



NAMUR - Interessengemeinschaft  
Automatisierungstechnik der Prozessindustrie e.V.

## AK-PRAXIS

# Patchmanagement

Stand: 19.02.2026

## AK 4.18 Automation Security

### Verfasser

Markus Lambeck, INEOS  
Dr. Alexander Piciorgros, Lanxess  
Dr. Walter Speth, Bayer  
Christian Stüttgen, Bayer  
Detlef Winkel, Bayer  
Michael Weyres, Covestro  
Björn Marmann, SpiraTec  
Tobias Halmans, admeritia  
Claudius Menthey, admeritia  
Bert De Wilde, ExxonMobil  
Sebastian Pfaller, ondeso  
Jens Wiesner, BSI  
Jens Cordt, BSI

AK-Leiter: Erwin Kruschitz, anapur

Diese AK-PRAXIS spiegelt die Erfahrungen der Mitglieder im AK 4.18 wider und ist im Rahmen des Arbeitskreises abgestimmt. Sie hat nicht den Konsensgrad einer NAMUR-Empfehlung oder eines NAMUR-Arbeitsblatts. Mit einer AK-PRAXIS hat der Arbeitskreis die Möglichkeit, zeitnah eigene Erfahrungen für interessierte Leser zur Verfügung zu stellen.

## Vorwort

Als Umfeld wird eine Automatisierungs-Infrastruktur für eine Anlage der Prozess-Chemie unterstellt.

Jede „Best Practice“ fokussiert ein Thema im Bereich Cyber Security (in der Sprachverwendung der IEC 62443 [1] [2]). Darunter fallen Abwehrmaßnahmen gegen Angriffe auf digitale intelligente Systeme der Produktions-Steuerung und – Überwachung und Angriffe unter Verwendung von digitalen intelligenten Systemen auf Produktionssysteme. Alle Themen beziehen sich auf eine Anlage, d.h. die Erhöhung der Angriffssicherheit oder die Erkennung, dass eine Anlagensteuerung kompromittiert ist oder die Maßnahmen, die in einem solchen Fall zu ergreifen sind, einschließlich der Bereinigung und der forensischen Aufklärung des Hergangs.

Es wird angenommen, dass die Leserschaft aus Personal im betrieblichen Umfeld besteht. Es richtet sich an IT-Administrierende insbesondere im Fachbereich der Operational Technology (OT). Insbesondere werden als Leserschaft nicht Security-Experten angenommen.

Im Nachfolgenden werden konkrete Handlungsempfehlungen gegeben, wie übliche Aufgaben so ausgeführt werden, dass die Cyber Security hinreichende Berücksichtigung findet.

Solange Angriffe nicht real sind, sondern lediglich von der Möglichkeit auszugehen ist, werden sie als „Bedrohung“ bezeichnet. Der Begriff „Gefährdung“ steht für Schaden, der ohne Intention „passiert“ (etwa Systemausfall infolge von Verschleiß) und wird dagegen abgegrenzt. Anstatt auf Bedrohungen abzustellen, könnte man auch das entstehende Risiko betrachten. Dazu wäre allerdings erforderlich, die Wahrscheinlichkeit des Angriffes einschätzen zu können, sowie den entstehenden Schaden. Dieser hängt allerdings von der konkreten Anlage ab und kann in der generellen Betrachtung nicht beziffert werden. Grundsätzlich nutzt ein Angriff eine Schwachstelle aus und mithin wäre alternativ zur Bedrohung auch eine Betrachtung der Schwachstellen möglich gewesen.

## Inhaltsverzeichnis

<b>1</b>	<b>Thema und Eingrenzung („Scope“)</b> .....	<b>4</b>
1.1.	Was bedeutet Patchen? .....	4
1.1.1.	Geltungsbereich von Patches .....	4
1.2.	Das „Zeitfenster der Gefährdung“ .....	4
1.3.	Berührte Sicherheitsziele .....	5
<b>2</b>	<b>Motivation und Zielsetzung</b> .....	<b>6</b>
<b>3</b>	<b>Empfehlungen</b> .....	<b>6</b>
3.1.	Generell.....	6
3.2.	Der Patchmanagement Prozess – Verantwortlichkeiten und Durchführung.....	7
3.2.1.	Voraussetzung .....	7
3.2.2.	Identifikation .....	7
3.2.3.	Klassifizierung .....	8
3.2.4.	Bezug der Patches.....	8
3.2.5.	Prüfung auf Verträglichkeit.....	8
3.2.6.	Freigabe zur Installation.....	9
3.2.7.	Einbringen der Patches.....	9
3.2.8.	Kontrolle und Korrektur .....	9
3.2.9.	Change-Management .....	10
<b>4</b>	<b>Technische Hintergrundinformation</b> .....	<b>10</b>
<b>5</b>	<b>Besondere Hinweise zum Patchen in Level 0,1 Systemen</b> .....	<b>11</b>
<b>6</b>	<b>Ausblick</b> .....	<b>12</b>
<b>7</b>	<b>Abbildungsverzeichnis</b> .....	<b>12</b>
<b>8</b>	<b>Literaturverzeichnis</b> .....	<b>12</b>

## 1 Thema und Eingrenzung („Scope“)

### 1.1. Was bedeutet Patchen?

Patchmanagement ist Teil einer umfassenden Cybersicherheitsstrategie, die die Cybersicherheit durch die Installation von Patches (auch Software-Updates, Software-Upgrades, Firmware-Upgrades, Service Packs, Hotfixes, BIOS-Updates (Basic Input Output System) und andere digitale elektronische Programm-Updates genannt) erhöht, um sowohl Fehler und Cybersicherheitschwachstellen zu beheben als auch Betriebsfähigkeit und Zuverlässigkeit sicherzustellen. [3]

Diese Definitionen können herstellerabhängig abweichen.

