Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

NRL
Norddeutsches
RealLabor

Arbeitspapier im Rahmen des
Norddeutschen Reallabors

Sicherer Wartungsbetrieb durch Schwachstellen-Monitoring und Patch-Management

Joshua Stock, Tom Petersen, Hannes Federrath

Universität Hamburg

Fachbereich Informatik

Arbeitsbereich SVS

8. September 2025

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Zusammenfassung

Die digitale Transformation der Energieinfrastruktur macht Komponenten der Operational Technology (OT) anfällig für Cyberbedrohungen. Das Patchmanagement, also das regelmäßige und durchdachte Ausrollen von Softwareupdates, ist hierbei entscheidend, steht aber vor großen Herausforderungen durch lange Lebenszyklen und hohe Verfügbarkeitsanforderungen.

Dieses Arbeitspapier untersucht die Besonderheiten und Hürden des Patchmanagements in der Energie-OT. Anhand von Vorfällen wie TRITON, NotPetya und den Angriffen auf die Ukraine wird aufgezeigt, wie unzureichendes Patchmanagement zu schwerwiegenden Betriebsunterbrechungen führen kann. Zudem werden beispielhaft gängige OT-Komponenten in der Energiewirtschaft eingeführt. Die von den Herstellern bereitgestellten Schnittstellen für Sicherheitslücken und -updates werden untersucht, um darauf aufbauend eine Strategie für ein herstellerübergreifendes, automatisches Patchmanagement zu entwickeln. Ziel ist es, risikobasierte Strategien zu entwickeln, um die Resilienz kritischer Energieinfrastrukturen zu stärken und eine zuverlässige Versorgung zu sichern.

Transparenzhinweis: Teile dieses Arbeitspapiers wurden unterstützt durch den Einsatz von generativer künstlicher Intelligenz (Google Gemini Flash 2.5 mit Deep Research, sowie ChatGPT GPT-4o) geschrieben.

Über das Norddeutsche Reallabor

Das Projekt Norddeutsches Reallabor (NRL) ist ein innovatives Verbundprojekt, das neue Wege zur Klimaneutralität aufzeigt. Dazu werden Produktions- und Lebensbereiche mit besonders hohem Energieverbrauch schrittweise defossilisiert – insbesondere in der Industrie, aber auch in der Wärmeversorgung und dem Mobilitätssektor. Hinter dem im April 2021 gestarteten Projekt steht eine wachsende Energiewende-Allianz mit mehr als 50 Partnern aus Wirtschaft, Wissenschaft und Politik. Das Großprojekt hat eine Laufzeit von fünf Jahren (04/2021-03/2026). Dabei beträgt das Investitionsvolumen der beteiligten Partner rund 405 Mio. Euro. Als Teil der Förderinitiative „Reallabore der Energiewende“ wird das Projekt mit rund 55 Mio. Euro durch das Bundesministerium für Wirtschaft und Energie (BMWE) gefördert. Weitere Fördermittel werden durch das Bundesministerium für Digitales und Verkehr (BMDV) bereitgestellt. Das NRL versteht sich als ausbaufähige Plattform für weitere Projekte. www.norddeutsches-reallabor.de

Über den Arbeitsbereich Sicherheit in verteilten Systemen

Der Arbeitsbereich Sicherheit in verteilten Systemen (SVS) am Fachbereich Informatik der Universität Hamburg (UHH) unter der Leitung von Prof. Dr. Hannes Federrath verfügt über umfangreiche Erfahrungen in der Konstruktion sicherer und datenschutzgerechter Infomationstechnologie (IT)-Systeme. Die am Lehrstuhl vorhandene Kompetenz im Bereich Informationssicherheit deckt sowohl übergreifende Aspekte der IT-Sicherheit wie Sicherheitsmanagement und wirtschaftliche Aspekte der Informationssicherheit als auch Techniken der IT-Sicherheit ab. Einen Schwerpunkt bildet dabei Grundlagenforschung zu datenschutzfreundlichen Techniken und deren Einsatz in verschiedenen Anwendungskontexten.

Innerhalb des NRL-Projektes widmet sich SVS in Teilvorhaben 2.2 der Sicherheit von IT- und OT-Systemen im Rahmen der Sektorenkopplung.

Inhaltsverzeichnis

Einleitung

Die zunehmende Digitalisierung industrieller Steuerungssysteme hat die Betriebstechnologie bzw. Operational Technology (OT) in kritischen Infrastrukturen wie Energieerzeugungsanlagen erheblich verändert. OT steht im Gegensatz zu Infomationstechnologie (IT): IT bezeichnet Hardware und Software, die für die Speicherung, Übertragung und Verwendung von Informationen für Zwecke des Geschäftsbetriebs genutzt wird. OT hingegen beschreibt Hardware und Software, die mit Komponenten gekoppelt sind, die Veränderungen in der physikalischen Welt hervorrufen können, etwa für die Prozessautomatisierung [1, 2]. OT-Systeme wie Prozessleitsysteme (DCS/PLS), speicherprogrammierbare Steuerungen (SPS/PLC) und Anwendungen im Bereich der Supervisory Control and Data Acquisition (SCADA) sind heute nicht nur zentral für die Steuerung und Überwachung technischer Prozesse, sondern auch potenziellen Cyberbedrohungen ausgesetzt. Angesichts steigender Angriffszahlen und regulatorischer Anforderungen – etwa durch das IT-Sicherheitsgesetz oder die NIS-Richtlinie[1] – rückt das Sicherheitsmanagement dieser Systeme verstärkt in den Fokus.

Ein zentrales Element der Sicherheitsstrategie ist das Patchmanagement. Während in klassischen IT-Umgebungen regelmäßige Sicherheitsupdates zum Standard gehören, stellt das Patchen von OT-Komponenten eine erhebliche Herausforderung dar. Die spezifischen Betriebsbedingungen, lange Lebenszyklen, eingeschränkte Updatefähigkeit und die enge Kopplung an physikalische Prozesse erschweren eine direkte Übertragung bewährter IT-Ansätze. Zudem sind Herstellerfreigaben, Testzyklen und Wartungsfenster oft limitierende Faktoren, die das Einspielen sicherheitskritischer Patches verzögern oder sogar verhindern.

Dieses Arbeitspapier untersucht die besonderen Anforderungen und Hindernisse beim Patchmanagement in industriellen OT-Systemen am Beispiel von Energieinfrastrukturen. Es analysiert bestehende Verfahren, regulatorische Rahmenbedingungen sowie technische und organisatorische Einschränkungen. Ziel ist es, praxisnahe Empfehlungen zu formulieren, die sowohl die Betriebssicherheit als auch die IT-Sicherheit in einem hochverfügbaren Umfeld gewährleisten können.

[1] EU-Richtlinie zur Netzwerk- und Informationssicherheit

Kapitel 1

Hintergrund und Recherche

1.1 Probleme für das Patchmanagement im OT-Umfeld

Das Patchmanagement in industriellen OT-Systemen unterscheidet sich grundlegend von klassischen IT-Prozessen und ist durch eine Vielzahl technischer, organisatorischer und betriebskultureller Einschränkungen geprägt. Diese Besonderheiten resultieren primär aus dem Spannungsfeld zwischen Sicherheit, Verfügbarkeit und Integrität industrieller Prozesse.

Ein zentrales Merkmal ist die starke Herstellerabhängigkeit. Patches für DCS/PLS, SPS/PLC oder SCADA-Komponenten dürfen in vielen Fällen ausschließlich nach Freigabe des Herstellers und in abgestimmten Versionen installiert werden. Dies betrifft nicht nur die Steuerungssysteme selbst, sondern auch zugrundeliegende Betriebssysteme wie Windows oder Linux, deren Sicherheitsupdates potenziell zu Instabilitäten führen können, wenn sie nicht vollständig qualifiziert sind.

Hinzu kommt, dass die kontinuierliche Anlagenverfügbarkeit in OT-Umgebungen häufig die höchste Priorität hat. Sicherheitsupdates können meist nur in geplanten Wartungsfenstern oder Stillstandszeiten eingespielt werden – Zeiträume, die in Energieinfrastrukturen oft Monate auseinanderliegen. Dies führt zwangsläufig zu Verzögerungen bei der Schließung kritischer Sicherheitslücken und erhöht die Exponiertheit gegenüber Angriffen.

Ein weiteres Problem stellt die fehlende Standardisierung von Patchprozessen in OT-Netzwerken dar. Während IT-Systeme auf etablierte Werkzeuge und automatisierte Prozesse zurückgreifen können, erfolgt das Patchmanagement in der OT vielfach manuell und dokumentationspflichtig. Gleichzeitig fehlt es häufig an realitätsnahen Testumgebungen, in denen die Auswirkungen von Updates vorab geprüft werden können. Das Risiko unbeabsichtigter Systemstörungen bleibt damit ein entscheidendes Problem.

Schließlich sind viele OT-Systeme über Jahrzehnte hinweg gewachsen und basieren auf veralteten oder proprietären Technologien, für die keine Sicherheitsupdates mehr verfügbar sind. Die Identifikation, Bewertung und Priorisierung dieser Altlasten erfordert ein hohes Maß an technischem Verständnis, ein konsistentes Asset-Management und – nicht zuletzt – interdisziplinäre Zusammenarbeit zwischen IT, OT und Herstellern.

Diese strukturellen und betrieblichen Rahmenbedingungen machen deutlich, dass konventionelle IT-Sicherheitsansätze im OT-Kontext nicht ohne Weiteres übertragbar sind. Vielmehr bedarf es spezifischer Strategien, die sowohl technische Zwänge als auch betriebliche Anforderungen in Einklang bringen.

1.2 Beispielhafter Patchprozess in OT-Umgebungen

Ein strukturierter Patchprozess in industriellen OT-Umgebungen folgt einem risikoorientierten, mehrstufigen Vorgehen, das technische Machbarkeit, betriebliche Einschränkungen und regulatorische Vorgaben berücksichtigt. Nachfolgend wird ein exemplarischer Ablauf skizziert, wie er in der Energiebranche bei kritischen Systemen wie SCADA, SPS/PLC oder DCS/PLS typischerweise angewendet wird.

Sicherheitsmonitoring und Patch-Informationsbeschaffung Der Prozess beginnt mit der kontinuierlichen Überwachung von Sicherheitsquellen. Dazu zählen CERT-Meldungen, Herstellerportale (z.

B. Siemens CERT[1], Schneider Electric Security Notifications[2]), branchenspezifische Information Sharing and Analysis Centers (ISACs) sowie automatisierte Threat-Intelligence-Dienste. Relevante Schwachstellen und veröffentlichte Patches werden zentral erfasst, klassifiziert und priorisiert.

Risikoanalyse und Relevanzprüfung Für jede identifizierte Sicherheitslücke wird geprüft, ob betroffene Komponenten im eigenen OT-Bestand existieren. Dies setzt ein aktuelles Asset-Inventory voraus. In einer anschließenden Risikobewertung wird beurteilt, ob die Schwachstelle mit Blick auf Anlagenverfügbarkeit, Netzsegmente, Exposure und Kompensationsmaßnahmen kritisch ist.

Herstellerfreigabe und Testplanung Bei systemkritischen Komponenten ist ein Patch nur zulässig, wenn er vom Hersteller offiziell freigegeben wurde. Häufig stellen Hersteller spezialisierte Patchbundles bereit, die für bestimmte Systemversionen getestet sind. Vor der produktiven Umsetzung werden Patches idealerweise in einer referenznahen Testumgebung oder in digitalen Zwillingen validiert.

Wartungsplanung und Genehmigung Die Umsetzung erfolgt grundsätzlich nur im Rahmen geplanter Wartungsfenster. In kritischen Infrastrukturen wie Kraftwerken müssen betriebliche Stillstände, Freigaben durch Leitwarte, Instandhaltung und ggf. externe Partner abgestimmt werden. Der Patchvorgang wird über ein Change-Management-System dokumentiert und formell genehmigt.

