PULSE

CVE-Überwachung für OT-Anlagen

Technisches Datenblatt für die IT- und Sicherheitsabteilung

Dieses Datenblatt ist zur Weitergabe an Ihre IT- oder Sicherheitsabteilung gedacht. Es beschreibt technisch, was das CVE-Schwachstellenmanagement in Pulse tut, welche Daten dabei wohin fließen, wie es sich zu NIS2, IEC 62443 und der kommenden EU-Cyber-Resilience-Act-Meldepflicht verhält – und wo seine Grenzen liegen.

Kurzfassung

- Laufender, automatisierter Abgleich Ihres OT-Geräteinventars mit maschinenlesbaren Herstellersicherheitshinweisen (CSAF)
- Präzises Matching über Bestellnummer (MLFB), Produktfamilie und Firmware-Versionsbereich – nicht nur Hersteller/Produktname
- Vollständig dokumentierter Triage-Workflow mit Audit-Historie über Re-Scans hinweg
- Läuft als Modul auf Ihrer On-Premises-Appliance; nur der Abgleich selbst benötigt ausgehenden Zugriff auf den Pulse-Gateway
- Unterstützt die Nachweispflichten aus NIS2 (Art. 21) und den Prozessrahmen aus IEC 62443-2-1 – ersetzt aber keine Rechtsberatung

Warum das jetzt relevant wird

Seit dem 6. Dezember 2025 ist das NIS-2-Umsetzungsgesetz in Kraft. Es betrifft schätzungsweise 29.500 Einrichtungen in Deutschland – deutlich mehr als der bisherige KRITIS-Kreis. Fertigungsbranchen (u. a. Maschinenbau, Elektrotechnik, Metallverarbeitung, Fahrzeugbau) fallen über Anhang II der NIS-2-Richtlinie in aller Regel als „wichtige Einrichtung“ darunter, sobald ein Betrieb mindestens 50 Mitarbeitende oder mehr als 10 Mio. € Jahresumsatz/Bilanzsumme hat. Auch kleinere Zulieferer werden zunehmend über Sicherheitsfragebögen größerer Kunden in die Pflicht genommen.

Art. 21 Abs. 2 lit. e der NIS-2-Richtlinie verlangt ausdrücklich Maßnahmen zur „Schwachstellenbehandlung und -offenlegung“. Eine naheliegende technische Umsetzung dafür beschreibt auch das BSI in seinen CSAF-Empfehlungen: Sicherheitshinweise im CSAF-Format lassen sich automatisiert von den Herstellern abrufen und mit dem eigenen Anlagenbestand abgleichen – genau der Mechanismus, den das CVE-Modul von Pulse umsetzt.

Für die technische Umsetzung orientieren sich Auditoren und Systemintegratoren in der DACH-Region an der Normenreihe IEC 62443. Teil 2-1 (Edition 2, 2024) definiert für Anlagenbetreiber unter anderem die Security Program Elements „Asset-Inventar“ (CM 1.1), „Patch-Management“ (COMP 3) und „Schwachstellenbehandlung“ (EVENT 1.9) – dieselbe Kette, die Pulse als laufenden Prozess statt als jährliche Übung abbildet.

Zwei weitere Fristen zeichnen sich ab, ohne dass Pulse selbst darunterfällt: Die EU-Cyber-Resilience-Act (VO (EU) 2024/2847) verpflichtet Hersteller vernetzter Produkte ab dem 11. September 2026 zur Meldung aktiv ausgenutzter Schwachstellen; die neue EU-Maschinenverordnung (VO (EU) 2023/1230) verlangt ab dem 20. Januar 2027 Schutz vor absichtlicher Manipulation für Maschinen mit digitalen Elementen. Beides betrifft in erster Linie Maschinenhersteller und -integratoren, nicht den Anlagenbetreiber direkt – erhöht dort aber den Druck, auch die verbaute Zulieferkette (etwa die eingesetzten SPS) im Blick zu behalten.

