

CHECKLISTE · TOMORIS TOOLBOX

Patch-Management: Checkliste mit Fristen, Rollen und Nachweis

Inventar, Priorisierung nach ausgenutzten Lücken, Fristen je Risiko, Ausnahmen und Nachweis, nach BSI OPS.1.1.3, NIST SP 800-40 und NISV 2026

STAND

25.10.2026

UMFANG

PDF, 11 Seiten

ONLINE

tomoris.com/downloads/patch-management-checkliste

AUF EINEN BLICK

3 Tage

kürzeste Frist der CISA nach BOD 26-04

4

Fragen entscheiden über die Frist der CISA

2. Di.

im Monat erscheinen Microsofts Sicherheitsupdates

6.6

Sicherheitspatch-Management im Anhang der DVO

FÜR WEN

- IT-Leitung und Administration, die Updates für Server, Arbeitsplätze und Netzwerkgeräte verantworten
- Informationssicherheitsbeauftragte, die Fristen, Ausnahmen und Nachweise festlegen
- Geschäftsführung wesentlicher und wichtiger Einrichtungen nach dem NISG 2026
- IT-Dienstleister, die Patch-Management für ihre Kunden übernehmen

WORUM ES GEHT

Sobald eine Sicherheitslücke öffentlich bekannt ist, steigt das Risiko in der Regel, weil Angreifer dann eher Exploits dafür entwickeln. Diese Checkliste macht Patch-Management zu einem festen Ablauf: Sie wissen, welche Systeme und Programme Sie betreiben, bewerten neue Updates nach dem tatsächlichen Risiko, halten Fristen ein und dokumentieren Ausnahmen. Grundlage sind der Baustein OPS.1.1.3 des BSI IT-Grundschutz-Kompendiums, NIST SP 800-40 Rev. 4 und die Fristen der US-Behörde CISA aus BOD 26-04. Für Einrichtungen unter dem NISG 2026 nennt die Checkliste die Anforderungen aus Anhang Nr. 6.6 und 6.10 der DVO (EU) 2024/2690.

Diese Checkliste ist eine Empfehlung von TOMORIS und ersetzt keine Rechtsberatung. Die Fristen der CISA gelten verbindlich nur für US-Bundesbehörden und dienen hier als Orientierung. Für Einrichtungen unter dem NISG 2026 maßgeblich sind der Gesetzestext, die NISV 2026 und die DVO (EU) 2024/2690 in der geltenden Fassung; Angaben von Herstellern können sich ändern.

INHALT

01	Patch-Management als fester Prozess	3
02	Voraussetzung: Inventar und Wartungsgruppen	4
03	Priorisieren nach tatsächlichem Risiko	5
04	Fristen festlegen: Empfehlung von TOMORIS	6
05	Der Ablauf je Update	7
06	Wenn kein Patch kommt	8
07	Rollen und Zuständigkeiten	9
08	Nachweis und Kennzahlen	10
09	Häufige Fehler	10
10	Quellen	11

01 —

Patch-Management als fester Prozess

Was Patch-Management umfasst und welche Vorgaben dafür gelten

NIST beschreibt Patch-Management als das Erkennen, Priorisieren, Beschaffen, Installieren und Überprüfen von Patches, Updates und Upgrades im ganzen Unternehmen und ordnet es als vorbeugende Wartung ein (NIST SP 800-40 Rev. 4). Ein Update einzuspielen oder auf eine Version ohne die Lücke umzusteigen, ist die einzige Reaktion, die eine Schwachstelle vollständig beseitigt, ohne Funktionen wegzunehmen (Abschnitt 2.1). NIST nennt vier Reaktionen auf das Risiko: akzeptieren, mindern, übertragen und vermeiden; das Patchen zählt zum Mindern.

§ 32 Abs. 4 lit. e NISG 2026

Wesentliche und wichtige Einrichtungen setzen Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen um, einschließlich Management und Offenlegung von Schwachstellen.