Patchbereitstellung und Installation Die Verteilung erfolgt manuell oder teilautomatisiert über zentrale Managementsysteme. In vielen Fällen werden Patches physisch vor Ort durch speziell geschultes Personal installiert. Besondere Anforderungen bestehen bei Systemen ohne direkte Internetanbindung oder mit proprietären Updateverfahren.

Funktionsprüfung und Rückfallebene Nach der Installation wird die Funktionsfähigkeit der betroffenen Systeme geprüft. Dazu gehören Validierungstests, Kommunikationstests und ggf. Wiederanfahrprozesse. Für kritische Systeme wird vor dem Patch ein Rücksicherungspunkt oder vollständiges Backup angelegt, um bei Problemen einen Rollback zu ermöglichen.

Dokumentation und Nachverfolgung Der gesamte Patchprozess wird revisionssicher dokumentiert – einschließlich Risikobewertung, Freigaben, installierten Versionen, Prüfberichten und ggf. Abweichungen. Diese Dokumentation ist essenziell für interne Audits und regulatorische Prüfungen (z. B. nach IT-Sicherheitsgesetz, ISO 27001, IEC 62443).

1.3 Gängige OT-Komponenten in der Energieinfrastruktur

Die OT-Landschaft der Energieinfrastruktur ist vielfältig und umfasst eine Reihe spezialisierter Systeme und Geräte. Die hier dargestellten Komponenten sind exemplarisch und decken die wichtigsten Kategorien ab.

1.3.1 Kern-OT-Systeme und -Komponenten

Prozessleitsysteme (DCS/PLS)

- **Beschreibung:** Umfassende Systeme zur Überwachung und Steuerung komplexer, kontinuierlicher Prozesse, bei denen die Steuerungsintelligenz auf mehrere Controller verteilt ist. Sie sind das Gehirn von Großanlagen und gewährleisten die Koordination und Optimierung aller Prozessschritte.
- **Hersteller/Produkte:**
  - **Siemens:** SIMATIC PCS 7
  - **ABB:** ABB Ability™ System 800xA, Symphony Plus
  - **Honeywell:** Experion PKS [3]
  - **Emerson:** Ovation™ (speziell für Kraftwerke), DeltaV™
  - **Schneider Electric:** EcoStruxure Foxboro DCS/PLS
  - **Yokogawa:** CENTUM VP

[1] https://www.siemens.com/global/en/products/services/cert.html
[2] https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp

  - **Rockwell Automation:** PlantPAx
  - **GE:** Mark VIe (für Turbinensteuerung)
- **Einsatzbereich:** Kraftwerke (konventionell, nuklear, erneuerbar), große Umspannwerke, Fernwärmenetze, Prozessindustrien.
- **Patchmanagement & Security:** Updates werden über dedizierte Kundenportale nach intensiver Prüfung bereitgestellt. Hersteller betreiben Product Security Incident Response Teams (PSIRTs) und veröffentlichen Sicherheitshinweise und Hardening Guides. Das Patchen erfolgt geplant während Wartungsfenstern, um die Systemverfügbarkeit nicht zu gefährden. Emerson bietet z.B. einen Patch Management Service für DeltaV DCS/PLS an, der Betriebssystems-, Anti-Virus- und DeltaV-Hotfixes abdeckt.

Supervisory Control and Data Acquisition (SCADA)

- **Beschreibung:** Übergeordnete Systeme zur Fernüberwachung und -steuerung von industriellen Prozessen. Sie sammeln Daten von Fernwirkeinheitens (RTUs) und SPS/PLCs, visualisieren diese für Bediener und ermöglichen Steuerbefehle. Sie sind entscheidend für die zentrale Koordination verteilter Infrastrukturen.
- **Hersteller/Produkte:**
  - **Siemens:** SIMATIC WinCC Open Architecture (WinCC OA), SIMATIC WinCC [4]
  - **Schneider Electric:** EcoStruxure Geo SCADA Expert (ehemals ClearSCADA), Wonderware System Platform, EcoStruxure ADMS (Advanced Distribution Management System) [5]
  - **AVEVA:** AVEVA PI System (Historian und Dateninfrastruktur), AVEVA System Platform, AVEVA Plant SCADA, AVEVA Enterprise SCADA [6]
  - **Rockwell Automation:** FactoryTalk View SE, PlantPAx (DCS/PLS mit SCADA-Fähigkeiten)
  - **ABB:** ABB Ability™ System 800xA (DCS/PLS mit SCADA-Fähigkeiten), Symphony Plus SCADA [7]
  - **GE Digital/Vernova:** CIMPLICITY, iFIX [8]
  - **Honeywell:** Experion PKS (DCS/PLS/SCADA)
  - **Inductive Automation:** Ignition SCADA
- **Einsatzbereich:** Überwachung und Steuerung von Stromnetzen (Übertragung und Verteilung), Pipelines, Wasser- und Abwassernetzen, Gasversorgungsanlagen, Großflächige Anlagenüberwachung.
- **Patchmanagement & Security:** Da SCADA-Software oft auf Standard-Betriebssystemen (z.B. Windows) läuft, ist regelmäßiges Patchen von Betriebssystem und Applikation notwendig. Hersteller bieten Patches und Sicherheitsrichtlinien (Hardening Guides) an. Netzwerksegmentierung und Least Privilege sind entscheidende Schutzmaßnahmen. Inductive Automation pflegt z.B. ein Trust Center für Updates und Schwachstellen. AVEVA verfügt über eine Software Support Lifecycle and Retirement Policy.

Speicherprogrammierbare Steuerungen (SPS/PLC)

- **Beschreibung:** Robuste Industriecomputer, die zur Automatisierung spezifischer Maschinen oder Prozessabläufe eingesetzt werden. Sie empfangen Signale von Sensoren und senden Befehle an Aktoren.
- **Hersteller/Produkte:**
  - **Siemens:** SIMATIC S7-1500, S7-1200, S7-300, S7-400 [9]
  - **Rockwell Automation (Allen-Bradley):** ControlLogix, CompactLogix, MicroLogix [10]
  - **Schneider Electric:** Modicon (z.B. M580, M340, M241, M251, M258) [11]
  - **Mitsubishi Electric:** MELSEC iQ-R, MELSEC Q

  - **ABB:** AC500 Serie [12]
  - **Honeywell:** ControlEdge RTU, UOC (Universal IO Controller), PCD (Process Control Device) [13]
  - **Beckhoff Automation:** TwinCAT (PC-basierte Steuerung)
  - **Wago:** PFC-Controller
- **Einsatzbereich:** Dezentrale Automatisierungsaufgaben in Umspannwerken, Steuerung von Anlagen in erneuerbaren Energien (z.B. Windkraftanlagen), Maschinensteuerung, dezentrale Prozessautomatisierung.
- **Patchmanagement & Security:** Firmware-Updates sind über Hersteller-Support-Portale erhältlich (oft servicevertrag-gebunden). Security Advisories werden über PSIRTs veröffentlicht. Anwender müssen Patches vor der Implementierung validieren und testen. Moderne SPS/PLCs bieten Features wie Zugriffskontrolle, Secure Boot und verschlüsselte Kommunikation.

Fernwirkeinheiten (RTU)

- **Beschreibung:** Mikroprozessor-gesteuerte Geräte, die Daten von Sensoren in abgelegenen Standorten sammeln und an ein zentrales SCADA-System übermitteln, sowie Steuerbefehle vom SCADA-System empfangen und an Aktoren weiterleiten.
- **Hersteller/Produkte:**
  - **ABB:** RTU500 Serie
  - **Schneider Electric:** PowerLogic T300, SCADAPack
  - **Siemens:** SIMATIC RTU3000C, SICAM A8000 [14] (modulare RTU/Telecontrol-Plattform, oft in SIPROTEC-Geräten integriert)
  - **Honeywell:** ControlEdge RTU [13]
  - **GE Digital:** MDS Orca (Telemetrie-Funkgeräte für RTUs)
  - **SEL:** Oft in Schutzrelais integriert (z.B. SEL-351S mit RTU-Funktionalität)
  - **Red Lion Controls:** Industrielle RTUs
- **Einsatzbereich:** Datenerfassung und Steuerung in dezentralen Stationen des Verteilnetzes (z.B. Ortsnetzstationen, Gasdruckregelstationen), Monitoring von abgelegenen Anlagen, Anbindung von Feldgeräten an die Leitstelle.
- **Patchmanagement & Security:** Updates erfolgen manuell und geplant. Die Sicherheit hängt stark von der sicheren Konfiguration, physischem Schutz des Standorts und verschlüsselter Kommunikation zur Leitstelle ab. Hersteller stellen Firmware-Updates und Sicherheitshinweise zur Verfügung.

Mensch-Maschine-Schnittstellen (HMI)

- **Beschreibung:** Grafische Benutzeroberflächen, die es Bedienern ermöglichen, mit den OT-Systemen zu interagieren, Prozessdaten zu visualisieren und Steuerungen auszuführen. Sie können als Touchpanels, Industrie-PCs oder Software auf Workstations ausgeführt sein.
- **Hersteller/Produkte:**
  - **Siemens:** SIMATIC HMI Comfort Panels, Basic Panels, Unified System [15], WinCC Runtime
  - **Schneider Electric:** Harmony ST6, STO, STU, GTO, GTU, GTUX, GK, Magelis XBT GH [16]
  - **Rockwell Automation:** PanelView HMI [17]
  - **ABB:** CP600 Serie [18]
  - **Honeywell:** Experion Panel PC, HCiR, HMI-DN [19]
  - **Pro-face (Schneider Electric):** GP-Pro EX (HMI-Software)
  - **GE Digital:** iFIX (HMI/SCADA-Software)

- **Einsatzbereich:** Bedienstationen in Leitwarten, lokale Bedienpanels an Maschinen und Anlagen, Visualisierung komplexer Prozesse.
- **Patchmanagement & Security:** HMIs, insbesondere PC-basierte, erfordern regelmäßige OS- und Anwendungs-Patches. Hersteller bieten Security Advisories und Updates an (oft über Support-Portale). Physischer Zugangsschutz und Netzwerksegmentierung sind wichtige Sicherheitsmaßnahmen.

1.3.2 Spezifische Komponenten für die Energieinfrastruktur

Schutzrelais / Intelligent Electronic Devices (IEDs)

- **Beschreibung:** Mikroprozessor-basierte Geräte, die elektrische Anlagen vor Fehlern (z.B. Überstrom, Kurzschlüssen, Unterspannung) schützen, indem sie Schutzfunktionen ausführen und Leistungsschalter auslösen. Sie bieten auch Mess- und Kommunikationsfunktionen und sind oft gemäß IEC 61850 standardisiert.
- **Hersteller/Produkte:**
  - **SEL (Schweitzer Engineering Laboratories):** SEL-300, SEL-400, SEL-500, SEL-600, SEL-700, SEL-800 Serien, SEL-401 Merging Units [20]
  - **Siemens:** SIPROTEC 5 Serie (z.B. 7SJ80, 7KE85) [21]
  - **ABB:** Relion® Serie (z.B. REF615, RET670) [22]
  - **GE Grid Solutions:** Multilin Serie (z.B. L90, D60) [23]
  - **Hitachi Energy:** NUMERICS Protection Relays (ehemals ABB Power Grids)
- **Einsatzbereich:** Schutz von Hoch- und Mittelspannungsanlagen (Leitungen, Transformatoren, Generatoren, Sammelschienen) in Umspannwerken und Kraftwerken. Sie sind die Kernkomponente moderner, nach IEC 61850 standardisierter Umspannwerke.
- **Patchmanagement & Security:** Aufgrund ihrer kritischen Schutzfunktion werden Firmware-Updates extrem konservativ gehandhabt. Hersteller stellen Updates nach intensiven Tests zur Verfügung (z.B. über spezielle Kundenportale wie ABB's Relays-Online, das oft eine Seriennummern-Prüfung erfordert). Die Konfiguration ist passwortgeschützt, und die Kommunikation erfolgt zunehmend über sichere Protokolle. Hersteller wie SEL veröffentlichen monatliche E-Mail-Zusammenfassungen für Updates und stellen diese auf einer "Latest Software VersionsSeite bereit. Digitale Signaturen für Updates sind Standard.