> *Dieser Abschnitt ordnet die regulatorischen Treiber ein, ersetzt aber keine Rechts- oder Compliance-Beratung. Maßgeblich sind stets die für Ihren Betrieb einschlägigen Rechtstexte und deren Auslegung durch Ihre Rechtsabteilung oder einen Auditor.*

Wie der Abgleich funktioniert

Quellen: Pulse bezieht Sicherheitshinweise im CSAF-Format (Common Security Advisory Framework) direkt von Siemens ProductCERT, ABB PSIRT und KUNBUS PSIRT sowie – über den CERT@VDE-Aggregator – von rund 40 wei-

teren Herstellern der Industrieautomation. Neue und aktualisierte Hinweise werden mehrmals täglich automatisch abgerufen.

Gerätebestand: Für jedes zu überwachende Gerät wird ein CVE-Monitor angelegt – mit Hersteller, Bestellnummer (bei Siemens die MLFB, z. B. `6ES7518-4AX00-1AB0`) und optional dem Firmwarestand. Das erfolgt manuell oder per CSV-Import; Pulse liest den Gerätebestand nicht selbstständig aus dem Netzwerk aus (siehe Abgrenzung unten). Bestellnummer und Firmwarestand müssen Sie dafür nicht am Schaltschrank ablesen – die Geräteerkennung liefert beides, sobald ein Administrator einen Suchlauf startet.

Matching: Der Abgleich läuft dreistufig – (1) exakte Bestellnummer, (2) Produktfamilien-Normalisierung (z. B. erkennt Pulse, dass eine SIPLUS-Variante `6AG1…` dieselben Advisories betrifft wie die zugehörige SIMATIC-Standardausführung `6ES7…`), (3) Eingrenzung über den Firmware-Versionsbereich der Advisory. Lässt sich ein Versionsbereich nicht eindeutig auswerten, bleibt der Fund als zu prüfender Kandidat bestehen, statt stillschweigend zu verschwinden.

Bewertung: Jeder Fund erscheint als **Finding** mit CVSS-Score und -Vektor, CWE-Klassifizierung, betroffener Version, empfohlener Abhilfe (inkl. der Version, in der der Hersteller den Fehler behoben hat) und einem Link auf den Original-Hinweis.

Triage, Nachweis und Reporting

Jeder Fund durchläuft einen Bewertungsstatus: **Offen**, **In Bearbeitung**, **Gelöst**, **Nicht betroffen** (mit Begründung), **Akzeptiertes Risiko** (mit Begründung und Wiedervorlagedatum) oder **Wird nicht behoben** (mit Begründung). Entscheidungen sind sticky: Sie überstehen jeden Re-Scan und werden nicht durch einen automatischen Fund überschrieben. Läuft eine Risikoakzeptanz ab, kehrt der Fund automatisch zur Wiedervorlage zurück.

Ein Aktivitäts-Feed protokolliert jedes Ereignis – Erkennung, Verschwinden, Wiederauftreten, Ablauf einer Risikoakzeptanz, Triage-Änderungen mit Vorher/Nachher-Status und Begründung, Kommentare – jeweils mit Zeitstempel und, bei menschlichen Aktionen, mit Urheber. Findings werden nie gelöscht: Verschwindet eine Schwachstelle aus einem Scan, wird sie als „nicht mehr erkannt“ markiert und bleibt für die Historie erhalten. Die Ansicht „Betroffene Geräte“ zeigt zu jeder CVE die Reichweite über die gesamte Flotte; Administratoren können eine CVE per Sammel-Triage für alle betroffenen Geräte auf einmal bewerten. Eine wöchentliche E-Mail an die Organisationsadministratoren fasst offene sowie neue kritische und hochseverer Funde zusammen.