DVO (EU) 2024/2690, Anhang Nr. 6.6

Sicherheitspatches innerhalb einer angemessenen Frist nach Verfügbarkeit anwenden, vor dem Einsatz in Produktionssystemen testen, nur aus vertrauenswürdigen Quellen beziehen und auf Integrität prüfen; ohne Patch oder bei bewusstem Verzicht zusätzliche Maßnahmen umsetzen und Restrisiken akzeptieren. Wer auf einen Patch verzichtet, weil die Nachteile überwiegen, dokumentiert und begründet das (Nr. 6.6.2).

DVO (EU) 2024/2690, Anhang Nr. 6.10

Informationen über Schwachstellen über geeignete Kanäle verfolgen, etwa Ankündigungen von CSIRTs und Herstellern, soweit angemessen Schwachstellen-Scans durchführen und aufzeichnen, als kritisch eingestufte Schwachstellen unverzüglich beheben und begründen, wenn eine Schwachstelle keine Abhilfe erfordert.

§ 2 NISV 2026

Erklärt Art. 2 samt Anhang der DVO auch für die Einrichtungsarten der Anlagen 1 und 2 des NISG 2026 für anwendbar, die die DVO selbst nicht erfasst. Damit gelten die Nummern 6.6 und 6.10 für alle wesentlichen und wichtigen Einrichtungen, soweit nicht sektorspezifisches EU-Recht mit gleichwertigem Niveau vorgeht (§ 27 NISG 2026).

BSI IT-Grundschutz, OPS.1.1.3

Baustein Patch- und Änderungsmanagement (Edition 2023). Konzept, Zuständigkeiten, Umgang mit Autoupdates und regelmäßige Aktualisierung sind Basis-Anforderungen (A1, A2, A3, A15). In Österreich ist der Grundschutz keine Rechtspflicht, sondern ein Standard, an dem sich diese Checkliste orientiert.

Die Checkliste ist eine Empfehlung von TOMORIS. NISG 2026, NISV 2026 und DVO nennen für das Einspielen von Patches keine Fristen in Tagen: Verlangt sind eine angemessene Frist (Anhang Nr. 6.6.1 lit. a) und die unverzügliche Behebung von Schwachstellen, die die Einrichtung als kritisch einstuft (Nr. 6.10.2 lit. c).

02 —

Voraussetzung: Inventar und Wartungsgruppen

Ohne aktuelles Inventar bleibt jede Priorisierung lückenhaft

NIST empfiehlt, Software-Inventare für physische und virtuelle Systeme einschließlich OT, IoT und Container ständig aktuell zu halten und dafür Automatisierung zu nutzen. Ein Inventar, das nur monatlich oder vierteljährlich über einen Schwachstellen-Scan entsteht, soll nicht mehr genügen (Abschnitt 3.2). Statt Ausnahmen zu sammeln, ordnet NIST jedes System einer Wartungsgruppe mit gleichen Bedürfnissen zu (Abschnitt 3.4).

- ☐ Server, Arbeitsplätze, Notebooks, Smartphones, Netzwerk- und Sicherheitsgeräte, Cloud-Dienste und Anwendungen mit Version erfasst, möglichst automatisch aktualisiert (NIST 3.2).
- ☐ Je System festgehalten: Plattform, wer es verwaltet, womit es verwaltet wird, Netzanbindung, vorhandene Schutzmaßnahmen, Nutzer und ihre Rechte (NIST 3.2).
- ☐ Je System auch: Bedeutung für den Betrieb, gesetzliche oder vertragliche Vorgaben zum Patchen und Einschränkungen, etwa Neustart nur im monatlichen Wartungsfenster (NIST 3.2).
- ☐ Wartungsgruppen gebildet, z. B. Notebooks der Mitarbeitenden, Server im eigenen Rechenzentrum, Smartphones, Container in der Cloud, nicht mehr patchbare OT-Systeme (NIST 3.4).
- ☐ Für jede eingesetzte Software festgelegt, wie mit integrierten Autoupdates umzugehen ist und wie sie abgesichert und konfiguriert werden; neue Komponenten auf ihre Update-Mechanismen geprüft (OPS.1.1.3.A3).
- ☐ Supportende je Produkt erfasst, damit rechtzeitig geprüft wird, ob es noch sicher betrieben werden kann (abgeleitet aus OPS.1.1.3.A15).
- ☐ Schwachstellen-Scans mit Anmeldung (authentifiziert), weil Scans ohne Anmeldung weniger Lücken finden (NIST 3.6).
- ☐ Angaben der Hersteller zur Softwarezusammensetzung (SBOM) genutzt, wo vorhanden (NIST 3.2).