Leistungsschalter und Schaltanlagen

- **Beschreibung:** Geräte zum Schalten und Schützen von Stromkreisen in Umspannwerken und Energieverteilungsnetzen. Schaltanlagen fassen diese Komponenten in einer physischen Einheit zusammen.
- **Hersteller/Produkte:**
  - **Siemens:** Gasisolierte Schaltanlagen (GIS), luftisolierte Schaltanlagen (AIS), Mittelspannungs-Leistungsschalter
  - **ABB:** Hochspannungs- und Mittelspannungs-Schaltanlagen und Leistungsschalter
  - **Schneider Electric:** Mittelspannungs-Schaltanlagen (z.B. Premset, GenieEvo)
  - **Eaton:** Eaton Power Xpert® FMX (Mittelspannungs-Schaltanlagen)
  - **GE Grid Solutions:** Hochspannungs-Gasisolierte Schaltanlagen (GIS), Leistungsschalter
- **Einsatzbereich:** Steuerung und Schutz von Stromkreisen auf allen Spannungsebenen in der Energieinfrastruktur.
- **Patchmanagement & Security:** Reine mechanische Schalter haben keine Software. Intelligente Leistungsschalter mit integrierten Steuer- und Überwachungsmodulen (oft IEDs) unterliegen den Patchmanagement-Richtlinien für IEDs. Die zugehörigen Betriebsmechanismen (federbetrieben,

motorbetrieben, hydraulisch-magnetisch) sind meist hardwarebasiert, aber die Steuerlogik ist in IEDs oder SPS/PLCs verankert.

Transformatoren (mit Überwachungssystemen)

- **Beschreibung:** Wandeln Spannungsniveaus um. Moderne Transformatoren sind oft mit intelligenten Überwachungssystemen (z.B. für Temperatur, Gas, Teilentladungen) ausgestattet, die OT-Schnittstellen bieten und Daten an Leitsysteme übertragen.
- **Hersteller/Produkte (Monitoring):**
  - **Siemens Energy:** Sensformer (digitale Transformatoren mit integrierter Sensorik)
  - **ABB:** TXpert™ (digitale Transformatorenlösungen)
  - **Weidmann Electrical Technology:** MONITRAN (Transformator-Überwachung)
- **Einsatzbereich:** Anpassung der Spannung in Übertragungs- und Verteilnetzen. Überwachungssysteme helfen bei der vorausschauenden Wartung und Fehlerdiagnose.
- **Patchmanagement & Security:** Die Überwachungssysteme können Firmware-Updates erhalten, die über die Herstellersupportkanäle bereitgestellt werden.

Sensoren und Aktoren

- **Beschreibung:** Die direkten Schnittstellen zur physikalischen Welt. Sensoren messen physikalische Größen (z.B. Spannung, Strom, Temperatur, Druck, Durchfluss), Aktoren wandeln Steuersignale in physikalische Aktionen um (z.B. Schalten von Leistungsschaltern, Regulieren von Ventilen).
- **Hersteller/Produkte (Auswahl):**
  - **Strom-/Spannungswandler:** ABB, Schneider Electric, Siemens, GE, Mitsubishi Electric, Hitachi Energy, Eaton, Magnelab, Triad Magnetics, Toshiba.
  - **Durchflusssensoren:** Siemens, ABB, Badger Meter, Sierra Instruments, Alicat Scientific, Flow Technology.
  - **Temperatur-/Drucksensoren:** Emerson Rosemount [24], Curtiss-Wright, Wika, Endress+Hauser.
  - **Leistungsschalter-Betriebsmechanismen:** ABB, Siemens, Schneider Electric, GE, Sensata Technologies, Carling Technologies, Square D (Typen: federbetrieben, motorbetrieben, hydraulisch-magnetisch).
- **Einsatzbereich:** Überall in der Energieinfrastruktur, wo physikalische Parameter gemessen oder Aktionen ausgelöst werden müssen.
- **Patchmanagement & Security:** Reine Hardware-Sensoren und einfache Aktoren haben keine direkt patchbare Software. Intelligente Sensoren oder Aktoren mit integrierter Elektronik (oft auch als IEDs kategorisiert) folgen den Patchmanagement-Praktiken ihrer Kategorie. Firmware-Updates sind seltener als bei Software, aber kritisch, wenn vorhanden.

Smart Metering Infrastructure (AMI)

- **Beschreibung:** Umfasst intelligente Stromzähler, Kommunikationsnetze und zentrale Datenmanagementsysteme zur automatisierten Erfassung von Verbrauchsdaten und zur Steuerung von Lasten. Teil der Smart Grid Entwicklung.
- **Hersteller/Produkte:** Landis+Gyr (Gridstream® AMI-Lösungen), Itron (OpenWay Riva™ AMI, Centron® Smart Meter), Kamstrup (OMNIA e-meter), Siemens (Smart Metering Solutions).
- **Einsatzbereich:** Verteilnetze zur detaillierten Verbrauchsmessung und Steuerung im Smart Grid, Lastmanagement.
- **Patchmanagement & Security:** Sicherheit ist hier extrem kritisch. Die Kommunikation wird Ende-zu-Ende verschlüsselt. Firmware-Updates können oft över-the-air"(OTA) eingespielt werden, erfordern aber sichere, signierte Pakete und ein robustes Rollen- und Rechtemanagement im zentralen System (Head-End System).

1.3.3 Kommunikationsinfrastruktur und Cybersicherheit

Industrielle Kommunikationsgeräte und Netzwerke

- **Beschreibung:** Industrielle Netzwerkkomponenten wie Switches, Router, Firewalls, Medienkonverter, die für die Kommunikation zwischen den verschiedenen OT-Geräten und -Systemen verwendet werden. Sie sind robust gebaut für raue Industrieumgebungen.
- **Hersteller/Produkte:**
  - **Siemens:** SCALANCE Industrielle Netzwerke
  - **Cisco:** Industrial Ethernet Switches (z.B. Catalyst IE3X00 Serie), Industrial Routers
  - **Moxa:** Industrielle Ethernet Switches, Media Converter
  - **Hirschmann (Belden):** Industrielle Switches und Router
- **Typische Protokolle:** Modbus (RTU, TCP/IP), DNP3, Profibus, EtherNet/IP, OPC UA, PROFINET, CAN bus, IO-Link, UMATI. Besonders wichtig ist IEC 61850 für die Kommunikation in Umspannwerken.
- **Einsatzbereich:** Aufbau von robusten und zuverlässigen Ethernet-Netzwerken in rauen Umgebungen wie Umspannwerken oder Produktionsanlagen. Sie unterstützen OT-Protokolle und Funktionen wie Redundanzverfahren (z.B. PRP/HSR).
- **Patchmanagement & Security:** Hersteller veröffentlichen regelmäßig Firmware-Updates zur Behebung von Sicherheitslücken. Wichtige Sicherheitsfunktionen sind Port-Security, VLANs zur Netzwerksegmentierung und RADIUS/TACACS+ zur Authentifizierung des administrativen Zugriffs. Updates werden typischerweise über Kundenportale bereitgestellt.

OT-Sicherheitslösungen (Spezialisierte Firewalls, Monitoring, IDS/IPS)

- **Beschreibung:** Spezialisierte Sicherheitslösungen, die für die Besonderheiten von OT-Netzwerken und -Protokollen ausgelegt sind, um Segmentierung, Anomalieerkennung, Bedrohungsanalyse und Incident Response zu ermöglichen.
- **Hersteller/Produkte:**
  - **Firewalls:** Fortinet (FortiGate Rugged), Palo Alto Networks, Siemens (SCALANCE S)
  - **OT-Netzwerk- und Bedrohungsanalyse:** Nozomi Networks (Guardian, Vantage, Central Management Console (CMC), Remote Collector, Guardian Air, Arc, Asset Intelligence, Threat Intelligence, Smart Polling), Dragos (Dragos Platform: Asset Discovery, Threat Detection, Vulnerability Management, Incident Response, Threat Intelligence Network), Claroty (xDome, Continuous Threat Detection (CTD), xDome Secure Access), Forescout (Forescout 4D Platform: Discover, Assess, Control, Govern; eyeSight, Assist for OT).
- **Einsatzbereich:** Segmentierung von IT- und OT-Netzwerken, Absicherung von Zonen innerhalb des OT-Netzwerks, Erkennung von Bedrohungen und Anomalien im OT-Verkehr (Deep Packet Inspection), Schwachstellenmanagement für OT-Geräte, Incident Response.
- **Patchmanagement & Security:** Als kritische Sicherheitskomponenten müssen diese Systeme stets aktuell gehalten werden. Hersteller bieten regelmäßige Signatur- und Softwareupdates an, oft über Subskriptionsmodelle. Ein zentrales Management ist entscheidend, um den Überblick über alle installierten Sicherheitslösungen zu behalten und deren Aktualität zu gewährleisten. Viele bieten dedizierte Security Portals und PSIRTs.

1.4 Analyse von Herstellerschnittstellen

Hersteller, die OT- (und IT-)Komponenten entwickeln, stellen in der Regel auch Informationen zu aktuellen Sicherheitslücken, sowie Firmware-Updates bereit. Beispielhaft sollen einige der Schnittstellen, über die Informationen dieser Art bereitgestellt werden, untersucht werden. Mit dem Ziel, die Schnittstellen mehrerer Hersteller in einer Übersicht zusammenzufassen, ist die automatische Abfrage und Auswertung von Informationen über die Schnittstellen ein Schwerpunkt in der folgenden Analyse.

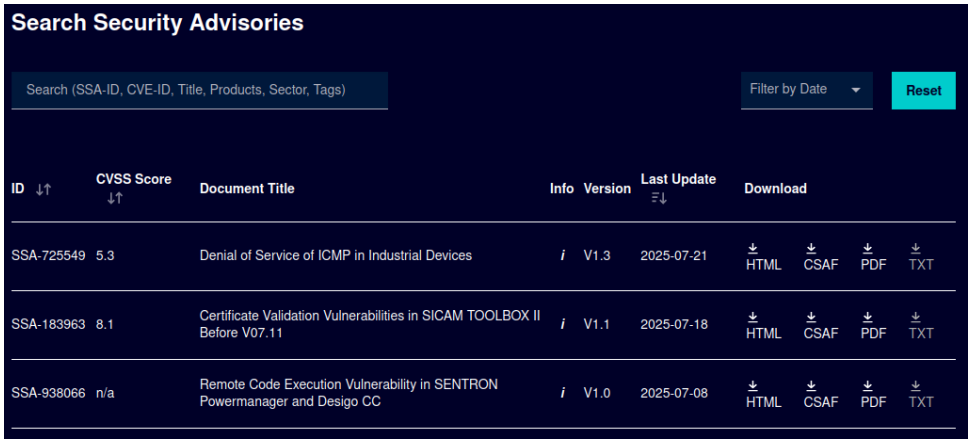

Abbildung 1.1: Übersicht aktueller Sicherheitslücken auf der Website *Siemens CERT* [25].