In diesem Dokument wird der Begriff Patch nur für Änderungen zum Beheben von Cybersicherheitschwachstellen oder Fehlfunktionen verwendet. Der Funktionsumfang erweitert sich nicht.

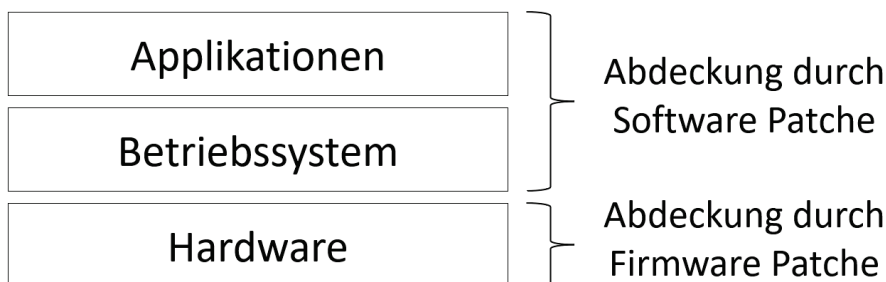
Durch die Installation von Updates bzw. Patches, werden Veränderungen am Betriebssystem vorgenommen, diese können zu Beeinträchtigungen an der Applikationssoftware des Automatisierungssystem-Herstellers führen. Daher sind Freigabeprozesse z.B. des Systemlieferanten üblich oder falls kein entsprechendes Angebot des Systemlieferanten vorhanden ist, können auch interne Testsysteme aufgebaut werden, an denen die möglichen Auswirkungen getestet werden können. Im Anschluss kann je nach Kritikalitätsstufe des entsprechenden Systems eine entsprechende (interne) Freigabe erfolgen.

Die Veröffentlichung von Patchen erfolgt sowohl chronologisch, z.B. monatlich, als auch ereignisgesteuert, z.B. bei einer kritischen Sicherheitslücke.

#### 1.1.1. Geltungsbereich von Patches

Ein Patch kann sich auf die Software eines Systems, also das Betriebssystem oder die Applikationen bzw. Programme oder auf eine darunter liegende Ebene beziehen, der hardwarenahe Sicherheitslücken und Fehler beheben soll. Hardwarenahe Sicherheitslücken z.B. im UEFI-Bios oder in der Management Engine können ohne Kenntnisnahme des Betriebssystems (inkl. installierter Virenschutzsoftware) über das Netzwerk ausgenutzt werden.

Dieses Dokument betrachtet im Allgemeinen alle Ebenen der Automatisierungspyramide, besondere Hinweise für die Ebenen 0 und 1 befinden sich in Kapitel 5.



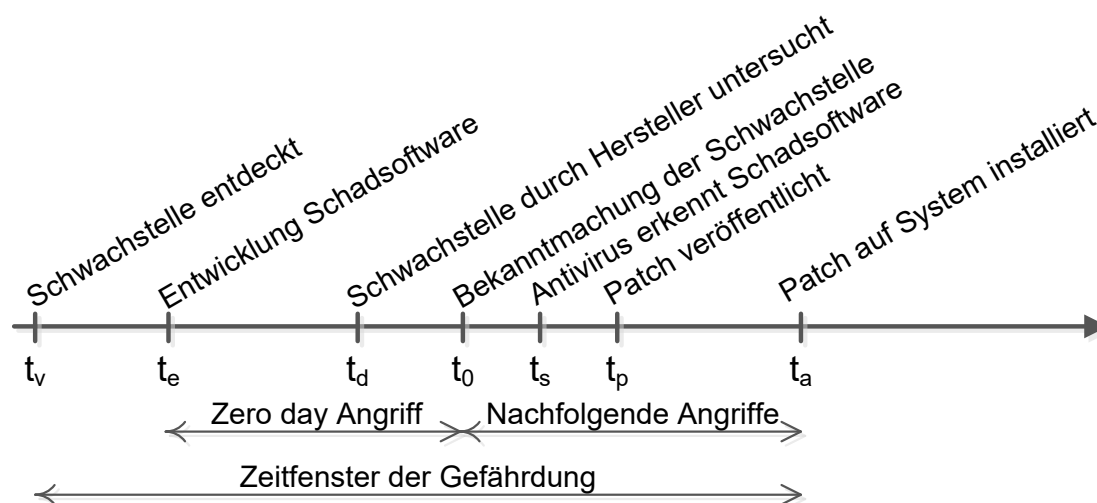
**Abbildung 1: Patchebenen**

„Software Hersteller“ meint im folgenden Text sowohl den Hersteller eines Betriebssystems als auch einer Applikation. Im Falle eines gesamten Automatisierungssystems bestehend aus Hardware, Betriebssystem und Applikationen wird der Begriff „Hersteller des Automatisierungssystems“ verwendet. Wird nur „Hersteller“ als Begriff verwendet, kann sowohl der Hersteller der Software als auch des Automatisierungssystems gemeint sein.

### 1.2. Das „Zeitfenster der Gefährdung“

Wie zuvor geschildert, enthält jede Soft-/Firmware neben den erwünschten Funktionen auch ggf. Fehlfunktionen, die kurzum Schwachstellen genannt werden. Angreifer versuchen mittels dafür entwickelter Schadsoftware diese Schwachstellen auszunutzen, um Zugriff auf das System zu bekommen oder dessen Funktionen zu beeinflussen. Die nachfolgende Beschreibung schildert den typischen Ablauf für das „Zeitfenster der Gefährdung“ (Window of exposure), kann in den einzelnen Punkten aber auch abweichen.

