, MÜSSEN die Entscheidung und die Gründe dafür dokumentiert werden.

Falls Hardware- oder Software-Produkte eingesetzt werden sollen, die nicht mehr von den Herstellenden unterstützt werden oder für die kein Support mehr vorhanden ist, MUSS geprüft werden, ob diese dennoch sicher betrieben werden können. Ist dies nicht der Fall, DÜRFEN diese Hardware- oder Software-Produkte NICHT mehr verwendet werden.

OPS.1.1.3.A16 ENTFALLEN (B)

Diese Anforderung ist entfallen.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

OPS.1.1.3.A4 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.3.A5 Umgang mit Änderungsanforderungen (S) [Fachverantwortliche]

Alle Änderungsanforderungen (Request for Changes, RfCs) SOLLTEN erfasst und dokumentiert werden. Die Änderungsanforderungen SOLLTEN von den jeweiligen Fachverantwortlichen für das Patch- und Änderungsmanagement daraufhin kontrolliert werden, ob die Aspekte der Informationssicherheit ausreichend berücksichtigt wurden.

OPS.1.1.3.A6 Abstimmung von Änderungsanforderungen (S)

Der zu einer Änderung zugehörige Abstimmungsprozess SOLLTE alle relevanten Zielgruppen und die Auswirkungen auf die Informationssicherheit berücksichtigen. Die von der Änderung betroffenen Zielgruppen SOLLTEN sich nachweisbar dazu äußern können. Auch SOLLTE es ein festgelegtes Verfahren geben, wodurch wichtige Änderungsanforderungen beschleunigt werden können.

OPS.1.1.3.A7 Integration des Änderungsmanagements in die Geschäftsprozesse (S)

Der Änderungsmanagementprozess SOLLTE in die Geschäftsprozesse beziehungsweise Fachaufgaben integriert werden. Bei geplanten Änderungen SOLLTE die aktuelle Situation der davon betroffenen Geschäftsprozesse berücksichtigt werden. Alle relevanten Fachabteilungen SOLLTEN über anstehende Änderungen informiert werden. Auch SOLLTE es eine Eskalationsebene geben, deren Mitglieder der

Leitungsebene der Institution angehören. Die Mitglieder dieser Eskalationsebene SOLLTEN in Zweifelsfällen über Priorität und Terminplanung einer Hard- oder Software-Änderung entscheiden.

OPS.1.1.3.A8 Sicherer Einsatz von Werkzeugen für das Patch- und Änderungsmanagement (S)

Anforderungen und Rahmenbedingungen SOLLTEN definiert werden, nach denen Werkzeuge für das Patch- und Änderungsmanagement ausgewählt werden. Außerdem SOLLTE eine spezifische Sicherheitsrichtlinie für die eingesetzten Werkzeuge erstellt werden.

OPS.1.1.3.A9 Test- und Abnahmeverfahren für neue Hardware (S)

Wenn neue Hardware ausgewählt wird, SOLLTE geprüft werden, ob die eingesetzte Software und insbesondere die relevanten Betriebssysteme mit der Hardware und deren Treibersoftware kompatibel sind. Neue Hardware SOLLTE getestet werden, bevor sie eingesetzt wird. Diese SOLLTE ausschließlich in einer isolierten Umgebung getestet werden.

Für IT-Systeme SOLLTE es ein Abnahmeverfahren und eine Freigabeerklärung geben. Die Zuständigen SOLLTEN die Freigabeerklärungen an geeigneter Stelle schriftlich hinterlegen. Für den Fall, dass trotz der Abnahme- und Freigabeverfahren im laufenden Betrieb Fehler festgestellt werden, SOLLTE es ein Verfahren zur Fehlerbehebung geben.

OPS.1.1.3.A10 Sicherstellung der Integrität und Authentizität von Softwarepaketen (S)

Während des gesamten Patch- oder Änderungsprozesses SOLLTE die Authentizität und Integrität von Softwarepaketen sichergestellt werden. Dazu SOLLTE geprüft werden, ob für die eingesetzten Softwarepakete Prüfsummen oder digitale Signaturen verfügbar sind. Falls ja, SOLLTEN diese vor der Installation des Pakets überprüft werden. Ebenso SOLLTE darauf geachtet werden, dass die notwendigen Programme zur Überprüfung vorhanden sind.

Software und Updates SOLLTEN grundsätzlich nur aus vertrauenswürdigen Quellen bezogen werden.

OPS.1.1.3.A11 Kontinuierliche Dokumentation der Informationsverarbeitung (S)

Änderungen SOLLTEN in allen Phasen, allen Anwendungen und allen Systemen dokumentiert werden. Dazu SOLLTEN entsprechende Regelungen erarbeitet werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.1.3.A12 Einsatz von Werkzeugen beim Änderungsmanagement (H)

Bevor ein Werkzeug zum Änderungsmanagement benutzt wird, SOLLTE sorgfältig geprüft werden, ob damit die Änderungen angemessen im Informationsverbund verteilt werden können. Zusätzlich SOLLTEN Unterbrechungspunkte definiert werden können, an denen die Verteilung einer fehlerhaften Änderung gestoppt wird.

OPS.1.1.3.A13 Erfolgsmessung von Änderungsanforderungen (H) [Fachverantwortliche]

Um zu überprüfen, ob eine Änderung erfolgreich war, SOLLTEN die jeweiligen Fachverantwortlichen für das Patch- und Änderungsmanagement sogenannte Nachtests durchführen. Dazu SOLLTEN sie

geeignete Referenzsysteme als Qualitätssicherungssysteme auswählen. Die Ergebnisse der Nachtests SOLLTEN im Rahmen des Änderungsprozesses dokumentiert werden.

OPS.1.1.3.A14 Synchronisierung innerhalb des Änderungsmanagements (H)

Im Änderungsmanagementprozess SOLLTE durch geeignete Mechanismen sichergestellt werden, dass auch zeitweise oder längerfristig nicht erreichbare Geräte die Patches und Änderungen erhalten.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Kapitel 12.1.2 Change Management Vorgaben, die für das Patch- und Änderungsmanagement relevant sind.

Die IT Infrastructure Library (ITIL) gibt Hinweise zum Aufbau eines Change-Management-Prozesses.