LAST UPDATED	TITLE	CVE	DESCRIPTION	PRODUCTS AND VERSIONS AFFECTED	PDF	CSAF
2025/07/08	EcoStruxure™ IT Data Center Expert	CVE-2025-6438 CVE-2025-50121 CVE-2025-50122 CVE-2025-50123 CVE-2025-50124 CVE-2025-50125	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') CWE-94: Improper Control of Generation of Code ('Code Injection') CWE-269: Improper Privilege Management CWE-331: Insufficient Entropy CWE-611: Improper Restriction of XML External Entity Reference CWE-918: Server-Side Request Forgery (SSRF)	EcoStruxure™ IT Data Center Expert Versions 8.3 and prior (Versions 8.3 and prior) (Formerly known as StruxureWare Data Center Expert)	SEVD-2025-189-01 PDF	SEVD-2025-189-01 CSAF
2025/07/08	System Monitor Application in Harmony and Pro-face PS5000		Schneider Electric is aware of a third-party vulnerability disclosed by GitHub	System Monitor application in Harmony Industrial PC HMIBMO/HMIBMI/ HMIPSO/	SEVD-2025-189-02 PDF	SEVD-2025-189-02 CSAF

Abbildung 1.2: Darstellung der *Security Notifications* auf der Website von Schneider Electric [26].

1.4.1 Siemens

Der Hersteller Siemens stellt Informationen zu Sicherheitslücken unter dem Namen *CERT Services*[25] zur Verfügung. Neben einer durchsuchbaren Tabelle auf der Website (siehe Abbildung 1.1) sind Details zu einzelnen Vorfällen in verschiedenen Formaten (HTML, PDF, TXT) anzeigbar. Außerdem sind die Informationen im Format Common Security Advisory Framework (CSAF) als maschinenlesbare JSON-Datei verfügbar. In den Details eines Vofalls sind stets alle betroffenen Produkte gelistet, sodass ein Filter für bestimmte Produkte, beispielsweise die verbauten Produkte im Werk eines Energielieferanten, problemlos möglich wären. Zu den betroffenen Produkten sind außerdem mögliche Lösungen des Problems gelistet, beispielsweise das Installieren bestimmter Firmware-Updates. Eine automatische Abfrage der Informationen an der Siemens CERT-Schnittstelle wird zudem über abonnierbare RSS- sowie CSAF-Feeds ermöglicht.

1.4.2 Schneider Electric

Schneider Electric stellen eine ähnliche Schnittstelle wie Siemens unter dem Namen *Security Notifications* zur Verfügung [26]. Auf einer Web Oberfläche werden aktuelle Benachrichtigungen als Tabelle angezeigt (siehe Abbildung 1.2). Die Informationen sind ebenfalls als PDF oder CSAF darstellbar. Ein RSS- oder CSAF-Feed wird nicht direkt angeboten, ein E-Mail Newsletter ist allerdings abbonierbar. Für die automatische Abfrage könnte ein Crawler zum Einsatz kommen, der die Tabelle auf der Website regelmäßig auf Neuigkeiten überprüft.

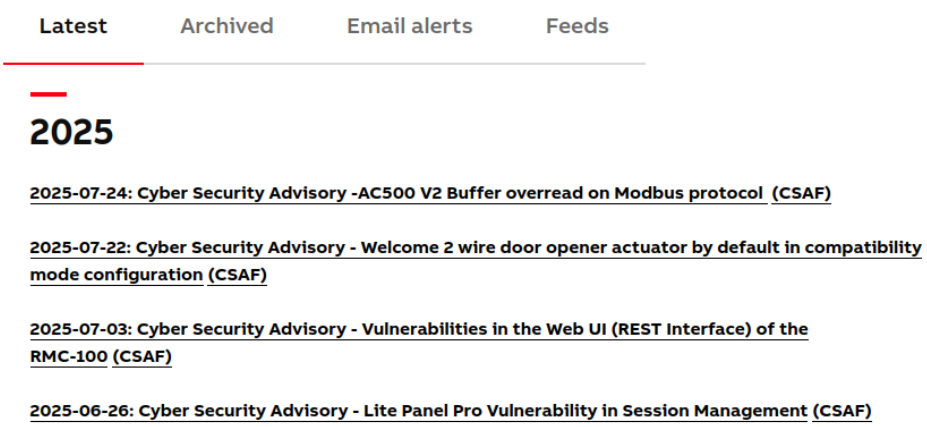

Abbildung 1.3: Darstellung der *Cyber security alerts and notifications* auf der Website von ABB [27].

1.4.3 ABB

Der Hersteller ABB betreibt eine Website mit *Cyber security alerts and notifications* [27]. Die Informationen werden im PDF- und CSAF-Format bereitgestellt und über eine Übersicht auf der Website dargestellt (siehe Abbildung 1.3). Es wird außerdem ein RSS-Feed zum Abonnieren angeboten. ABB stellt zudem für einzelne Produktgruppen Websites mit aktuellen Firmware-Patches zur Verfügung, bspw. für Relays [3].

1.4.4 Zusammenfassung der Schnittstellen

Die drei untersuchten Schnittstellen von Siemens [25], Schneider Electric [26] und ABB [27] stellen Informationen zu Sicherheitslücken übersichtlich und im maschinenlesbaren Industrie-Standard CSAF zur Verfügung. Bis auf Schneider Electric werden zudem RSS- bzw. CSAF-Feeds für den automatischen Empfang von neuen Informationen zur Verfügung gestellt. In Kombination mit einem Crawler für die Website von Schneider Electric könnten die Schnittstellen jedoch ohne Weiteres zu einem Pool zusammengefasst werden, was die automatische Bereitstellung von Informationen zu benötigten Patches ermöglichen würde.

1.5 Schwachstellen im Patchmanagement

Patchprozesse stellen in industriellen OT-Umgebungen nicht nur ein zentrales Mittel zur Härtung der Systemlandschaft dar, sondern können selbst Ziel gezielter Angriffe werden. Angreifer nutzen dabei spezifische Schwachstellen in der Update-Infrastruktur, im organisatorischen Ablauf oder im menschlichen Verhalten aus, um Schadsoftware einzuschleusen oder Systeme gezielt ungeschützt zu lassen. Im Folgenden werden zentrale Angriffsvektoren exemplarisch erläutert.

- **Supply-Chain-Angriffe auf Update-Quellen**: Ein besonders wirkungsvoller Angriffsvektor ist die Kompromittierung von Hersteller-Update-Servern oder Build-Umgebungen. Durch Manipulationen an der Quelle können Schadkomponenten mit offiziellen Updates verbreitet werden. Prominente Beispiele wie der SolarWinds-Vorfall (2020) zeigen die Tragweite solcher Supply-Chain-Angriffe. Im OT-Kontext stellt dies eine erhebliche Bedrohung dar, da viele Betreiber signierte Updates als vertrauenswürdig einstufen und ohne tiefgehende Prüfung einspielen.
- **Verbreitung gefälschter oder manipulierter Patches**: Angreifer können auch sogenannte *Rogue Updates* einsetzen – also gefälschte oder manipulierte Patches, die Schadcode enthalten. Diese werden entweder über Social Engineering, kompromittierte externe Datenträger oder durch Einschleusung in lokale Netzwerke verbreitet. Gerade in OT-Umgebungen, in denen Updates manuell und über nicht abgesicherte Wege (z. B. USB-Sticks) erfolgen, stellt dies ein realistisches Angriffsszenario dar.
- **Manipulation von Patchmanagement-Systemen**: Viele industrielle Betreiber nutzen zentrale Patchmanagement-Systeme oder Herstellerportale zur Verwaltung von Updates (z. B. Siemens Patch-

[3] https://relays.protection-control.abb/downloads/firmware-updates

Manager, Emerson Guardian). Ein erfolgreicher Angriff auf diese Systeme kann dazu führen, dass falsche Patchzustände angezeigt, sicherheitskritische Patches ausgelassen oder gezielt manipulierte Updates ausgerollt werden.

- **Ausnutzung von Wartungsfenstern und temporären Konfigurationen**: Während geplanter Wartungs- und Patchphasen werden häufig temporäre Ausnahmen in Firewalls, zusätzliche Fernwartungszugänge oder erhöhte Benutzerrechte aktiviert. Diese Zeitfenster bieten Angreifern eine Gelegenheit, sich lateral im Netzwerk zu bewegen, persistente Backdoors zu etablieren oder gezielt Angriffe auf ungepatchte Redundanzsysteme durchzuführen.
- **Schwachstellen im Patchprozess selbst**: Auch der eigentliche Update-Mechanismus kann Angriffspotenzial bieten. Schwachstellen in Hersteller-Tools, unzureichende Prüfung von digitalen Signaturen, unverschlüsselte Kommunikationskanäle oder lokale Privilegieneskalationen in Patch-Installationsroutinen sind dokumentierte Einfallstore, die gezielt ausgenutzt werden können.

Fehlendes oder unzureichendes Patchmanagement kann eine Ursache für erfolgreiche Cyberangriffe auf OT-Systeme sein. Die folgenden Vorfälle demonstrieren, wie Schwachstellen in der Aktualisierung von Software und Firmware ausgenutzt wurden, um kritische Infrastrukturen zu kompromittieren.

1.5.1 TRITON (TRISIS) Angriff auf eine Ölraffinerie (2017)

- **Angriffsausführung:** Cyberakteure (vermutlich staatlich gesponsert) erlangten Zugriff auf das industrielle Steuerungssystem einer Ölraffinerie. Sie setzten die Malware TRITON (auch bekannt als TRISIS) ein, die speziell entwickelt wurde, um die Schneider Electric Triconex Tricon Safety Instrumented System (SIS) Controller zu manipulieren. Die Malware interagierte direkt mit der Firmware der Sicherheitssysteme, um deren Funktionalität zu stören und eigene, bösartige Logik zu injizieren. Dies führte zu mehreren Notabschaltungen der Anlage.
- **Genutzte Schwachstellen im Patchmanagement:** Der Angriff nutzte spezifische, zum Zeitpunkt des Angriffs unbekannte (Zero-Day-)Schwachstellen in der Firmware der Triconex Tricon SIS-Controller (später identifiziert als CVE-2018-8872 und CVE-2018-7522). Schneider Electric stellte nach der Entdeckung Patches zur Verfügung, was darauf hindeutet, dass die betroffenen Systeme vor dem Angriff ungepatcht waren und die Schwachstellen aktiv ausgenutzt wurden, bevor eine Behebung verfügbar war oder angewendet werden konnte [28].
- **Konsequenzen:** Die Raffinerie musste für mehrere Tage den Betrieb einstellen. Das primäre Ziel der Angreifer war wahrscheinlich nicht nur die Unterbrechung des Betriebs, sondern die Verursachung physischer Schäden, indem die Sicherheitsmechanismen, die vor gefährlichen Betriebszuständen schützen sollen, ausgeschaltet wurden.
- **Betroffene OT-Komponenten/Hersteller:** Schneider Electric Triconex Tricon Safety Instrumented Systems (Modell 3008).

1.5.2 NotPetya (2017)

- **Angriffsausführung:** NotPetya war eine weitreichende Ransomware-Attacke, die sich über den Microsoft SMBv1-Exploit „EternalBlue“ verbreitete, der zuvor durch die NSA offengelegt worden war. Die initiale Infektion erfolgte oft über eine kompromittierte Software-Update-Mechanismus des ukrainischen Buchhaltungsprogramms M.E.Doc (Supply-Chain-Angriff). Einmal im Netzwerk, nutzte NotPetya EternalBlue, um sich schnell lateral auszubreiten, auch in IT-Netzwerke, die mit OT-Systemen verbunden waren.
- **Genutzte Schwachstellen im Patchmanagement:** Der Angriff hätte laut Experten weitgehend verhindert werden können, wenn Organisationen den Patch für EternalBlue, der von Microsoft bereits zwei Monate vor dem Angriff (im April 2017) veröffentlicht worden war, angewendet hätten. Millionen von Betriebssystemen waren zu diesem Zeitpunkt noch nicht aktualisiert und boten NotPetya somit eine weite Angriffsfläche. Dies ist ein klares Beispiel für das Ausnutzen von unzureichendem Patchmanagement auf der IT/OT-Schnittstelle oder in IT-Systemen, die für den OT-Betrieb unerlässlich sind [29].
- **Konsequenzen:** NotPetya verursachte geschätzte 10 Milliarden US-Dollar Schaden weltweit und legte wichtige Sektoren lahm, darunter auch Teile der Energieinfrastruktur. Viele Unternehmen muss-

ten den Betrieb vorübergehend einstellen, was zu massiven Produktionsausfällen und finanziellen Verlusten führte.