Die Erkennung von Schwachstellen durch den Angreifer mit der Entwicklung von Schadsoftware geschieht häufig, bevor der Hersteller auf die Schwachstelle aufmerksam wird oder reagiert und die Fehlfunktion untersucht. Eine öffentliche Bekanntmachung von Schwachstellen erfolgt in der Regel erst, wenn der Hersteller die Schwachstelle selbst entdeckt oder von Dritten informiert wird. In solchen Fällen erfolgt die Veröffentlichung beispielsweise über die National Vulnerability Database (NVD), den Warn- und Informationsdienst (WID) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder über CERT@VDE (Computer Emergency Response Team). Es gibt jedoch auch Fälle sogenannter Full Disclosure, bei denen Sicherheitsforscher Schwachstellen ohne vorherige Abstimmung mit dem Hersteller direkt öffentlich machen. Die Hersteller von Antivirus-Produkten untersuchen die Schadsoftware und nehmen diese für die Erkennung in ihre Signaturen auf. Es wird nicht immer eine Schadsoftware entwickelt. Es wird ein Exploit entwickelt, der in eine Schadsoftware integriert werden kann oder auch manuell im Verlauf eines Angriffs genutzt werden kann. Die Erkennung erfolgt zudem nicht immer durch ein Anti-Virus-Programm, sondern kann auch über netzwerkbasierende Intrusion Detection Systeme (IDS) erfolgen. Diese Systeme überwachen den Netzwerkverkehr auf verdächtige Aktivitäten und Anomalien, um potenzielle Angriffe zu erkennen. Es benötigt Zeit, bis der Hersteller einen Patch veröffentlicht, welcher die Schwachstelle schließt. Erst mit der Installation des Patches durch den Anwender ist die Schwachstelle geschlossen. Der Zeitraum von der Entdeckung einer Schwachstelle bis zur Installation des Patches ist das „Zeitfenster der Gefährdung“.



**Abbildung 2: Zeitfenster der Gefährdung**

### 1.3. Berührte Sicherheitsziele

Das Einbringen eines Patches erfolgt meist durch eine Installationsroutine, die abschließend, falls benötigt, auch einen Neustart des Rechners nach sich zieht. Für die Automatisierungssysteme ist die Verfügbarkeit i.d.R. ein hohes Schutzziel neben der Vertraulichkeit und Integrität (z.B. bei Safety stärker ausgeprägt). Die Verfügbarkeit wird durch die Installation und den nachfolgenden Neustart reduziert. Die Integrität und auch die Verfügbarkeit des Systems können durch neue Fehlfunktionen oder Kompatibilitätsprobleme des Patches negativ beeinflusst werden.

Es sollte jedoch auch beachtet werden, welche Sicherheitsziele gefährdet sind, wenn der Patch nicht installiert wird. In diesem Fall kann die Verfügbarkeit ebenfalls beeinträchtigt werden, wenn die zugrunde liegende Schwachstelle ausgenutzt wird. Zudem droht eine Verletzung der Integrität des Systems durch die Möglichkeit von Manipulationen nach einem erfolgreichen Angriff auf die Schwachstelle. Je nach Schwere der Schwachstelle kann es sogar notwendig sein, das betroffene System bis zum nächsten Wartungsfenster zu isolieren, um weitere Schäden zu verhindern.

## 2 Motivation und Zielsetzung

Moderne Automatisierungssysteme bauen fast ausschließlich auf Standard-Betriebssysteme und können unter Umständen auch Applikationen aus dem Office-IT Umfeld nutzen. Jedoch können bestimmte Methoden aus der Office-IT nicht ohne eine besondere Planung und ggf. testen in einer Testumgebung angewendet werden. In jeder Software gibt es Schwachstellen (unerwünschte Funktionen), die ein Angreifer ausnutzen kann. Bei Automatisierungssystemen sind Angreifer im extremen Fall beispielsweise in der Lage, die Kontrolle über das System zu übernehmen und den Produktionsprozess zu beeinflussen.

Das Ziel von Patchmanagement ist das „Zeitfenster der Gefährdung“ (s.o.) über den nachfolgend beschriebenen Prozess je nach Gefährdung möglichst kurz zu halten und somit das Risiko zu minimieren. Dieses Papier beschreibt einen Weg Patches zu bewerten und möglichst gezielt zu installieren, um die Verfügbarkeit der Anlage maximal zu gewährleisten. Es müssen Prozesse etabliert sein, die eine interne Bewertung der Schwachstellen vornimmt, die zur Entscheidung führt, welcher Kritikalität die Schwachstelle zuzuordnen ist. Bei besonders kritischen Schwachstellen kann es notwendig sein, kurzfristig zu handeln, bei weniger kritischen die Installation gebündelt in einem geplanten Wartungsfenster durchzuführen.

In manchen Fällen vergeht viel Zeit, bis der Hersteller die Patches veröffentlicht bzw. freigibt. In diesen Fällen sollte der Betreiber Ersatzmaßnahmen implementieren, welche das Risiko trotz fehlender Patches reduziert.

Im Folgenden wird ein Prozess beschrieben, der diese Aspekte berücksichtigt und konkrete Empfehlungen zum Patchmanagement beinhaltet.

## 3 Empfehlungen

### 3.1. Generell

Die beste Schutzmaßnahme ist der Verzicht auf Funktionen und Programme (siehe NAMUR BP Härtung) nach dem Motto: „Was nicht installiert ist, muss auch nicht gepatcht werden.“

Darüber hinaus kann die Notwendigkeit zum Patchen durch Ersatzmaßnahmen deutlich reduziert werden (siehe z.B. NAMUR BP System Architecture).