03 —

Priorisieren nach tatsächlichem Risiko

KEV, EPSS und CVSS richtig einsetzen und die Fristen der CISA kennen

OPS.1.1.3.A15 verlangt, Patches zeitnah nach Veröffentlichung zu bewerten und zu priorisieren; dabei soll geprüft werden, ob es zu dem Patch bekannte Schwachstellen gibt. Drei frei verfügbare Quellen helfen bei der Einstufung.

KEV-Katalog der CISA

Schwachstellen mit CVE-Nummer, für die es verlässliche Belege einer Ausnutzung und eine klare Abhilfe gibt, etwa ein Update des Herstellers. Die CISA empfiehlt allen Organisationen, den Katalog zu verfolgen, die Lücken vorrangig zu beheben und ihn als Eingangsgröße der eigenen Priorisierung zu nutzen.

EPSS (FIRST)

Schätzt täglich für jede veröffentlichte CVE die Wahrscheinlichkeit, dass sie in den nächsten 30 Tagen ausgenutzt wird, als Wert zwischen 0 und 1; frei als CSV-Datei und über eine Schnittstelle abrufbar.

CVSS (FIRST)

Beschreibt die technischen Merkmale einer Schwachstelle und ihre Schwere im Vergleich zu anderen. Laut Spezifikation eine Eingangsgröße für das Schwachstellenmanagement, das für die Rangfolge auch Faktoren außerhalb von CVSS berücksichtigt.

Die CISA hat ihre Vorgaben für US-Bundesbehörden am 10.06.2026 mit BOD 26-04 neu gefasst; sie ersetzt BOD 22-01 und BOD 19-02. Die Fristen der Tabelle gelten für die Behörden spätestens 180 Tage nach Erlass (Phase III). Die Frist hängt von vier Fragen ab: Ist das System öffentlich erreichbar? Steht die Lücke im KEV-Katalog? Kann ein Angreifer alle Schritte der Ausnutzung automatisieren? Erlangt er teilweise oder vollständige Kontrolle? Die Antworten zu den letzten drei Fragen veröffentlicht die CISA für jede CVE, etwa über ihr Programm Vulnrichment.

CISA BOD 26-04, Tabelle 1: Fristen für US-Bundesbehörden in Kalendertagen

INTERNET	KEV	AUTOMATISIERBAR	KONTROLLE	FRIST
ja	ja	ja	vollständig	3 Tage + Forensik
ja	ja	ja	teilweise	3 Tage
ja	ja	nein	vollständig	3 Tage + Forensik
ja	ja	nein	teilweise	14 Tage
ja	nein	ja	vollständig	3 Tage
ja	nein	ja	teilweise	14 Tage
ja	nein	nein	vollständig	14 Tage
ja	nein	nein	teilweise	60 Tage

nein	ja	ja	vollständig	3 Tage + Forensik
nein	ja	ja	teilweise	14 Tage
nein	ja	nein	vollständig	14 Tage
nein	ja	nein	teilweise	14 Tage
nein	nein	ja	vollständig	60 Tage
nein	nein	ja	teilweise	60 Tage
nein	nein	nein	vollständig	bei Erneuerung
nein	nein	nein	teilweise	bei Erneuerung

„Forensik“ heißt: innerhalb der drei Tage beheben oder abschwächen und das System auf eine Kompromittierung untersuchen. „Bei Erneuerung“ heißt: bei der nächsten geplanten größeren Aktualisierung oder Neuinstallation. Die Frist beginnt, sobald die CISA die Lücke in den KEV-Katalog aufnimmt oder die Behörde sie auf einem System findet, je nachdem, was früher eintritt. Nimmt man ein System vom Internet, verlängert sich die Frist meist; kommt die Lücke in den KEV-Katalog, verkürzt sie sich.