- **Betroffene OT-Komponenten/Hersteller:** Windows-basierte IT/OT-Systeme wie HMIs, Engineering-Workstations und Server, die mit den Energieinfrastrukturen verbunden waren und nicht rechtzeitig gepatcht wurden.

1.5.3 Dragonfly/Energetic Bear Kampagne (2012-2014)

- **Angriffsausführung:** Die Dragonfly-Kampagne zielte gezielt auf Unternehmen der Energiebranche ab. Eine der Hauptmethoden war ein Supply-Chain-Angriff, bei dem die Angreifer die Websites führender Hersteller von industriellen Steuerungssystemen kompromittierten und bösartige Software (Havex-Malware) in legitime Software-Updates einschleusten. Kunden, die diese infizierten Updates herunterluden, installierten unwissentlich Backdoors in ihren Systemen. Die Malware scannte dann die Netzwerke nach ICS/SCADA-Geräten.
- **Genutzte Schwachstellen im Patchmanagement:** Dieser Angriff nutzte nicht direkt eine ungepatchte Schwachstelle im herkömmlichen Sinne, sondern *die Vertrauenskette des Patchmanagements selbst*. Das bedeutet, Angreifer kaperten den Mechanismus, über den Systeme normalerweise sicher aktualisiert werden, um Malware einzuschleusen. Zudem verdeutlicht der Vorfall die Herausforderung, dass viele ältere OT-Systeme nicht ohne Weiteres gepatcht oder aktualisiert werden können, was langfristige Sicherheitslücken schafft [30].
- **Konsequenzen:** Über 17.000 Geräte in den USA waren infiziert. Obwohl keine direkten physischen Schäden oder Ausfälle berichtet wurden, verschafften sich die Angreifer langfristigen Zugang zu sensiblen Systemen der Energieinfrastruktur, was die potenzielle Fähigkeit zur Störung der Stromversorgung und anderer kritischer Dienste barg.
- **Betroffene OT-Komponenten/Hersteller:** Diverse ICS- und SCADA-Systeme von verschiedenen Herstellern, deren Software-Update-Mechanismen kompromittiert wurden oder deren Systeme aufgrund ihres Alters nicht aktualisierbar waren.

1.5.4 Angriff auf US-Stromnetzbetreiber (2019)

- **Angriffsausführung:** Bei diesem Vorfall wurde ein US-Stromnetzbetreiber für rund zehn Stunden von Cyberangreifern ins Visier genommen. Die Angreifer verursachten wiederholt das Rebooten von Firewalls im Netzwerk des Betreibers.
- **Genutzte Schwachstellen im Patchmanagement:** Der Vorfall wurde durch eine *bekannte und ungepatchte Schwachstelle in der Firmware der verwendeten Firewalls* ermöglicht. Der Netzbetreiber hatte es versäumt, die notwendigen Firmware-Updates auf die kompromittierten Firewalls anzuwenden. Dies wurde durch das Fehlen eines ordnungsgemäßen Prozesses zur Überprüfung und Implementierung von Sicherheitsupdates (Firmware Review Process) noch verschärft [30].
- **Konsequenzen:** Obwohl es zu keiner Unterbrechung der Stromversorgung kam, führten die wiederholten Neustarts der Firewalls zu einer zehnstündigen Störung des Netzwerkbetriebs und des Managements. Der Vorfall unterstrich die Notwendigkeit robuster Patchmanagement-Prozesse, auch für Netzwerkkomponenten in OT-Umgebungen.
- **Betroffene OT-Komponenten/Hersteller:** Firewalls (Hersteller nicht spezifisch genannt), die zur Segmentierung und Absicherung des OT-Netzwerks dienten.

1.5.5 Sandworm-Angriff auf ukrainische Energieinfrastruktur (2022)

- **Angriffsausführung:** Der Angriff der russischen Hackergruppe Sandworm (auch bekannt als UAC-0082) zielte auf die Energieinfrastruktur der Ukraine ab. Die Angreifer erlangten Zugang zur OT-Umgebung, wahrscheinlich über einen zuvor kompromittierten IT-Bereich. Sie nutzten einen Hypervisor, der eine SCADA-Management-Instanz hostete (MicroSCADA), und nutzten eine neuartige Technik, um über eine optische Disc (ISO)-Image ein natives MicroSCADA-Binary auszuführen. Dadurch konnten sie bösartige Steuerbefehle senden, um Umspannwerke abzuschalten. Parallel wurde in der IT-Umgebung die Wiper-Malware CADDYWIPER eingesetzt, um Beweise zu vernichten.

- **Genutzte Schwachstellen im Patchmanagement:** Ein kritischer Aspekt dieses Angriffs war die Ausnutzung einer *End-of-Life (EOL) MicroSCADA-Steuerungssystem-Installation* [31]. Systeme am Ende ihres Lebenszyklus erhalten keine Sicherheitsupdates oder Patches mehr, was sie zu einer erheblichen Schwachstelle macht. Das Versäumnis, auf unterstützte Systeme zu migrieren, stellte ein Versäumnis im Lebenszyklus-Management dar, das eng mit dem Patchmanagement verbunden ist.
- **Konsequenzen:** Der Angriff führte zu einem ungeplanten Stromausfall, der mit den parallelen Raketenangriffen Russlands auf die Ukraine zusammenfiel. Es demonstrierte die Fähigkeit der Angreifer, physische Auswirkungen in kritischer Infrastruktur zu erzielen.
- **Betroffene OT-Komponenten/Hersteller:** MicroSCADA Überwachungssystem (EOL-Version), Leistungsschalter für Schaltanlagen.

1.5.6 Weitere Vorfälle

Es gab weitere bedeutsame Angriffe auf die Energieinfrastruktur, bei denen Patchmanagement zwar eine Rolle im Kontext der allgemeinen Cybersicherheit spielte, die Hauptangriffsvektoren jedoch nicht direkt die Ausnutzung ungepatchter OT-Komponenten waren.

- **Angriffe auf das ukrainische Stromnetz 2015 und 2016:** Während diese Angriffe (BlackEnergy in 2015, Industroyer/CrashOverride in 2016) weitreichende Konsequenzen hatten und die OT-Welt aufrüttelten, konzentrierten sich die Berichte primär auf Social Engineering (Phishing), Fernzugriff auf ICS über legitime VPN-Zugänge, die Manipulation von Schaltgeräten und das Löschen von Systemdaten. Eine direkte, nachweisliche Ausnutzung spezifischer, ungepatchter OT-Software- oder Firmware-Schwachstellen als primärer Angriffsvektor wurde in den verfügbaren Analysen weniger explizit hervorgehoben als bei den oben genannten Beispielen. Die Angreifer nutzten hier oft legitimate Zugangsdaten und die Funktionalität der Systeme selbst aus.
- **Colonial Pipeline Ransomware-Angriff (2021):** Dieser Angriff führte zur vorsorglichen Abschaltung der Pipeline in den USA. Die initiale Kompromittierung erfolgte über ein kompromittiertes VPN-Passwort in einem IT-System, nicht über eine direkt ausgenutzte OT-Schwachstelle im Patchmanagement. Die Auswirkungen auf die OT waren eine Konsequenz der Abschaltung der IT-Systeme.

1.5.7 Zwischenfazit

Die Integrität des Patchprozesses ist essenziell für die Sicherheit von OT-Systemen. Angriffe auf diesen Prozess zielen nicht nur auf technische Schwachstellen, sondern auch auf organisatorische Lücken und menschliche Fehler ab. Daraus ergibt sich die Notwendigkeit, den Patchprozess selbst wie ein zu schützendes IT-System zu behandeln – mit Authentizitätsprüfungen, Zugriffsschutz, Monitoring und einem durchgängigen Vertrauensmodell. Sicherheitsmaßnahmen wie digitale Signaturen, kryptografisch gesicherte Verbindungen, eingeschränkte Wartungsmodi und kontrollierte Update-Infrastrukturen sind dabei unerlässlich.

1.6 Fazit

Die Operational Technology (OT) ist das Rückgrat der Energieinfrastruktur, und ihre Sicherheit ist von größter Bedeutung für die Funktionsfähigkeit kritischer Dienste. Die vorgestellte Liste gängiger OT-Komponenten zeigt die Vielfalt der eingesetzten Systeme, von SPS/PLCs und DCS/PLS bis hin zu spezialisierten Schutzrelais und intelligenten Messsystemen. Jeder dieser Bereiche erfordert spezifische Patchmanagement-Strategien, die die hohe Verfügbarkeitsanforderungen und die oft längeren Lebenszyklen der OT-Hardware berücksichtigen. Schnittstellen von Herstellern, die den aktuellen Stand über Sicherheitsvorfälle und -lücken darstellen, sind zudem weitestgehend automatisch und im Industriestandard CSAF abrufbar, sodass das Zusammenfassen von Informationen über mehrere Hersteller hinweg keine große technische Hürde darstellt.

Die beleuchteten Sicherheitsvorfälle, darunter TRITON, NotPetya, Dragonfly, der Angriff auf den US-Stromnetzbetreiber 2019 und der Sandworm-Angriff 2022 auf die Ukraine, machen die gravierenden Konsequenzen von Schwachstellen im Patchmanagement deutlich. Ob durch das Versäumnis, bekannte Patches zeitnah anzuwenden, durch die Ausnutzung von EOL-Systemen oder durch Supply-Chain-Angriffe,

die die Update-Mechanismen selbst kompromittieren – unzureichendes Patchmanagement kann zu Betriebsunterbrechungen, physischen Schäden und weitreichenden finanziellen Verlusten führen.

Ein effektives Patchmanagement in der OT erfordert nicht nur technische Prozesse zur Bereitstellung und Installation von Updates, sondern auch eine strategische Planung, Risikobewertung, gründliche Testphasen und ein kontinuierliches Schwachstellenmanagement. Angesichts der evolutionären Bedrohungslandschaft ist dies unerlässlich, um die Resilienz der Energieinfrastruktur gegen Cyberangriffe zu stärken und die zuverlässige Energieversorgung sicherzustellen.

Kapitel 2

Konzept für das Patch-Management

Das vorliegende Kapitel beschreibt ein strukturiertes Patch-Managementkonzept für den sicheren und ausfallsicheren Betrieb von OT-Komponenten in kritischen Energieinfrastrukturen. Ziel ist es, sicherheitsrelevante Software- und Firmware-Updates effektiv zu verwalten, vorhandene Schwachstellen zu minimieren und gleichzeitig die hohen Anforderungen an Verfügbarkeit, Integrität und Stabilität der Systeme zu erfüllen.

Im Unterschied zu klassischen IT-Umgebungen erfordert das Patch-Management im OT-Kontext besondere technische und organisatorische Maßnahmen. Begrenzte Wartungsfenster, Echtzeitanforderungen, heterogene Systemlandschaften sowie herstellerspezifische Abhängigkeiten stellen besondere Herausforderungen dar. Daher bedarf es klar definierter Prozesse, risikobasierter Entscheidungen und einer engen Koordination aller beteiligten Akteure.

Das Kapitel gliedert sich in einzelne Abschnitte:

- Abschnitt 2.1 führt kurz in Anforderungen aus existierenden Regularien ein.
- In Abschnitt 2.2 wird eine Übersicht über den vorgesehenen Patch-Prozess geliefert.
- Die nachfolgenden Abschnitte gehen auf einzelne Details dieses Prozesses ein.
- Abschnitt 2.3 beschreibt Ansätze für die Reduzierung von Ausfallszeiten durch eine geeignete Roll-Out-Strategie.
- In Abschnitt 2.4 wird detaillierter auf die notwendige Verfifikation von Patches eingegangen.
- Zuletzt stellt Abschnitt 2.5 ergänzende Sicherheitsmaßnahmen zur Absicherung des Patch-Prozesses dar.