Es sollte möglichst eine Software oder ein Automatisierungssystem eingesetzt werden, für welches der Hersteller zeitnah Patches veröffentlicht und einen möglichst langen Supportzeitraum bietet. Die Verantwortlichkeit dafür liegt beim Hersteller, der seine Applikation rechtzeitig für neue Plattformen mit verfügbarem Support vorbereiten muss (so ist z.B. Software in Package Units als „Verschleißteil“ zu betrachten). Bei neuer Software ist durch die fehlende Bewährung anfangs eine geringere Stabilität und somit Verfügbarkeit des Automatisierungssystems einzukalkulieren.

Die Windows Update Funktion bietet nicht automatisch alle Patches und Updates für ein System über die windowseigene Updatefunktion an. Herstellerspezifische und individuelle Updates, unternehmensspezifische Patches und spezielle Hotfixes können ausgeschlossen sein und es obliegt dem Betreiber, sich über die zusätzlichen Patches zu informieren, auf Nebenwirkungen zu untersuchen und die für ihn passenden auswählen, dazu kann der Microsoft Update-Katalog genutzt werden [4].

Es wird empfohlen alle vom Softwarehersteller veröffentlichten Patches zunächst auf Testsystemen und im Anschluss auf weniger kritischen Systemen auszurollen, für die es auch eine Freigabe des Automatisierungssystem Herstellers gibt. Je nach Volumen ist eine Liste der nicht für die Installation freigegebenen Patches (Patch Blacklist, auch „Deny List“, „Exclude List“ oder „Block List“) von Vorteil. Dabei ist jedoch der „Nachlauf“ zu beachten, der entstehen kann, wenn der Automatisierungssystem Hersteller Updates noch nicht kategorisiert und damit freigegeben hat. Alternativ kann auch eine Liste der für eine Installation freigegebenen Patches (Patch WhiteList, auch „Allow List“, „Trustlist“, or „Safe List“) zum Einsatz kommen.

Eine Liste der freigegebenen Patches für die verwendeten Programme und Funktionen des Systems sollte vom jeweiligen Systemhersteller eingefordert werden.

Es sollte eine Automatisierung des Patchmanagements angestrebt werden. Dies gilt insbesondere für den Bezug von Informationen zu Patches, sowie den Abgleich mit der bestehenden Infrastruktur. Hierfür kann beispielsweise das Common Security Advisory Framework genutzt werden. Dies spezifiziert sowohl ein maschinenverarbeitbares Format der Informationen zu Cybersicherheitsschwachstellen und deren Behebung durch Patches oder Workarounds, als auch den automatisierten Bezug [5] [6].

### 3.2. Der Patchmanagement Prozess – Verantwortlichkeiten und Durchführung

Für eine sorgsame Planung und Durchführung ist es ratsam, sich vorbereitend mit dem Prozess vom Hersteller des Automatisierungssystems und seinem Rollenverständnis vertraut zu machen. Die dabei wichtigen Punkte sind in die nachfolgenden Teilschritte eingeflossen.

#### 3.2.1. Voraussetzung

Für den Ist-Zustand sollte der Betreiber eine Inventarisierung aller Automatisierungskomponenten mit den spezifischen Merkmalen, z.B. Hardwarestand, Firmwarestand, installierte Software und Patches vornehmen. Hierbei ist insbesondere auch Drittanbietersoftware zu berücksichtigen, die eine automatisierte Inventarisierung aller Systemkomponenten inkl. der Softwareständen durchführt. Dies kann durch Hersteller mittels einer Software Bill of Materials (SBOM) erfolgen. Details dazu finden sich unter anderem in [7].

Hervorzuheben ist, dass solche Anwendungen alle Informationen in eine Datenbank schreiben und somit eine händische Dokumentation entfallen kann. Dies kann Bestandteil eines Asset-Managements sein.

Bei Systemen die End of Support sind, für die keine sicherheitsrelevanten Updates mehr bereitgestellt werden, sind gesonderte Abwägungen zu treffen. Diese werden im Dokument „Umgang mit "End of Support" in industriellen Steuerungs- und Automatisierungssystemen“ [8] beschrieben.

#### 3.2.2. Identifikation

Um die Frage beantworten zu können, welche Schwachstellen und Patches es gibt, bedarf es eines wiederkehrenden Soll/Ist-Vergleichs. Zeitpunkt und Person für den Vergleich sind festzulegen.

Für den Soll-Zustand muss der Hersteller eine zyklisch aktualisierte Liste der freigegebenen Patches zur Verfügung stellen. Dies kann z.B. für die Microsoft-Patches in Form einer XML-Datei erfolgen, die sich an die Vorgabe der IEC 62443 2-3 [1] [2] hält.

Der Betreiber sollte sich damit auseinandersetzen, wie und wann der Hersteller über Schwachstellen und Patches informiert. Für diese Information kann/sollte das Common Security Advisory Format (CSAF) genutzt werden [9]. Dies ermöglicht den automatisierten Bezug von Security-Advisories und Abgleich mit dem Inventar. Dabei können sowohl Softwarehersteller direkt als auch Automatisierungssystemhersteller als Informationsquelle genutzt werden.

Ferner ist der vom Hersteller zugesicherte Supportzeitraum für die Bereitstellung der Patches zu berücksichtigen und bei Bedarf zu verhandeln (Life Cycle Management). Sollte das nicht gelingen, sind bei einem Betrieb des Systems über das Supportende hinaus Ersatzmaßnahmen bis hin zur Abschottung zu ergreifen.

Es ist mit dem jeweiligen Hersteller zu klären, wer die Patches installieren darf und wie die Gewährleistung für das System geregelt ist.

In Ergänzung sollten auch unabhängige Quellen beobachtet werden, wie z.B. Fachpresse, BSI und ICS-CERT. Hilfreich kann hier auch die Auswertung von CVE (Common Vulnerabilities and Exposures) sein, die vom Hersteller oder aber auf spezialisierten Seiten im Internet zur Verfügung gestellt werden.