04

Fristen festlegen: Empfehlung von TOMORIS

Die Stufen der CISA übernehmen und mit dem monatlichen Update-Rhythmus verbinden

Die DVO verlangt eine angemessene Frist, nennt aber keine Tage. TOMORIS empfiehlt, die Fristen der CISA-Tabelle als Obergrenze zu übernehmen, weil sie Erreichbarkeit, Ausnutzung und Auswirkung zusammenführen. Legen Sie Fristen und Verfahren im Konzept nach OPS.1.1.3.A1 fest und lassen Sie es von der Geschäftsleitung freigeben.

Verfahren je Frist (Empfehlung von TOMORIS, Verfahren nach NIST SP 800-40 Rev. 4, Abschnitt 3.5)

FRIST LAUT TABELLE	VERFAHREN	BETEILIGT
3 Tage	Notfall-Patching: kurz auf wenigen Testsystemen prüfen, dann sofort verteilen. Gibt es noch keinen Patch, Notfall-Abschwächung (Funktion abschalten, System isolieren). Bei „Forensik“ das System auf Kompromittierung untersuchen.	IT-Betrieb, ISB; Geschäftsleitung informieren
14 Tage	Beschleunigtes Verfahren außerhalb des Monatszyklus: Test auf Pilotsystemen, dann gestaffelte Verteilung.	IT-Betrieb, ISB informieren
60 Tage	Regulärer Monatszyklus mit gestaffelter Verteilung, zuerst technisch versierte Pilotgruppe, dann alle; nach einer Schonfrist Installation erzwingen.	IT-Betrieb
bei Erneuerung	Mit der nächsten geplanten größeren Aktualisierung; liegt vorher ein reguläres Update vor, im Monatszyklus mitnehmen.	IT-Betrieb

Das monatliche Sicherheitsupdate von Microsoft für Windows erscheint am zweiten Dienstag jedes Monats, in der Regel um 10:00 Uhr Pacific Time; außerplanmäßige Updates kommen nach Bedarf (Microsoft Learn). Planen Sie das reguläre Wartungsfenster danach und halten Sie das Notfallverfahren für außerplanmäßige Updates bereit.

05

Der Ablauf je Update

Von der Sicherheitsmeldung bis zur Kontrolle der Installation

1

Meldungen verfolgen

Sicherheitsmeldungen von Herstellern, CSIRTs und Behörden über feste Kanäle beziehen und diese Kanäle in geplanten Abständen überprüfen (DVO Anhang Nr. 6.10.2 lit. a, Nr. 6.10.4). Neue Einträge im KEV-Katalog können Sie bei der CISA per E-Mail abonnieren.

2

Bewerten und priorisieren

Jeden Patch zeitnah nach Veröffentlichung bewerten: Welche Systeme sind betroffen, ist die Lücke ausgenutzt, ist das System aus dem Internet erreichbar? Daraus folgt die Frist (OPS.1.1.3.A15).

3

Entscheiden und begründen

Entscheiden, ob der Patch eingespielt wird. Wird er nicht eingespielt, Entscheidung und Gründe dokumentieren und zusätzliche Maßnahmen festlegen (OPS.1.1.3.A15, DVO Anhang Nr. 6.6.1 lit. d, 6.6.2).

4

Herkunft und Integrität prüfen

Updates nur aus vertrauenswürdigen Quellen beziehen und vorhandene Prüfsummen oder digitale Signaturen vor der Installation prüfen (OPS.1.1.3.A10, DVO Anhang Nr. 6.6.1 lit. c).