2.1 Regulatorische Anforderungen

Die Umsetzung eines strukturierten und risikobasierten Patch-Managements in OT-Umgebungen kritischer Infrastrukturen erfolgt nicht nur aus betrieblichen Erwägungen heraus, sondern ist zunehmend auch gesetzlich und regulatorisch vorgeschrieben. Die folgenden Regelwerke und Normen sind in diesem Zusammenhang besonders relevant:

IT-Sicherheitsgesetz (IT-SiG 2.0) Das IT-Sicherheitsgesetz verpflichtet Betreiber Kritischer Infrastrukturen (KRITIS) zur Umsetzung angemessener technischer und organisatorischer Maßnahmen zum Schutz ihrer Systeme. Gemäß § 8a BSIG müssen diese Maßnahmen dem Stand der Technik entsprechen. Dazu gehört ausdrücklich auch ein strukturiertes Patch- und Schwachstellenmanagement, das Sicherheitsupdates zeitnah bewertet, priorisiert und umsetzt. Zudem sind Nachweise über die getroffenen Maßnahmen auf Anfrage der zuständigen Aufsichtsbehörde (BSI) vorzulegen.

NIS-2-Richtlinie (EU 2022/2555) Die NIS-2-Richtlinie verpflichtet Betreiber wesentlicher Einrichtungen innerhalb der EU zur Einführung und Aufrechterhaltung eines Sicherheitskonzepts für Netz- und Informationssysteme. Darin ist die Pflicht zur Risikobewertung und zum Patch-Management

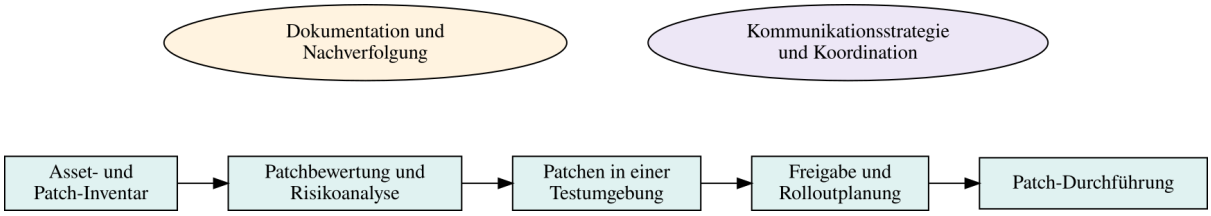

Abbildung 2.1: Übersicht über den Patchprozess

ausdrücklich verankert. So fordert Artikel 21 Absatz 2 (d) etwa die Umsetzung von „Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen“. Die NIS-2-Richtlinie ist Stand heute noch nicht in nationales Recht umgesetzt.

ISO/IEC 27001 und ISO/IEC 27019 Die international anerkannten Normen der ISO/IEC 27000-Reihe definieren Anforderungen an ein Informationssicherheits-Managementsystem (ISMS). In ISO/IEC 27001 wird im Anhang A Abschnitt A.12 gefordert, dass Schwachstellen im System regelmäßig identifiziert, bewertet und behoben werden. Die branchenspezifische Norm ISO/IEC 27019 für den Energiesektor konkretisiert dies um Anforderungen an Energieerzeugungs- und Verteilungsanlagen und empfiehlt insbesondere regelmäßige Updates sicherheitsrelevanter Komponenten.

BSI IT-Grundschutz Der BSI IT-Grundschutz formuliert in dem Bausteinen OPS.1.1.3 (Patch- und Änderungsmanagement) konkrete Umsetzungsempfehlungen für ein systematisches Patch-Management, einschließlich Rollenverteilung, Dokumentation und Testverfahren.

Aus den genannten Regelwerken können für das Patch-Management unter anderem folgende Anforderungen abgeleitet werden:

- **Inventarisierung:** Vollständige Erfassung aller patchfähigen Systeme und deren Softwarestände
- **Bewertung:** Risikobasierte Einschätzung der Relevanz und Kritikalität jedes Updates
- **Testprozesse:** Nachweisbare Prüfung der Update-Wirkung in geeigneten Testumgebungen
- **Rolloutplanung:** Zeitlich abgestimmte Umsetzung mit Rückfallstrategien
- **Dokumentation:** Lückenlose Erfassung der Durchführung, Bewertung und Entscheidungsprozesse
- **Nachweisführung:** Bereitstellung von Reports und Nachweisen für Behörden oder Audits
- **Verantwortlichkeiten:** Eindeutige Zuordnung von Rollen und Zuständigkeiten innerhalb der Organisation

Diese Anforderungen werden in unserem Konzept für ein sicheres Patch-Management, das im restlichen Kapitel beschrieben wird, umgesetzt. Ein robustes Patch-Management ist somit nicht nur für einen sicheren Betrieb notwendig, sondern ist auch ein zentraler Bestandteil in der Erfüllung regulatorischer Anforderungen.

2.2 Übersicht: Patch-Management-Prozess im OT-Kontext

Ein strukturierter Patch-Management-Prozess ist die Grundlage für ein sicheres und zuverlässiges Aktualisieren von OT-Komponenten in kritischen Infrastrukturen. Die folgenden Schritte beschreiben die notwendigen Aktivitäten dieses Prozesses in Energieinfrastrukturen. Eine Übersicht ist in Abbildung 2.1 zu finden.

2.2.1 Asset- und Patch-Inventar

Im ersten Schritt des Patch-Management-Prozesses ist eine vollständige und aktuelle Inventarisierung aller relevanten OT-Komponenten (siehe Abschnitt 1.3) erforderlich. Zu jeder Komponente sind die aktuell eingesetzten Software- und Firmwarestände, Herstellerinformationen und eindeutige Identifikatoren (z. B. Seriennummern, IP-Adressen) zu dokumentieren.

Parallel dazu muss ein Mechanismus zur kontinuierlichen Erfassung verfügbarer Patches etabliert werden. Dies kann beispielsweise durch die automatisierte Abfrage von Herstellerdatenbanken (siehe Abschnitt 1.4), die Beobachtung von CVE-Datenbanken oder durch direkte Lieferantenkommunikation erfolgen. Die Aktualität dieses Inventars ist entscheidend, um bekannte Schwachstellen zeitnah adressieren zu können.

2.2.2 Patchbewertung und Risikoanalyse

Nicht jeder verfügbare Patch ist für die jeweilige OT-Umgebung unmittelbar relevant oder gefahrlos einspielbar. Daher ist für jedes Update eine strukturierte Bewertung erforderlich. Dabei sind sowohl sicherheitsrelevante Aspekte (z. B. CVSS-Score, Angriffsvektor, Ausnutzbarkeit) als auch betriebskritische Auswirkungen (z. B. notwendige Systemneustarts, Kompatibilität mit anderen Komponenten) zu berücksichtigen.

Ein multidisziplinäres Team bestehend aus IT-Security, OT-Betrieb und ggf. externen Fachleuten bewertet den Patch hinsichtlich seines Risikopotenzials und entscheidet über die Aufnahme in die Rollout-Planung. Je nach Kritikalität der betroffenen Systeme und des Patches kann auch eine tiefergehende Bedrohungs- und Schwachstellenanalyse (z. B. mit einem Risikoanalysemodell) notwendig sein.

2.2.3 Patchen in einer Testumgebung

Um ungewollte Störungen in der Produktivumgebung zu vermeiden, ist das Einspielen und Testen von Patches in einer dedizierten Testumgebung zwingend erforderlich. Diese sollte den produktiven OT-Systemen in Architektur, Konfiguration und Netzwerktopologie möglichst exakt entsprechen. Alternativ kann ein sogenannter digitaler Zwilling eingesetzt werden, der eine simulationsbasierte Bewertung ermöglicht.

In der Testumgebung werden der Patch und alle damit verbundenen Abläufe (z. B. Neustarts, Konfigurationsänderungen) realitätsnah erprobt. Zudem sind Regressionstests durchzuführen, um sicherzustellen, dass bestehende Funktionalitäten nach dem Update weiterhin stabil laufen. Die Ergebnisse dieser Tests bilden die Grundlage für die Entscheidung, ob ein Rollout in der produktiven Umgebung erfolgen kann.

2.2.4 Freigabe und Rolloutplanung

Nach erfolgreich bestandenen Tests ist eine formale Freigabe durch das zuständige Gremium (z. B. Change-Advisory-Board, OT-Sicherheitsverantwortlicher, Fachabteilung) einzuholen. Daraufhin wird eine Rolloutstrategie erstellt, die den spezifischen Anforderungen der Energieinfrastruktur gerecht wird. Dabei sind Aspekte wie Systemverfügbarkeit, Netzlast, Personalverfügbarkeit und Betriebszeitfenster zu berücksichtigen. Details werden in Abschnitt 2.3 behandelt.

2.2.5 Patch-Durchführung

Die Durchführung von Patches in OT-Umgebungen erfolgt abhängig von Systemtyp, Netzwerkanbindung und Sicherheitsanforderungen auf unterschiedlichen Wegen. Grundsätzlich lassen sich drei Hauptvarianten unterscheiden:

- **Remote-Update:** Bei netzseitig angebundenen Systemen kann der Patch zentral über gesicherte Wartungskanäle (z. B. VPN, Management-Netz, Fernwartungszugang) eingespielt werden. Dies erfordert stabile Kommunikationswege und geeignete Authentifizierungsmechanismen.
- **Manuelles Vor-Ort-Update:** In isolierten oder besonders sicherheitskritischen Anlagen erfolgt die Aktualisierung oft lokal durch autorisiertes Personal. Patches werden dabei z. B. per USB-Stick oder Service-Laptop übertragen. Diese Variante ist ressourcenintensiv, aber in Air-Gap-Szenarien notwendig.
- **Update über Engineering-Tools oder HMI:** Einige Systeme erlauben das Einspielen von Firmware oder Konfigurationsupdates direkt über herstellerspezifische Softwarelösungen oder lokale Bedienoberflächen. Auch hier sind Authentizität und Integrität des Updates sicherzustellen.

Die Auswahl der geeigneten Methode erfolgt auf Basis der Kritikalität, Systemarchitektur und betrieblichen Rahmenbedingungen. Unabhängig vom Verfahren ist eine vorherige Datensicherung sowie eine dokumentierte Durchführung mit eventuellen Rollback-Optionen obligatorisch.

2.2.6 Dokumentation und Nachverfolgung

Eine lückenlose und nachvollziehbare Dokumentation ist essenzieller Bestandteil eines wirksamen Patch-Managements in OT-Umgebungen. Sie dient sowohl der internen Nachvollziehbarkeit als auch dem Nachweis gegenüber Aufsichtsbehörden, Prüfern oder im Rahmen von Sicherheitsvorfällen.

In einem vorgelagerten Schritt muss der Patch-Management-Prozess durch verbindliche Betriebsanweisungen, Sicherheitsrichtlinien oder Handlungsleitfäden geregelt werden. Diese sollten u. a. Kriterien für die Risikobewertung, Freigabeprozesse und Eskalationswege definieren. Die nachfolgenden Aspekte sind während des Prozesses zu beachten.

Für jede gepatchte Komponente ist eine Patch-Historie zu führen, die unter anderem den Zeitpunkt des Updates, Versionsinformationen, Freigaben, durchführende Personen sowie Besonderheiten bei der Umsetzung enthält. Ebenso sind die Ergebnisse von Tests (z. B. in Testumgebungen oder Pilotanlagen) zu dokumentieren, um die Eignung und Stabilität des Updates nachweisen zu können.

Alle Entscheidungen zur Durchführung oder auch zum bewussten Verzicht auf bestimmte Patches müssen nachvollziehbar begründet und archiviert werden. Dies betrifft insbesondere kritische Systeme, bei denen etwa aus Kompatibilitäts- oder Verfügbarkeitsgründen keine kurzfristige Aktualisierung möglich ist.