Für qualifizierte Anlagen ist das Einspielen von Patchen oder generell die Verwendung von nicht vom Hersteller zertifizierter Software im Vorfeld zu bewerten. Die am Markt befindlichen Automatisierungskomponenten werden mit einer Bescheinigung geliefert, dass sie der FDA-Richtlinie 21 CFR Part 11 [10] [11] genügen.

Dies dient idR. als Basis für die Qualifizierung der Anwendung. Software ist für ein bestimmtes Betriebssystem mit einem festgelegten Patch Stand freigegeben. Wird davon abgewichen, ist die bescheinigte Übereinstimmung mit der FDA-Richtlinie in Frage zu stellen.

Resultierend daraus dürfen nur vom Hersteller der Automatisierungskomponente explizit für den Betrieb in einer qualifizierten Umgebung freigegebene Software oder deren Modifikationen auf dem System eingebracht werden. Dies schließt Updates und Patches für das Betriebssystem ein.

Bei der Auswahl der zu installierenden Patches ist die Hard- und Firmware zu berücksichtigen, da Abhängigkeiten in Bezug auf die zu installierende Software bestehen können, siehe dazu Abbildung 1: Patchebenen.

### 3.2.3. Klassifizierung

Für ein vereinfachtes Vorgehen in großen Installationen ist eine Klassifizierung der Automatisierungssysteme mit Grundregeln für das Einbringen von Patches ratsam. Z.B.: Systeme im Falle einer Fehlfunktion oder eines Systemausfalls.

A. ohne negativen Einfluss auf die Produktion:

- Zeitnahe vollständige Installation der Patches

B. mit negativem Einfluss auf die Produktion:

- Vollständige Installation der Patches zum nächstmöglichen Zeitpunkt
- Oder Installation ausgewählter Patches zum nächstmöglichen Zeitpunkt (z.B. nur Patches, die kritische Schwachstellen beheben)

Es sind mögliche Risiken zu betrachten, die durch das Patchen entstehen können und evtl. Gegenmaßnahmen im Vorfeld einzuplanen. Eine existenzielle Gegenmaßnahme kann z.B. die Sicherstellung eines existierenden Backups vor dem Patchen sein. Zudem ist zu erwähnen, dass der Erfolg der Backup-Erstellung geprüft werden sollte und die Prüfung idealerweise Teil des Freigabe-Prozesses ist.

Steht kein Patch zur Verfügung oder kann das System nicht gepatcht werden, sollten in einer Risikobetrachtung alternative Maßnahmen festgelegt werden, um eine Ausnutzung der Schwachstelle zu verhindern. Dabei sollte nicht nur die Kritikalität des Patches (CVSS, Common Vulnerability Scoring System [12]) im Vordergrund stehen, sondern auch die Exposition (wie einfach kann ein Angreifer das System erreichen) sowie betriebliche Auswirkungen einer Kompromittierung berücksichtigt werden (z. B. mittels des SSVC, Stakeholder specific vulnerability classification [13]). Als alternative Maßnahme ist es beispielsweise möglich, die betroffenen Automatisierungssysteme in ein separates Netzsegment zu platzieren.

### 3.2.4. Bezug der Patches

Es muss mit dem Hersteller geklärt werden, wie und wo die Patches bereitgestellt werden. In jedem Fall ist eine vertrauenswürdige Quelle zu wählen.

Neben dem Beschaffungsweg ist die Überprüfung auf Freiheit von Schadsoftware und der sichere Ablageort festzulegen und wie die Patches zur Installation auf die Systeme gelangen.

In großen Installationen ist der Einsatz von Werkzeugen zur Software-Distribution empfehlenswert, insbesondere, da es nicht üblich ist, im Automatisierungsnetz Internetzugang zu haben. Auch kann so sichergestellt werden, dass vom Hersteller der Automatisierungskomponente nicht freigegebene Patches auch nicht installiert werden.

### 3.2.5. Prüfung auf Verträglichkeit

Die Verträglichkeit eines Patches sollte in Abhängigkeit der Softwareversionen überprüft und in Listenform z.B. laut IEC 62443 2-3 [1] [2] im XML-Format, vom Hersteller bereitgestellt werden. Das muss in einem Zusammenspiel zwischen dem Hersteller des Automatisierungssystems, und Betreiber festgelegt werden. Sofern besondere Randbedingungen gelten, sind diese durch den Hersteller mitzuteilen (z.B. Installieren weiterer Softwarepakete, um die Verträglichkeit sicherzustellen). Gibt es keine Freigabe für einen Patch, aufgrund folgender Probleme:

- Keine Freigabe des Patches, weil eine Hardwareinkompatibilität vorliegt
- Der Hersteller des entsprechenden Systems hat die Freigabe des Patches abgelehnt
- Der Patch hat das System im Test zum Absturz gebracht

Dann ist durch den Hersteller aufzuführen, welche Ersatzmaßnahmen empfohlen sind.

Die Anforderungen vom Betreiber an den Hersteller sollten an einer Stelle gesammelt dargestellt werden, damit diese nicht aus den einzelnen Abschnitten herausgesucht werden müssen. Alternativ könnten die Anforderungen besonders formatiert/hervorgehoben werden.

Ferner ist mit dem Hersteller des Automatisierungssystems abzustimmen, mit welcher Tiefe und Umgebung er die Patches auf Verträglichkeit geprüft hat: Wurde das System nach dem Patchen nur auf offensichtliche Fehler untersucht, oder gab es eine detaillierte Überprüfung aller Funktionen?