5

Testen

Vor dem Einsatz in Produktionssystemen testen (DVO Anhang Nr. 6.6.1 lit. b). NIST rät, eine gestaffelte Verteilung zu erwägen: zuerst wenige Systeme, etwa von Administratoren, dann eine größere Gruppe, dann alle (Abschnitt 3.5.1).

6

Mit Rückfall-Lösung ausrollen

Für jede Installation eine Rückfall-Lösung bereithalten (OPS.1.1.3.A1). Reguläre Updates nach einer Schonfrist erzwingen, wie es NIST empfiehlt, statt sie beliebig verschieben zu lassen.

7

Erfolg kontrollieren

Prüfen, ob der Patch auf allen relevanten Systemen erfolgreich eingespielt wurde (OPS.1.1.3.A15). Geräte, die zeitweise nicht erreichbar sind, gesondert nachverfolgen (OPS.1.1.3.A14, bei erhöhtem Schutzbedarf).

8

Dokumentieren

Patches und Änderungen geplant, genehmigt und dokumentiert halten (OPS.1.1.3.A1, A11). Die Dokumentation dient auch als Grundlage für Nachweise nach § 33 NISG 2026.

06 —

Wenn kein Patch kommt

Notfall-Abschwächung, nicht patchbare Systeme und Produkte ohne Herstellersupport

NIST nennt Gründe, warum sofortiges Patchen nicht immer möglich ist: Der Patch ist noch nicht verfügbar, der Hersteller unterstützt die Software nicht mehr, oder das System muss lange ohne Unterbrechung laufen. Für diese Fälle sollen Notfall-Abschwächungen und langfristige Schutzmaßnahmen vorab geplant sein (Abschnitte 2.1, 3.3, 3.5.3 und 3.5.4).

- ☐ Notfall-Abschwächungen vorbereitet: verwundbare Funktion abschalten, System isolieren; Abläufe und Werkzeuge dafür vorab festgelegt (NIST 3.5.3).
- ☐ Für jede Abschwächung ein Termin, bis wann der dauerhafte Patch eingespielt und die Abschwächung wieder entfernt ist (NIST 3.5.3).
- ☐ Nicht patchbare Systeme isoliert, etwa durch Segmentierung, und die Schutzmaßnahmen regelmäßig neu bewertet (NIST 3.5.4).
- ☐ Ist kein Patch verfügbar oder wird er bewusst nicht eingespielt: zusätzliche Maßnahmen umgesetzt und das Restrisiko bewusst akzeptiert (DVO Anhang Nr. 6.6.1 lit. d).
- ☐ Produkte ohne Herstellersupport geprüft: Können sie noch sicher betrieben werden? Wenn nicht, dürfen sie nicht mehr verwendet werden (OPS.1.1.3.A15).
- ☐ Kann eine NIS2-pflichtige Einrichtung eine Anforderung vorübergehend nicht erfüllen: kompensierende Maßnahmen umsetzen, begründet dokumentieren, Wirksamkeit mindestens jährlich prüfen (§ 4 NISV 2026).
- ☐ Ausnahmen von den Wartungsplänen zentral erfasst, überwacht und regelmäßig darauf geprüft, ob der Plan jetzt umsetzbar ist (NIST 3.5.5).

Geräte am Netzrand, etwa Firewalls, Router, Switches und WLAN-Zugangspunkte, sind ein attraktives Ziel; die CISA beobachtet breit angelegte Angriffe auf solche Geräte ohne Herstellersupport. Mit BOD 26-02 vom 05.02.2026 verpflichtet sie US-Bundesbehörden, sie innerhalb von 12 bis 18 Monaten außer Betrieb zu nehmen und durch unterstützte Geräte zu ersetzen. Für andere Organisationen ist das eine Orientierung.