Darüber hinaus sind strukturierte Freigabeprozesse, Protokolle und Rollback-Dokumentationen Bestandteil der Gesamtaufzeichnung. Die regelmäßige Pflege dieser Informationen erlaubt eine konsistente Übersicht über den Patch-Status der gesamten Infrastruktur und ermöglicht automatisierte Auswertungen (z. B. Patch-Quote, Reaktionszeit auf Schwachstellen).

Ein dokumentierter Patch-Prozess ist damit nicht nur Teil eines sicheren Betriebs, sondern auch Voraussetzung für die Erfüllung regulatorischer Anforderungen gemäß IT-Sicherheitsgesetz, NIS2 oder ISO/IEC 27001.

2.2.7 Kommunikationsstrategie und Koordination

Ein reibungsloser Patch-Rollout in OT-Umgebungen setzt eine sorgfältig abgestimmte Kommunikations- und Koordinationsstrategie voraus. Alle beteiligten Parteien, insbesondere IT-Sicherheit, OT-Betrieb, Fachabteilungen und gegebenenfalls externe Dienstleister, müssen frühzeitig eingebunden werden. Zuständigkeiten, Eskalationspfade und Kommunikationswege sind klar zu definieren.

Wartungsfenster sollten so gewählt werden, dass kritische Betriebsphasen (z. B. Lastspitzen, Schaltvorgänge im Netzbetrieb) nicht beeinträchtigt werden. Ebenso ist eine rechtzeitige Information aller betroffenen Betriebsstellen sicherzustellen, um auf mögliche Einschränkungen vorbereitet zu sein. Bei besonders sicherheitskritischen oder hochverfügbaren Systemen kann eine erweiterte Freigabestufe mit zusätzlicher Absicherung erforderlich sein.

Die Koordination mit dem Herstellersupport oder spezialisierten Dienstleistern ist ebenfalls ein zentraler Bestandteil, insbesondere bei komplexen oder herstellerspezifischen Patchvorgängen.

2.3 Reduzierung von Ausfallzeiten durch Roll-Out-Strategie

Ein bewährtes Vorgehen besteht im gestaffelten Ausrollen der Patches in mehreren Stufen (Pilot, Teilbereich, Gesamtsystem), ggf. unter Nutzung redundanter Betriebsführungen zur Reduktion von Ausfallzeiten. Jeder Rolloutschritt ist zu dokumentieren, zu überwachen und mit einem definierten Rollback-Mechanismus zu versehen, um bei Problemen eine schnelle Wiederherstellung des vorherigen Zustands zu ermöglichen.

2.3.1 Gestaffelter Roll-Out

Um die Stabilität des Gesamtsystems zu gewährleisten und das Risiko unbeabsichtigter Betriebsstörungen zu minimieren, sollte das Einspielen von Patches in OT-Umgebungen stets gestaffelt und kontrolliert

erfolgen. Dieses sogenannte “Staged Rollout”-Verfahren erlaubt es, neue Updates zunächst in isolierten oder weniger kritischen Teilbereichen zu testen, bevor sie flächendeckend in der Produktionsumgebung implementiert werden.

Das gestaffelte Ausrollen gliedert sich in der Regel in drei Phasen:

1. **Pilotphase:** Zunächst wird das Update auf einer einzelnen, repräsentativen Komponente oder einem Testsystem eingespielt. Das Verhalten wird unter realistischen Bedingungen beobachtet und dokumentiert.
2. **Teilweise Ausbringung:** Nach erfolgreichem Test erfolgt das Patchen in einem ausgewählten Teilsegment der Infrastruktur, beispielsweise in einem nicht kritischen Versorgungsbereich. Auch hier findet eine engmaschige Überwachung statt.
3. **Vollständiger Rollout:** Erst nach Freigabe und stabiler Laufzeit im Testsegment erfolgt das Ausrollen auf alle übrigen relevanten Systeme.

Während jeder Phase ist ein definierter Rollback-Mechanismus vorzuhalten, der eine zügige Wiederherstellung des vorherigen Systemzustands bei Problemen ermöglicht. Das gestaffelte Vorgehen reduziert das Risiko eines systemweiten Ausfalls erheblich und erleichtert die Ursachenanalyse bei etwaigen Fehlern.

2.3.2 Redundante Betriebsführung und Failover-Konzepte

In hochverfügbaren OT-Umgebungen, insbesondere innerhalb von Energieinfrastrukturen, ist der kontinuierliche Betrieb essenziell. Daher muss das Patch-Managementkonzept mit redundanten Betriebsführungs- und Failover-Mechanismen kombiniert werden, um auch während Wartungsarbeiten oder unerwarteter Störungen die Systemverfügbarkeit sicherzustellen.

Ein bewährtes Verfahren ist der Einsatz von redundanten Systemen im Hot-Standby- oder Active/Passive-Betrieb. Dabei wird zunächst das Sekundärsystem (Standby) aktualisiert und intensiv getestet. Nach erfolgreicher Validierung wird der Betrieb auf das gepatchte System umgeschaltet. Erst dann wird das Primärsystem ebenfalls aktualisiert. Diese Umschaltstrategie erlaubt ein risikofreies Patching im laufenden Betrieb.

Bei virtualisierten oder containerisierten OT-Komponenten kann ein Rolling-Update-Verfahren angewendet werden. Dabei werden einzelne Knoten innerhalb eines Clusters nacheinander aktualisiert, während die übrigen weiterhin produktiv arbeiten. So lassen sich selbst größere Umgebungen ohne nennenswerte Ausfallzeiten aktualisieren.

Zusätzlich empfiehlt sich eine regelmäßige Überprüfung der Failover-Funktionalitäten im Rahmen von Wartungs- oder Testfenstern. Nur so kann sichergestellt werden, dass die Redundanzmechanismen im Ernstfall wie vorgesehen greifen.

2.4 Verifikation von Patches

Ein zentraler Sicherheitsaspekt beim Patch-Management in OT-Umgebungen ist die Verifikation der Integrität und Authentizität von Software- und Firmware-Updates. Ohne eine solche Prüfung besteht das Risiko, dass manipulierte oder gefälschte Patches (siehe Abschnitt 1.5) in Produktivsysteme eingebracht werden, was gravierende Auswirkungen auf Verfügbarkeit, Steuerungsfunktionen und Sicherheit haben kann. Daher ist die technische Verifikation von Patches ein unverzichtbarer Bestandteil eines sicheren Update-Prozesses.

2.4.1 Digitale Signaturprüfung

Die gängigste Methode zur Verifikation von Patches ist die Verwendung digitaler Signaturen. Hierbei signiert der Hersteller das Update mit einem privaten kryptografischen Schlüssel. Auf der Empfängerseite – also im OT-System, in der Testumgebung oder auf dem Update-Server – wird die Signatur mithilfe des entsprechenden öffentlichen Schlüssels überprüft. Nur wenn die Signatur gültig ist und mit dem Patchinhalt übereinstimmt, wird das Update akzeptiert.

Die Prüfung kann an unterschiedlichen Stellen im Prozess erfolgen:

- **Bereits beim Herunterladen des Patches**, z. B. durch ein zentrales Update-Management-System.
- **Vor dem Einspielen in Testumgebungen**, um nur gültige Dateien zu testen.
- **Direkt auf der Zielkomponente**, sofern diese über die notwendigen Prüfmechanismen verfügt.

Im besten Fall erfolgt die Überprüfung auf der Zielkomponente, um sicherzustellen, dass der letztendlich installierte Patch direkt vom Hersteller stammt und nicht verändert wurde. Ist dies nicht möglich, so muss sichergestellt werden, dass nach Prüfung der Signatur eine Manipulation des Patches (etwa durch Innentäter) bestmöglich ausgeschlossen werden kann.

2.4.2 Herkunft und Verwaltung kryptografischer Schlüssel

Die zur Verifikation verwendeten öffentlichen Schlüssel werden üblicherweise durch den Hersteller oder Herausgeber des Patches bereitgestellt, entweder eingebettet in das Gerät (z. B. in Firmware oder TPM-Modul), als Teil einer Zertifikatskette oder über eine abgesicherte Verteilplattform.

Um die Vertrauenswürdigkeit der Signaturprüfung zu gewährleisten, müssen folgende Anforderungen erfüllt sein:

- Die öffentlichen Schlüssel müssen aus einer sicheren Quelle stammen und vor unbefugtem Austausch geschützt werden (z. B. durch Hash-Werte oder Eintrag in eine Trust-Store-Datei).
- Die Schlüssel müssen regelmäßig auf Gültigkeit überprüft und bei Ablauf oder Kompromittierung ersetzt werden können (Key Rollover).
- Eine Versionskontrolle oder Seriennummerierung hilft dabei, gezielt gegen die Verwendung kompromittierter Schlüssel vorzugehen.

2.4.3 Key-Rollover und Schlüsselrotation

Ein *Key-Rollover*, der planmäßige oder außerplanmäßige Austausch kryptografischer Schlüssel, ist ein kritischer Moment in der Sicherheitsarchitektur. Er kann z. B. notwendig werden durch

- Ablauf eines Schlüssels oder Zertifikats,
- Einführung neuer Hash- oder Signaturalgorithmen oder
- Kompromittierung des Schlüssels (z. B. durch einen Sicherheitsvorfall beim Hersteller).

Der Rollover-Prozess muss so gestaltet sein, dass grundsätzlich sowohl alte als auch neue Signaturen vorübergehend parallel überprüfbar sind, aber bei Schlüsselkompromittierung sichergestellt werden kann, dass diese Schlüssel nicht mehr verwendet werden. Dazu ist ein Mechanismus erforderlich, der mehrere gültige öffentliche Schlüssel unterstützt und die Versionsverwaltung der Schlüssel sicherstellt. Besondere Vorsicht ist bei Offline-Systemen geboten, da veraltete Schlüssel ohne manuelle Aktualisierung zu verweigerter Patch-Verarbeitung führen können.

Kryptoagilität als Voraussetzung für langfristige Verifikation

Ein zukunftssicheres Patch-Verifikationskonzept für potentiell langlebige OT-Komponenten muss flexibel bezüglich der kryptographischen Verfahren sein – also in der Lage, diese Verfahren flexibel auszutauschen, ohne grundlegende Systemänderungen zu erfordern. Angesichts des fortschreitenden Wissens über Schwächen bestehender Algorithmen (z. B. SHA-1, RSA mit geringer Schlüssellänge) sowie möglicher Entwicklungen im Bereich der Quantenkryptografie ist es essenziell, dass Signaturprüfungen und Schlüsselverwaltungen dynamisch an neue Sicherheitsstandards angepasst werden können.

Dies betrifft sowohl die verwendeten Signaturalverfahren als auch die unterstützten Schlüssel- und Zertifikatsformate. Entsprechende Systeme sollten daher mehrere Verfahren parallel unterstützen (z. B. ECDSA und Ed25519) und die Möglichkeit bieten, neue Zertifikatsketten oder Prüfroutinen ohne Software-Neuinstallation zu integrieren. Nur so kann die Integrität der Patch-Prüfung auch über längere Systemlaufzeiten und bei schrittweisen Umstellungen gewahrt bleiben.