Der Verantwortliche auf Betreiberseite muss festlegen, ob eine Prüfung der Verträglichkeit in der Betreiberumgebung erforderlich ist. Dafür kann es sinnvoll sein, ein eigenes Testsystem vorzuhalten, auf dem die Patches vor Einbringen in die produktiven Systeme installiert und auf evtl. unerwünschte Auswirkungen getestet werden. Dies ist besonders bei komplexeren Systemen empfehlenswert. Eine virtualisierte Umgebung kann hier von Nutzen sein.

Sollte eine Verträglichkeitsprüfung in einem Testsystem nicht möglich sein, so sollte mit unkritischen Systemen begonnen werden. Dabei sollte eine Beobachtung des entsprechenden Systems erfolgen, so dass bei Auffälligkeiten die Auswirkungen nicht zu gravierend sind.

### 3.2.6. Freigabe zur Installation

In der Betreiberorganisation sollten Rollen und Rechte definiert sein (z.B.: Systemverantwortlicher und Betreiber, (externe) Service Dienstleister). In einer Verantwortlichkeit können mehrere Rollen enthalten sein.

Der Installationszeitpunkt ist immer zwischen dem Systemverantwortlichen, dem Betreiber und den Anwendern abzustimmen. Dabei sind Produktions- und Wartungszeiträume zu berücksichtigen.

Im Anschluss ist festzulegen, wer die Patches zur Installation anweist und wer diese darauf hin installiert.

### 3.2.7. Einbringen der Patches

Es ist festzulegen, ob vor dem eigentlichen Einbringen der Patches ein Backup benötigt wird, um bei einem anschließenden Fehlverhalten ein Restore durchführen zu können (für Backup/Restore müssen Prozesse etabliert sein). Für die Installation ist eine Anleitung zu erstellen.

Das Einbringen der Patches ist mit allen Detailinformationen vorzugeben und danach durchzuführen:

- Information über die Patches mit genauer Bezeichnung
- Systeme auf denen die Patches installiert werden sollen
- Zeitpunkt und Zeitraum der Installation
- Name des Durchführenden oder der ausführenden Einheit

Bei einer Installation von Patchen auf gleichartigen Systemen ist es ratsam, die Systeme nacheinander zu behandeln und mit weniger kritischen zu beginnen, um den Patchvorgang bei Fehlfunktionen unterbrechen und eine Korrektur herbeiführen zu können. Bei redundanten Systemen sind die Vorgaben vom Hersteller des Automatisierungssystems zu berücksichtigen. Dabei ist der fachgerechte Prozess beim Herunterfahren eines Systems inkl. des Stoppens der Runtime und anschließendes Entladen der Projekte zwingend einzuhalten.

Hinweis: Wenn es durch den Hersteller freigegeben ist oder es keine Herstellergarantie mehr gibt, kann das nachfolgende Vorgehen angewendet werden.

Auf Windows-basierten Systemen findet sich in manchen Fällen ein „Write Filter“, welcher permanente Änderungen am System unterbindet. Das steht einer bewussten Anpassung des Systems über die Installation von Updates natürlicherweise im Wege. In älteren Varianten des Betriebssystems ist die Funktion auch unter „File Based Write Filter“ (FBWF) bzw. „Enhanced Write Filter“ (EWF), mit jeweils etwas abweichender Detailfunktion, enthalten. [14]

Im Falle eines solchen Schreibschutzes sollte vorab ein Backup durchgeführt werden, da ein vorhandener Schreibschutzfilter für den Updatevorgang temporär deaktiviert wird.

Sowohl die sorgsame Installation der Patches als auch die Ausführung der Technik in Redundanz erhöhen die Verfügbarkeit des Systems.

### 3.2.8. Kontrolle und Korrektur

Es ist festzulegen, wie nach der Installation der Patches die Funktion und Integrität des Systems sichergestellt wird. Hierbei ist eine Checkliste empfehlenswert.

Es sollte vorbereitet werden, wie bei einem Fehlverhalten des Systems vorzugehen ist. Dazu gehören neben dem Informationsfluss auch Restore-Maßnahmen, um das System in den stabilen Zustand vor dem Patchen zurückzuführen. Alternativ können weitere Korrekturmaßnahmen den Systemzustand stabilisieren.

Zu guter Letzt ist eine Überprüfung des neuen Softwarestandes in der Inventarisierung der Automatisierungssysteme notwendig und unter GxP konformen Voraussetzungen auch verpflichtend.

### 3.2.9. Change-Management

Die zuvor beschriebenen Schritte des Patchmanagement Prozesses sollten in ein Change-Management eingebunden werden. Dadurch entsteht eine nachvollziehbare Dokumentenlage.

Alternativen:

Es können alternative Techniken wie das Whitelisting, auch „Allowlisting“, „Trustlisting“ oder „Safelisting“ genannt, von Anwendungen oder virtuelles Patchen eingesetzt werden. Sollte kein Patchen möglich sein, muss eine Segmentierung, Einsatz von Sicherheit Gateways bis hin zu einer kompletten Netzwerktrennung in Betracht gezogen werden.

## 4 Technische Hintergrundinformation

Im Falle einer vollständigen Netzwerktrennung (Inselsystem) ist ein direktes Deployment von Patches nicht möglich. Hierbei ist die Frage zu betrachten, ob ein aktueller Patch für dieses Inselsystem überhaupt erforderlich ist, da dieses nicht von außen angreifbar ist.

Hier sollten Maßnahmen wie Zugangsbeschränkungen (Berechtigungen und physisch) in der Regel ausreichen, Siehe hierzu auch AK Praxis Härtung.

Sollte es trotzdem notwendig werden ein Inselsystem zu patchen, so muss sichergestellt werden, dass der Patch (die erforderlichen Dateien) unverändert in das Inselsystem eingebracht werden. Hierzu kann z.B. die Hashwert oder Signatur validiert werden. Außerdem ist zu beachten, dass verwendete Übertragungsmedien frei von Schadsoftware sind.