07

Rollen und Zuständigkeiten

Wer entscheidet, wer umsetzt und wer kontrolliert

Rollen nach BSI OPS.1.1.3 und NISG 2026

ROLLE	AUFGABE	FUNDSTELLE
Geschäftsleitung	Stellt die Umsetzung der Risikomanagementmaßnahmen sicher und beaufsichtigt sie. Als Eskalationsebene soll die Leitungsebene in Zweifelsfällen über Priorität und Termin einer Änderung entscheiden.	§ 31 Abs. 1 NISG 2026; OPS.1.1.3.A7
Informationssicherheitsbeauftragte	Sorgt dafür, dass die Anforderungen des Bausteins erfüllt und überprüft werden; ist bei größeren Änderungen beteiligt.	OPS.1.1.3, Abschnitt 3; A1
IT-Betrieb	Grundsätzlich zuständig: bewertet, testet, verteilt und kontrolliert Patches und dokumentiert Entscheidungen.	OPS.1.1.3, Abschnitt 3; A15
Fachverantwortliche	Planen und genehmigen Änderungen, prüfen Änderungsanforderungen auf Sicherheitsaspekte, bei erhöhtem Schutzbedarf Nachtests.	OPS.1.1.3.A1, A5, A13
Alle Bereiche	Für jeden Organisationsbereich sind Zuständige benannt; die Zuständigkeiten spiegeln sich im Berechtigungskonzept.	OPS.1.1.3.A2

Zuständigkeiten in Ihrem Unternehmen (zum Ausfüllen)

AUFGABE	ZUSTÄNDIG	VERTRETUNG
Konzept und Fristen freigeben	_____	_____
Sicherheitsmeldungen und KEV-Katalog verfolgen	_____	_____
Server und Virtualisierung	_____	_____
Arbeitsplätze, Notebooks, Smartphones	_____	_____
Firewalls, Router, VPN, WLAN	_____	_____
Fachanwendungen und Cloud-Dienste	_____	_____
Ausnahmen genehmigen	_____	_____
Bericht an die Geschäftsleitung	_____	_____

08 —

Nachweis und Kennzahlen

Was Sie dokumentieren und wie Sie die Wirksamkeit messen

NIST rät von zu einfachen Kennzahlen ab, etwa dem Anteil gepatchter Lücken im ganzen Unternehmen: Sie sagen nichts darüber, ob die wichtigen Systeme und die gefährlichen Lücken behoben sind. Besser ist eine Matrix nach Bedeutung des Systems und der Schwachstelle mit dem Anteil, der innerhalb der Frist behoben wurde, sowie mittlerer und medianer Dauer (Abschnitt 3.6, Tabelle 1).

- ☐ Konzept für Patch- und Änderungsmanagement mit Fristen, Rollen und Umgang mit Ausnahmen schriftlich festgelegt und befolgt (OPS.1.1.3.A1).
- ☐ Je Patch nachvollziehbar: Bewertung, Entscheidung, Test, Installationszeitpunkt und Kontrolle (OPS.1.1.3.A1, A15).
- ☐ Liste der Ausnahmen mit Begründung, Ersatzmaßnahme, Verantwortlichen und nächstem Prüftermin (DVO Anhang Nr. 6.6.2, § 4 Abs. 3 NISV 2026).
- ☐ Ergebnisse der Schwachstellen-Scans in geplanten Abständen aufgezeichnet (DVO Anhang Nr. 6.10.2 lit. b).
- ☐ Kennzahl „innerhalb der Frist behoben“ je Wartungsgruppe und Fristenstufe, dazu mittlere und mediane Dauer (NIST 3.6).
- ☐ Wirksamkeit der Maßnahmen nach einem festgelegten Verfahren bewertet (DVO Anhang Nr. 7.1).
- ☐ Für NIS2-pflichtige Einrichtungen: Angaben zu den umgesetzten Risikomanagementmaßnahmen für die Selbstdeklaration vorbereitet, fällig innerhalb von zwölf Monaten nach Eintritt der Registrierungspflicht (§ 33 Abs. 1 NISG 2026).

