OPS.1.1: Kern-IT-Betrieb / Kernaufgaben

OPS.1.1.3: Patch- und Änderungsmanagement

1 Beschreibung

1.1 Einleitung

Die immer schnellere Entwicklung in der Informationstechnik und die steigenden Anforderungen der Benutzer stellen viele Behörden und Unternehmen vor große Herausforderungen. Eine davon ist die Aufgabe, die Komponenten ihrer Informationstechnik korrekt und zeitnah zu aktualisieren. Auch 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 aber schnell zu Sicherheitslücken in den einzelnen Komponenten und damit 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 Patch- und Änderungsmanagement in einer Institution aufgebaut und wie der entsprechende Prozess kontrolliert und optimiert werden kann.

1.3 Abgrenzung und Modellierung

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

Die Beschreibungen in diesem Baustein konzentrieren sich auf den IT-Betrieb, können aber auch sinngemäß in anderen Geschäftsprozessen oder Fachaufgaben umgesetzt werden. Mit Änderungsmanagement wird die Aufgabe bezeichnet, Änderungen zu planen und zu steuern. Da dieser Prozess sehr aufwändig ist, zielen die Standard-Anforderungen des Bausteins vor allem auf größere Informationsverbünde ab. Kleinere Institutionen können die Erfüllung der Standard-Anforderungen zwar prüfen, der Aufwand sollte aber nicht über den Nutzen gestellt werden.

Das Patchmanagement stellt einen Teilbereich bzw. einen speziellen Prozess innerhalb des Änderungsmanagements dar, der auf die Aktualisierung von Software abzielt und in jedem Fall anzuwenden ist. In den einzelnen Bausteinen der Schichten SYS *IT-Systeme* und APP *Anwendungen* finden sich zusätzliche Anforderungen bezüglich des Patchmanagements, je nachdem wo dieses

erforderlich ist.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* von besonderer Bedeutung:

2.1 Mangelhaft festgelegte Verantwortlichkeiten

Durch mangelhaft festgelegte, sich überschneidende oder ungeklärte Verantwortlichkeiten 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 Verantwortlichkeiten 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 Geschäftsziele 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 IT-Verantwortlichen 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 verfügbar, 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 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 im gesamten Informationsverbund verteilt werden, wodurch große Sicherheitsprobleme entstehen können. Besonders gravierend ist es, wenn auf vielen 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 Außendienstmitarbeiter, die ihre IT-Systeme nur selten und unregelmäßig an das LAN 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 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 gefährdet.

2.7 Mangelhafte Berücksichtigung von mobilen Endgeräten

Mobile Endgeräte sind eine besondere Herausforderung für das Änderungsmanagement, da sie wegen ihrer wechselnden Einsatzorte und ihrer Anbindung an Funknetze nicht immer in die automatisierte Verteilung von Patches und Änderungen eingebunden sind. Auch sind Bandbreite und stabile Datenübertragung bei mobilen Endgeräten nicht immer gewährleistet. Werden solche Geräte im Patch- und Änderungsmanagement nicht gesondert berücksichtigt, können Patches und Änderungen möglicherweise nur unvollständig verteilt werden oder beanspruchen mehr Zeit als geplant. Sie bedeuten zudem auch immer ein Sicherheitsrisiko.

2.8 Unzureichendes Notfallvorsorgekonzept für das Patch- und Änderungsmanagement

Das Patch- und Änderungsmanagement trägt dazu bei, Informationssicherheit in einer Institution technisch umzusetzen. Die von diesem Prozess verwendeten IT-Systeme sind als kritisch für den IT-Betrieb anzusehen. Dazu gehören beispielsweise die zentralen Server, die Patches und Änderungen verteilen, die Datenbanken mit den aktuellen Konfigurationen der IT-Systeme sowie die Backupserver für die Wiederherstellungspunkte. Fällt z. B. der Server aus, der die Änderungen verteilt, können eventuell neu erscheinende kritische Updates nicht mehr zeitnah eingespielt werden. Des Weiteren können fehlende Datensicherungen der aktuellen Konfigurationen der IT-Systeme dazu führen, dass in einem Notfall nicht mehr sichergestellt ist, dass wichtige IT-Komponenten möglichst schnell wieder in den ursprünglichen Zustand versetzt werden können.

2.9 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.

2.10 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 Angreifern gelingen sollte, die beteiligten Server zu übernehmen, könnten sie über diesen zentralen Punkt manipulierte Softwareversionen gleichzeitig auf eine Vielzahl von IT-Systemen verteilen. Oft entstehen weitere Angriffspunkte dadurch, dass diese Systeme von externen Partnern betrieben werden (Outsourcing). Es könnte auch Wartungszugänge geben, die es Angreifern ermöglichen, auf den zentralen Server zur Verteilung von Änderungen zuzugreifen.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen für den Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* aufgeführt. Grundsätzlich ist der *IT-Betrieb* für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche, Änderungsmanager, Leiter IT

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* vorrangig umgesetzt werden:

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

Wenn IT-Komponenten, Software oder Konfigurationsdaten geändert werden sollen, MUSS es dafür Vorgaben geben, die auch Sicherheitsaspekte berücksichtigen. Alle Patches und Änderungen MÜSSEN geeignet geplant, genehmigt und dokumentiert werden. Patches und Änderungen SOLLTEN vorab geeignet getestet werden. Patches und Änderungen SOLLTEN nach Wichtigkeit und Dringlichkeit klassifiziert und entsprechend umgesetzt werden. Wenn Patches installiert und Änderungen durchgeführt werden, MÜSSEN Rückfall-Lösungen vorhanden sein. An größeren Änderungen MUSS zudem der Informationssicherheitsbeauftragte beteiligt sein. Insgesamt MUSS sichergestellt werden, dass das angestrebte Sicherheitsniveau während und nach den Änderungen erhalten bleibt.