Für alle anderen Systeme sollte ein klare Compliance Anforderungen erstellt und angewendet werden, diese kann je nach Angreifbarkeit des Systems , Kritikalität des Systems und Risiken/Folgen eines Angriffs den jeweiligen Bedürfnissen angepasst werden.

Es ist empfehlenswert hierzu ein automatisiertes System zu nutzen, welches in der Lage ist, entsprechend der definierten Compliance Richtlinien auf relevante und kritische Updates zu prüfen und entsprechend zu benachrichtigen.

Compliance-Anforderungen für Betriebssysteme				
Zone	Klasse	Installiert	Zulässiges Alter (ab Veröffentlichungsdatum)	Überprüfungshäufigkeit
MES	Security	Alle	z.B. 30 Tage <sup>(1)</sup>	z.B. 60 Tage
Plant	Security	Alle	z.B. 30 Tage <sup>(1)</sup>	z.B. 60 Tage
DCS	Security	Herstellerspezifisch	z.B. 45 Tage <sup>(2)</sup>	z.B. 60 Tage
1 Nach der Veröffentlichung durch Microsoft®				
2 Nach der Freigabe durch den DCS-Hersteller				

Tabelle 1: Compliance-Anforderungen für Betriebssysteme

Ferner sind Patch-Zeitrahmen und Dringlichkeitsbewertungen durchzuführen.

Patch-Zeitrahmen	Bedingungen
Unverzöglich	Patches, die eine hohe Dringlichkeit erfordern (z. B. kritische Zero-Day-Schwachstellen) [15] [2]
Innerhalb eines Monats	Patches, die eine mittlere Dringlichkeit haben [2]
Im nächsten regulären Patch-Zyklus	Patches, die eine niedrige Dringlichkeit haben oder nicht sicherheitsrelevant sind [2]
Anlagenstillstand	Patches, die wegen Verfügbarkeitsanforderungen der Produktionsanlage nur während eines geplanten Stillstands installiert werden können [2]
Niemals	Patches, die gemäß Risikoanalyse als schädlich eingestuft wurden oder vom Hersteller nicht freigegeben sind [2]

Tabelle 2: Patch-Zeitrahmen und Dringlichkeitsbewertungen

### Besonderheiten für Prozessleitsysteme

In industriellen Umgebungen unterliegen Prozessleitsysteme hohen Verfügbarkeitsanforderungen. Daher erfolgt das Einspielen von Betriebssystem-Patches, die keine unmittelbare Sicherheitsbedrohung darstellen, im Rahmen der festgelegten Systemwartung. Patches für Automatisierungs- und Steuerungssysteme erfordern oft spezielle Freigaben und Tests, um die Betriebssicherheit zu gewährleisten. Ein unkontrolliertes Patchen könnte zu unerwarteten Systemausfällen oder Inkompatibilitäten führen. Daher ist eine enge Abstimmung mit den entsprechenden Sicherheits- und Wartungsteams erforderlich.

## 5 Besondere Hinweise zum Patchen in Level 0,1 Systemen

Bei Automatisierungssystemen, die eine direkte Interaktion mit dem Prozess haben, müssen folgende weiterführenden Überlegungen thematisiert werden. Mit dem Bezug auf das Purdue-Modell [16] befinden sich diese Systeme und Geräte in der Regel auf den Ebenen 0 und 1 dazu gehören folgende industrielle Steuerungssysteme (ICS): Schutzsysteme, SPS, Steuerung und Schutz von Turbomaschinen, Kesselmanagementsysteme, Prozessanalytoren, Motorsteuerungszentren, intelligente Motorrelais, Frequenzumrichter, automatisierte Ventile, Feldmessungen usw.

Bei Systemen die Prozesse im Dauerbetrieb und mit sehr langen Laufzeiten abbilden (z.B. kann ein Öl- und Gasraffinerieprozess einen Stillstand nur alle 7 Jahre haben) werden häufig Systeme und Geräte eingesetzt, die Teil einer maßgeschneiderten integrierten Lösung sind. Diese bestehen meist aus einem Zusammenschluss aus Legacy-Systemen und neueren Technologien.

Beim Patchen (z. B. ein Firmware-, Software- oder Anwendungsupdate) dieser Systeme besteht das Risiko erhebliche Wechselwirkungen auf Prozesse zu erzeugen, mit denen sie interagieren, dies können Prozesssicherheitsvorfälle, Produktionsunterbrechungen, ungeplante Kapazitätsverluste, nicht spezifikationskonforme Produkte oder gar Ausfallzeiten sein. Somit wird das Patchen zu einer komplexen Aufgabe, die viel Planung, Vorbereitung und Vorabtests in einer integrierten Offline-Testumgebung erfordert, um unerwünschtes/unregelmäßiges Verhalten eines Soft- oder Firmware-Updates zu vermeiden. Wenn in speziellen Fällen keine integrierte Offline-Testumgebung verfügbar ist, oder keine Möglichkeit besteht diese zu entwickeln, gibt es nur begrenzte Patch-Möglichkeiten.

In solchen Fällen sollten Sicherheitsmaßnahmen, die ein eventuelles Patchen vermeiden können, in die Sicherheitsstrategie einfließen:

- Reduzierung oder Beseitigung von Bedrohungsszenarien: z.B. vorübergehende Abschaltung eines Remote-Dienstes.
- Härtung des Designs, der Architektur und Konfiguration: z.B. Segmentierung, Zonierung, Verwendung von Firewalls, Datendiodeen usw.
- Verringerung der Abhängigkeit von Turnarounds für Software-/Firmware-/Systemaktualisierungen: z.B. durch Erhöhung der Redundanz auf Geräteebene, durch redundante Systeme, durch den Einsatz von Systemen, die keine Firmware- oder Software-Updates erfordern.