09 —

Häufige Fehler

Was Patch-Management in der Praxis aushebelt

- Reguläre Updates werden verschoben, weil sie nicht dringend wirken. Das öffnet Angreifern zusätzliche Zeitfenster und macht Notfall-Patches schwerer, weil erst ältere Patches nachgezogen werden müssen (NIST 3.3).
- Nur der KEV-Katalog wird beachtet. Auch Lücken außerhalb des Katalogs können dringend sein: BOD 26-04 setzt etwa für automatisierbar ausnutzbare Lücken an Systemen im Internet 3 oder 14 Tage.
- Priorisiert wird nur nach der CVSS-Punktzahl, ohne Erreichbarkeit, Ausnutzung und Bedeutung des Systems zu berücksichtigen (CVSS-Spezifikation, BOD 26-04).

- Notfall-Abschwächungen bleiben dauerhaft bestehen, weil kein Termin für Patch und Rückbau festgelegt wurde (NIST 3.5.3).
- Nicht entschiedene oder nicht dokumentierte Ausnahmen: Für jeden nicht eingespielten Patch braucht es Entscheidung und Begründung (OPS.1.1.3.A15).
- Netzwerkgeräte, Firmware und Fachanwendungen fehlen im Inventar und damit im Patch-Zyklus (NIST 3.2).

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

Software-Hinweise der Website

tomoris.com/tools/versions-check

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

10

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- 1 **NIST SP 800-40 Rev. 4: Guide to Enterprise Patch Management Planning (April 2022)**
Abschnitte 2.1, 3.2 bis 3.6, gelesen am 25.10.2026
doi.org/10.6028/NIST.SP.800-40r4
- 2 **BSI IT-Grundschutz-Kompendium, Baustein OPS.1.1.3 Patch- und Änderungsmanagement (Edition 2023)**
Anforderungen A1 bis A3, A5, A7, A10, A11, A13 bis A15 und Rollen, gelesen am 25.10.2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- 3 **CISA: Binding Operational Directive 26-04, Prioritizing Security Updates Based on Risk (10.06.2026)**
Hintergrund, Ablösung von BOD 22-01 und 19-02, Anhang A mit Tabelle 1, gelesen am 25.10.2026
www.cisa.gov/news-events/directives/bod-26-04-prioritizing-secu...
- 4 **CISA: Reducing the Significant Risk of Known Exploited Vulnerabilities (KEV-Katalog)**
Drei Kriterien für die Aufnahme, Empfehlung für alle Organisationen, FAQ, gelesen am 25.10.2026
www.cisa.gov/known-exploited-vulnerabilities
- 5 **CISA: Binding Operational Directive 26-02, Mitigating Risk From End-of-Support Edge Devices (05.02.2026)**
Hintergrund, Begriffe, Required Actions, gelesen am 25.10.2026
www.cisa.gov/news-events/directives/bod-26-02-mitigating-risk-e...
- 6 **NISG 2026, BGBl. I Nr. 94/2025, geltende Fassung im RIS**
§ 27, § 31 Abs. 1, § 32 Abs. 4 lit. e, § 33 Abs. 1, gelesen am 25.10.2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 7 **NISV 2026, BGBl. II Nr. 290/2026**
§ 2 Anwendbarkeit der DVO, § 4 kompensierende Maßnahmen, gelesen am 25.10.2026
www.ris.bka.gv.at/eli/bgbl/II/2026/290
- 8 **Durchführungsverordnung (EU) 2024/2690, deutsche Fassung auf EUR-Lex**
Anhang Nr. 6.6, 6.10 und 7.1, gelesen am 25.10.2026
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu
- 9 **FIRST: Exploit Prediction Scoring System (EPSS)**
Beschreibung des Modells, gelesen am 25.10.2026
www.first.org/epss
- 10 **FIRST: Common Vulnerability Scoring System v4.0, Specification Document**
Abschnitt Introduction, gelesen am 25.10.2026
www.first.org/cvss/v4.0/specification-document
- 11 **Microsoft Learn: Update-Releasezyklus für Windows-Clients**
Monatliches Sicherheitsupdate, außerplanmäßige Updates, gelesen am 25.10.2026
learn.microsoft.com/de-de/windows/deployment/update/release-cyc...