2.4.4 Herausforderungen und potenzielle Probleme

Trotz etablierter Verfahren können in der Praxis verschiedene Probleme auftreten:

- **Nicht signierte Patches:** Ältere Komponenten oder Hersteller ohne etablierte Signaturpraxis liefern Updates ohne Prüfmöglichkeit. In solchen Fällen muss durch alternative Verfahren (Checksummen, manuelle Freigaben, isolierte Testläufe) ein Mindestmaß an Integritätskontrolle gewährleistet werden.
- **Ungültige oder abgelaufene Zertifikate:** Selbst bei signierten Patches kann eine fehlerhafte Zertifikatsverwaltung dazu führen, dass gültige Patches fälschlich abgelehnt oder manipulierte akzeptiert werden.
- **Verlorene Schlüssel oder fehlende Vertrauenskette:** Wenn öffentliche Schlüssel nicht mehr zugänglich oder verifizierbar sind, ist keine sichere Verifikation möglich. Daher müssen Schlüssel systematisch archiviert und verteilt werden.
- **Fehlende Unterstützung durch Komponenten:** Manche OT-Geräte verfügen über keine integrierte Verifikationsfunktionalität. In diesen Fällen muss die Prüfung extern erfolgen, z. B. durch vorgelagerte Update-Proxys oder Managementsysteme.

2.5 Ergänzende Sicherheitsmaßnahmen

Patch-Management in OT-Umgebungen ist stets als Teil eines ganzheitlichen Sicherheitskonzepts zu betrachten. Da nicht alle Systeme jederzeit gepatcht werden können — etwa aufgrund fehlender Herstellerunterstützung, begrenzter Wartungsfenster oder technischer Einschränkungen — sind zusätzliche Schutzmechanismen notwendig, um die verbleibenden Risiken abzumildern. Diese ergänzenden Maßnahmen erhöhen die Resilienz der Umgebung gegenüber Angriffen und mindern die Auswirkungen potenzieller Schwachstellen.

2.5.1 Netzsegmentierung und Zugriffskontrollen

Eine klare Trennung von Netzsegmenten nach Sicherheitszonen ist unerlässlich. So kann z. B. eine Verwundbarkeit in einem Steuergerät isoliert bleiben und nicht ohne Weiteres auf andere Systeme übergreifen. Durch kontrollierte Übergänge zwischen Zonen (z. B. Firewalls, Data Diodes) wird die Angriffsfläche erheblich reduziert. Zudem sollten Zugriffe auf OT-Komponenten strikt nach dem Prinzip der minimalen Rechte (“Least Privilege”) erfolgen und nachvollziehbar protokolliert werden.

2.5.2 Applikations- und Geräte-Whitelisting

Für Systeme, die nicht regelmäßig gepatcht werden können, bietet sich ein Whitelisting-Ansatz an. Dabei wird nur der explizit freigegebene Code bzw. die zugelassene Kommunikation erlaubt. Dies verhindert die Ausführung unbekannter oder potenziell schädlicher Programme und blockiert unautorisierte Netzwerkverbindungen. Whitelisting ist insbesondere für Embedded-Systeme oder alte Betriebssysteme ohne aktuellen Support sinnvoll.

2.5.3 Backup- und Wiederherstellungsstrategien

Vor dem Einspielen eines Patches sollte stets ein aktuelles Backup der betroffenen Systeme erstellt werden. Dies gilt sowohl für Systemkonfigurationen als auch für anlagenspezifische Daten. Im Fehlerfall muss eine schnelle Wiederherstellung möglich sein. Die regelmäßige Validierung der Backup- und Restore-Prozesse ist daher elementarer Bestandteil des Sicherheitskonzepts und sollte in Form von Testszenarien geprobt werden.

2.5.4 Monitoring und Intrusion Detection

Die kontinuierliche Überwachung der Systemintegrität und der Netzwerkkommunikation kann helfen, Angriffsversuche oder Fehlverhalten in Folge eines Patches frühzeitig zu erkennen. Der Einsatz von Intrusion Detection Systemen (IDS) oder Anomalieerkennung, speziell für industrielle Protokolle, bietet

zusätzliche Sicherheitsschichten. Eine lückenlose Protokollierung und Alarmierung ermöglicht zudem eine schnelle Reaktion im Ernstfall.

2.5.5 Schulungen und Awareness

Technische Maßnahmen entfalten ihre Wirkung nur im Zusammenspiel mit geschultem Personal. Regelmäßige Schulungen zu sicherem Patch-Management, Umgang mit Updates, Backup-Verfahren und relevanten Sicherheitsanforderungen sind essenziell, um menschliche Fehler zu vermeiden und das Sicherheitsniveau dauerhaft hoch zu halten.

2.6 Fazit

Ein wirksames Patch-Management stellt eine zentrale Maßnahme zur Absicherung von OT-Systemen in Energieinfrastrukturen dar. Es trägt maßgeblich dazu bei, bekannte Schwachstellen zu beheben, regulatorische Anforderungen zu erfüllen und die Resilienz der Systeme gegenüber Cyberangriffen zu erhöhen. Im Unterschied zur klassischen IT erfordert das Patchen in OT-Umgebungen jedoch eine besondere Sorgfalt, da hier hohe Verfügbarkeitsanforderungen, herstellerspezifische Abhängigkeiten und eingeschränkte Wartungsfenster berücksichtigt werden müssen.

Das vorliegende Konzept zeigt, dass ein sicheres und praxistaugliches Patch-Management nur durch ein Zusammenspiel technischer, organisatorischer und prozessualer Maßnahmen möglich ist. Zentrale Elemente sind die strukturierte Erfassung von Assets, die risikobasierte Bewertung von Updates, das gestaffelte und kontrollierte Einspielen von Patches sowie eine nachvollziehbare Dokumentation aller Prozessschritte. Ergänzt wird dieser Kernprozess durch Querschnittsfunktionen wie Kommunikationsstrategie, Signaturprüfung, Redundanzmanagement und Schulung des involvierten Personals.

Nicht zuletzt ist Patch-Management kein einmaliger Vorgang, sondern ein kontinuierlicher Prozess. Nur durch regelmäßige Überprüfung, Verbesserung und Anpassung an neue Bedrohungslagen und regulatorische Vorgaben kann dauerhaft ein hohes Schutzniveau gewährleistet werden. Das hier beschriebene Konzept bietet hierfür eine Grundlage.

Literatur

[1] Canadian Centre for Cyber Security. *Cyber threat bulletin: The cyber threat to Canada's electricity sector*. 2020. URL: https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-canadas-electricity-sector (besucht am 23. 07. 2025).

[2] Tom Petersen, Joshua Stock und Hannes Federrath. *Bedrohungsszenarien für Energieinfrastrukturen*. 2023. URL: https://svs.informatik.uni-hamburg.de/publications/2023/2023-07-28-NRL-Whitepaper-UHH.pdf (besucht am 23. 07. 2025).

[3] Honeywell. *Experion® Process Knowledge System (PKS)*. URL: https://process.honeywell.com/us/en/solutions/experion-pks (besucht am 22. 07. 2025).

[4] Siemens. *SIMATIC WinCC SCADA System*. URL: https://www.siemens.com/global/en/products/automation/industry-software/automation-software/scada.html (besucht am 22. 07. 2025).

[5] Schneider Electric. *EcoStruxure ADMS - Advanced Distribution Management System*. URL: https://www.se.com/de/de/product-range/61751-ecostruxure-adms/ (besucht am 22. 07. 2025).

[6] AVEVA. *AVEVA System Platform*. URL: https://www.aveva.com/de-de/products/system-platform/ (besucht am 22. 07. 2025).

[7] ABB. *ABB Ability™ System 800xA*. URL: https://new.abb.com/control-systems/system-800xA (besucht am 22. 07. 2025).

[8] GE Vernova. *Proficy HMI Scada Software*. URL: https://www.gevernova.com/software/products/hmi-scada (besucht am 22. 07. 2025).

[9] Siemens. *SIMATIC S7-300*. URL: https://www.siemens.com/de/de/produkte/automatisierung/systeme/industrie/sps/simatic-s7-300.html (besucht am 22. 07. 2025).

[10] Rockwell Automation. *Human Machine Interface Allen-Bradley*. Zugegriffen: 21. Juli 2022. URL: https://www.rockwellautomation.com/en-gb/products/hardware/hmi.html (besucht am 22. 07. 2025).

[11] Schneider Electric. *Modicon M580 ePAC*. URL: https://www.se.com/ch/de/work/campaign/m580-epac/ (besucht am 22. 07. 2025).

[12] ABB. *AC500 PLC*. URL: https://new.abb.com/plc/programmable-logic-controllers-plcs/ac500 (besucht am 22. 07. 2025).

[13] Honeywell. *Controledge Family Controller*. URL: https://process.honeywell.com/us/en/initiative/control-edge/controledge-family-controller (besucht am 22. 07. 2025).

[14] Siemens. *Automatisierungs- und Fernwirkgeräte – SICAM A8000*. URL: https://www.siemens.com/de/de/produkte/energie/energieautomatisierung-und-smart-grid/stationsautomatisierung/automatisierungs-und-fernwirkgeraete-sicam-a8000.html (besucht am 22. 07. 2025).

[15] Siemens. *SIMATIC HMI Panels*. URL: https://www.siemens.com/global/en/products/automation/simatic/hmi/panels.html (besucht am 22. 07. 2025).

[16] Schneider Electric. *Harmony ST6*. URL: https://www.se.com/de/de/product-range/65770-harmony-st6/ (besucht am 22. 07. 2025).

[17] Rockwell Automation. *Bedienerschnittstelle (HMI) Allen-Bradley*. URL: https://www.rockwellautomation.com/de-de/products/hardware/hmi.html (besucht am 22. 07. 2025).

[18] ABB. *CP600-Panels*. URL: https://new.abb.com/plc/control-panels/cp600 (besucht am 22. 07. 2025).

[19] Honeywell. *Human Machine Interfaces (HMI) - Honeywell Process Solutions*. URL: https://process.honeywell.com/us/en/products/control-and-supervisory-systems/human-machine-interfaces-hmi (besucht am 22. 07. 2025).

[20] Schweitzer Engineering Laboratories (SEL). *Products: Protection Relays*. URL: https://www.selinc.com/protection/ (besucht am 22. 07. 2025).

[21] Siemens. *SIPROTEC 5*. URL: https://www.siemens.com/de/de/produkte/energie/energieautomatisierung-und-smart-grid/schutztechnik/siprotec-5.html (besucht am 22. 07. 2025).

[22] ABB. *Relion Schutz- und Steuerungsprodukte*. URL: https://new.abb.com/medium-voltage/de/mittelspannungsprodukte/distribution-automation-produkte-und-l%C3%B6sungen/relion-schutz--und-steuerungsprodukte (besucht am 22. 07. 2025).
[23] GE Grid Solutions. *Multilin 8 Series Protection & Control Relays*. URL: https://www.gevernova.com/grid-solutions/automation/protection-control-metering/multilin-8-series (besucht am 22. 07. 2025).
[24] Emerson. *Druckmessumformer und -wandler*. URL: https://www.emerson.com/de-de/automation/measurement-instrumentation/pressure-measurement/pressure-transmitters-and-transducers (besucht am 22. 07. 2025).
[25] Siemens. *CERT Services*. 2025. URL: https://www.siemens.com/global/en/products/services/cert.html (besucht am 29. 07. 2025).
[26] Schneider Electronics. *Security Notifications*. 2025. URL: https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp (besucht am 29. 07. 2025).
[27] ABB. *Cyber security alerts and notifications*. 2025. URL: https://global.abb/group/en/technology/cyber-security/alerts-and-notifications (besucht am 29. 07. 2025).
[28] CISA. *Advisory (AA22-083A): APT Cyber Actors Target Energy Sector Organizations*. URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-083a (besucht am 22. 07. 2025).
[29] Claroty. *NotPetya: Looking Back Six Years Later*. URL: https://claroty.com/blog/notpetya-looking-back-six-years-later (besucht am 22. 07. 2025).
[30] Avertium. *Top 5 Cyber Threats in the Energy Sector*. URL: https://www.avertium.com/resources/threat-reports/top-5-cyber-threats-in-energy-sector (besucht am 22. 07. 2025).
[31] Mandiant (via Google Cloud Blog). *Sandworm disrupts power in Ukraine with new OT attack: A detailed analysis*. URL: https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/ (besucht am 22. 07. 2025).