OPS.1.1.3.A2 Festlegung der Verantwortlichkeiten [Leiter IT] (B)

Für alle Organisationsbereiche MÜSSEN Verantwortliche für das Patch- und Änderungsmanagement festgelegt werden. Die definierten Zuständigkeiten MÜSSEN sich auch im Berechtigungskonzept widerspiegeln. Zudem SOLLTE ein dedizierter Änderungsmanager (Change Manager) benannt werden. Alle beteiligten Personen MÜSSEN mit den Begriffen des Patch- und Änderungsmanagements, der Informationssicherheit und der kryptografischen Verfahren vertraut sein.

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

Es MUSS innerhalb der Strategie zum Patch- und Änderungsmanagement 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 diese haben.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein OPS.1.1.3 *Patch- und Änderungsmanagement*. Sie SOLLTEN grundsätzlich umgesetzt werden.

OPS.1.1.3.A4 Planung des Änderungsmanagementprozesses [Änderungsmanager] (S)
Es SOLLTE ein Änderungsmanagementprozess definiert werden. Es SOLLTE geprüft werden, ob die Institution sich dabei am Change-Management-Prozess der „IT Infrastructure Library" (ITIL) orientieren kann. Alle Änderungen von Hard- und Softwareständen, sowie von Konfigurationen, SOLLTEN über den Prozess des Änderungsmanagements gesteuert und kontrolliert werden.

OPS.1.1.3.A5 Umgang mit Änderungsanforderungen [Änderungsmanager] (S)
Anträge für Änderungen SOLLTEN nach einem festgelegten Verfahren eingereicht und bearbeitet werden. Es SOLLTEN alle Änderungsanforderungen (Request for Changes, RfCs) erfasst, dokumentiert und danach vom Änderungsmanager kontrolliert werden. Jede akzeptierte Änderungsanforderung SOLLTE priorisiert und kategorisiert werden. Dabei SOLLTE sichergestellt sein, dass für die jeweiligen Prioritäten auch die benötigten Ressourcen verfügbar sind.

OPS.1.1.3.A6 Abstimmung von Änderungsanforderungen [Änderungsmanager] (S)
Der zu einer Änderung zugehörige Abstimmungsprozess SOLLTE alle relevanten Zielgruppen 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 [Änderungsmanager] (S)
Der Änderungsmanagementprozess SOLLTE in die Geschäftsprozesse beziehungsweise Fachaufgaben integriert werden. So SOLLTE bei geplanten Änderungen 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. Sie 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)
Es SOLLTEN Anforderungen und Rahmenbedingungen 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 Hard- und Software (S)
Neue Hard- und Software SOLLTE getestet werden, bevor sie eingesetzt wird. Dazu SOLLTEN ausschließlich isolierte Testsysteme verwendet werden. Auch SOLLTE es für Software ein Abnahmeverfahren und eine Freigabeerklärung geben. Der Verantwortliche SOLLTE die Freigabeerklärung an geeigneter Stelle schriftlich hinterlegen. Für den Fall, dass trotz der Abnahme- und Freigabeverfahren im laufenden Betrieb Fehler in der Software 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- und 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. Ebenso SOLLTE darauf geachtet werden, dass die notwendigen Programme zur Überprüfung vorhanden sind.

OPS.1.1.3.A11 Kontinuierliche Dokumentation der Informationsverarbeitung [Änderungsmanager] (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 den Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

OPS.1.1.3.A12 Skalierbarkeit beim Änderungsmanagement (H)

Bevor ein Werkzeug zum Änderungsmanagement benutzt wird, SOLLTE seine Umsetzungsgeschwindigkeit sorgfältig geprüft werden. Es SOLLTEN Unterbrechungspunkte definiert werden können, an denen die Verteilung einer fehlerhaften Änderung gestoppt wird.

OPS.1.1.3.A13 Erfolgsmessung von Änderungsanforderungen (H)

Um zu überprüfen, ob eine Änderung erfolgreich war, SOLLTE der Änderungsmanager sogenannte Nachtests durchführen. Dazu SOLLTE er 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 [Änderungsmanager] (H)

Wenn Institutionen Änderungen an der IT-Infrastruktur vornehmen, SOLLTE der Änderungsmanagementprozess darauf reagieren. Zeitweise oder permanent nicht erreichbare Geräte SOLLTEN im Änderungsmanagementprozess durch geeignete Mechanismen berücksichtigt werden.

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.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* von Bedeutung.

G 0.9 Ausfall oder Störung von Kommunikationsnetzen

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.33 Personalausfall

G 0.37 Abstreiten von Handlungen

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen Anforderungen	CIA	G 0.18	G 0.19	G 0.20	G 0.23	G 0.25	G 0.26	G 0.27	G 0.28	G 0.33	G 0.37	G 0.39	G 0.40	G 0.45	G 0.46
OPS.1.1.3.A1		X													
OPS.1.1.3.A2		X						X		X	X				
OPS.1.1.3.A3			X	X	X	X	X		X			X	X		X
OPS.1.1.3.A4		X													
OPS.1.1.3.A5		X		X		X	X	X			X				
OPS.1.1.3.A6		X				X	X	X		X	X				
OPS.1.1.3.A7		X				X	X	X		X	X				
OPS.1.1.3.A8			X	X	X	X	X	X	X			X	X	X	X
OPS.1.1.3.A9						X	X		X						
OPS.1.1.3.A10			X	X	X				X			X	X		X
OPS.1.1.3.A11		X									X				
OPS.1.1.3.A12	A	X				X	X	X		X					
OPS.1.1.3.A13	IA	X													
OPS.1.1.3.A14	CIA	X						X							