## 6 Ausblick

Aktuell ist der Aufwand für Patchmanagement überaus hoch, da bislang sehr wenige Schritte automatisiert durchgeführt werden können. Mit CSAF steht zukünftig ein mächtiges Werkzeug zur Verfügung, das zumindest die Schritte Identifikation und Entscheidung über Notwendigkeit der Anwendung eines Patches stark vereinfachen wird. [17] [9]

## 7 Abbildungsverzeichnis

Abbildung 1: Patchebenen ..... 4

Abbildung 2: Zeitfenster der Gefährdung..... 5

## 8 Literaturverzeichnis

- [1] IEC, „Understanding IEC 62443,“ 2015. [Online]. Available: <https://www.iec.ch/blog/understanding-iec-62443>. [Zugriff am 11 2024].
- [2] Cyber-Regulierung.de, „IEC 62443 – Cybersicherheit für die Industrie,“ 2015. [Online]. Available: <https://www.cyber-regulierung.de/normen-standards/iec-62443/>. [Zugriff am 11 2024].
- [3] ?, „?,“ [Online].
- [4] Microsoft, „Microsoft Update-Katalog,“ [Online]. Available: <https://www.catalog.update.microsoft.com/Home.aspx>. [Zugriff am 11 2024].
- [5] OASIS - CSAF.io, „Common Security Advisory Framework (CSAF),“ [Online]. Available: <https://csaf.io>. [Zugriff am 3 2025].
- [6] BSI, „Common Security Advisory Framework (CSAF) - Maschinenverarbeitbares Format ermöglicht automatisierten Datenbankabgleich,“ [Online]. Available: [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/CSAF/CSAF\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/CSAF/CSAF_node.html). [Zugriff am 3 2025].
- [7] BSI, „Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products - Part 2: Software Bill of Materials (SBOM) Version 2.0.0 (PDF),“ [Online]. Available: [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03183/BSI-TR-03183-2-2\\_0\\_0.pdf?\\_\\_blob=publicationFile&v=3](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03183/BSI-TR-03183-2-2_0_0.pdf?__blob=publicationFile&v=3). [Zugriff am 3 2025].
- [8] BSI, „Umgang mit "End of Support" in industriellen Steuerungs- und Automatisierungssystemen“,“ [Online]. Available: [https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS\\_145.pdf?\\_\\_blob=publicationFile&v=8](https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_145.pdf?__blob=publicationFile&v=8). [Zugriff am 11 2024].
- [9] BSI, „Technische Richtlinie BSI TR-03191 Common Security Advisory Framework (CSAF) (PDF),“ [Online]. Available: [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03191/BSI-TR-03191.pdf?\\_\\_blob=publicationFile&v=5](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03191/BSI-TR-03191.pdf?__blob=publicationFile&v=5). [Zugriff am 11 2024].
- [10] U.S. FOOD & DRUG Administration (FDA), „GUIDANCE DOCUMENT Part 11, Electronic Records; Electronic Signatures - Scope and Application,“ 09 2003. [Online]. Available: <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application>. [Zugriff am 11 2024].

- 
- [11] U.S. FOOD & DRUG Administration (FDA), „Download GUIDANCE DOCUMENT Part 11, Electronic Records; Electronic Signatures - Scope and Application,“ 09 2003. [Online]. Available: <https://www.fda.gov/media/75414/download>. [Zugriff am 11 2024].
- [12] FIRST.ORG, Inc., „Common Vulnerability Scoring System SIG (CVSS),“ [Online]. Available: <https://www.first.org/cvss/>. [Zugriff am 11 2024].
- [13] Cybersecurity & Infrastructure Security Agency, „Stakeholder-Specific Vulnerability Categorization (SSVC),“ [Online]. Available: <https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc>. [Zugriff am 11 2024].
- [14] Microsoft, „Microsoft Learning - Windows IoT,“ [Online]. Available: <https://learn.microsoft.com/en-us/windows/iot/iot-enterprise/customize/unified-write-filter>. [Zugriff am 11 2024].
- [15] BSI, „IT-Grundschutz-Kompendium (Edition 2023),“ [Online]. Available: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT\\_Grundschutz\\_Kompendium\\_Edition2023.pdf?\\_\\_blob=publicationFile&v=4](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4). [Zugriff am 2025].
- [16] SI | Sichere Industrie GmbH, „Purdue Reference Model: komplexe Automationsnetze klar strukturiert,“ [Online]. Available: <https://www.sichere-industrie.de/purdue-model/>. [Zugriff am 11 2024].
- [17] BSI, „Common Security Advisory Framework (CSAF),“ [Online]. Available: [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/CSAF/CSAF\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/CSAF/CSAF_node.html). [Zugriff am 11 2024].
- [18] ENISA, „Window of exposure... a real problem for SCADA systems?,“ [Online]. Available: [https://www.enisa.europa.eu/publications/window-of-exposure-a-real-problem-for-scada-systems/at\\_download/fullReport](https://www.enisa.europa.eu/publications/window-of-exposure-a-real-problem-for-scada-systems/at_download/fullReport). [Zugriff am 11 2024].
- [19] NAMUR, „Kurzfassung zu NE 153 „Automation Security Agenda 2020 – Design, Implementierung und Betrieb industrieller Automatisierungssysteme“,“ 11 6 2015. [Online]. Available: <https://www.namur.net/de/publikationen/news-archiv/die-ne-153-ist-neu-erschienen.html>. [Zugriff am 11 2024].
- [20] WIKIPEDIA, „Common Vulnerabilities and Exposures,“ 8 10 2024. [Online]. Available: [https://de.wikipedia.org/wiki/Common\\_Vulnerabilities\\_and\\_Exposures](https://de.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures). [Zugriff am 11 2024].