Dieser durchgehende Nachweis – wer hat wann welche Schwachstelle wie bewertet, und warum – ist genau das Artefakt, das ein Auditor oder eine Geschäftsleitung im Rahmen von NIS2 oder IEC 62443-2-1 sehen möchte, statt einer Excel-Liste oder einer Bauchgefühl-Entscheidung.

Datenfluss und Betrieb

Pulse läuft als Appliance in Ihrer eigenen Infrastruktur. Die Kernüberwachung (OPC-UA/S7), das Vorfallmanagement und die E-Mail-Alarmierung funktionieren vollständig auch ohne Internetzugang. Der CVE-Abgleich ist die eine Ausnahme: Da der laufend aktualisierte Sicherheitshinweis-Katalog zentral bei Pulse gepflegt wird, fragt Ihre Appliance ihn per verschlüsselter HTTPS-Verbindung beim Pulse-Gateway ab – authentifiziert über die signierte Geräteidentität Ihrer Appliance, nicht anonym zugänglich.

Übertragen werden dabei ausschließlich Hersteller, Bestellnummer und Firmwarestand der angelegten CVE-Monitore – keine Prozess-, Produktions- oder Messdaten. Der Katalog selbst (die Sicherheitshinweise) ist öffentlich; es handelt sich also nicht um den Versand sensibler Betriebsdaten, sondern um eine Abfrage „betrifft uns diese öffentliche Schwachstelle?“. Für den Firewall-/Proxy-Regelsatz Ihrer IT-Abteilung bedeutet das: Für dieses Modul ist ein ausgehender HTTPS-Zugriff (Port 443) der Appliance auf die Pulse-Gateway-Domain erforderlich.

> *Dieser Abschnitt beschreibt den Betrieb als Appliance in Ihrem eigenen Netzwerk. Pulse Cloud betreiben wir; den Datenfluss und den Regelsatz dafür stellen wir Ihrer IT-Abteilung auf Anfrage in derselben Form zusammen.*

Abgrenzung: was Pulse (heute) nicht ist

- **Kein passiver Netzwerk-Scan.** Pulse hört den Netzverkehr nicht mit – kein SPAN-Port, kein Tap, kein Traffic-Mirroring. Die Geräteerkennung findet Geräte aktiv, aber nur, wenn ein Administrator einen Suchlauf auf einem Bereich startet, den Sie vorgeben; ein CVE-Monitor entsteht daraus erst, wenn Sie ihn anlegen. Das reduziert Netzwerk-Risiko, ersetzt aber keine durchgehende Bestandsführung im Hintergrund.
- **Kein SBOM-Werkzeug.** Pulse verwaltet keine Software-Stücklisten Ihrer eigenen Produkte – relevant für Maschinenhersteller unter der Cyber-Resilience-Act, aber ein separates Thema von der hier beschriebenen Schwachstellenüberwachung zugekaufter Komponenten.
- **Konservative Versionsauswertung.** Lässt sich ein Firmware-Versionsbereich nicht zweifelsfrei parsen, behält Pulse den Fund als Kandidat, statt ihn zu verwerfen – im Zweifel ein Fund zu viel, nie ein übersehener.

- **Keine Segmentierungs- oder Firewall-Funktion.** Pulse bewertet und dokumentiert Schwachstellen; die Umsetzung von Abhilfemaßnahmen (Patch, Workaround, Netzwerksegmentierung) bleibt Aufgabe Ihres Teams.

Warum ein zusätzliches Werkzeug – und kein Excel-Sheet

Herstelleradvisories werden heute meist als PDF, Newsletter oder Webseite veröffentlicht – uneinheitlich, unstrukturiert, kaum systematisch mit dem eigenen Anlagenbestand abzugleichen. Klassische IT-Schwachstellenscanner wiederum arbeiten netzwerkbasiert und sind auf IT-Umgebungen zugeschnitten: Sie benötigen Netzwerkzugriff auf Ebene der Steuerung, liefern CVSS-Werte ohne OT-Kontext und sind selten auf kleine bis mittlere Anlagenparks preislich zugeschnitten. Pulse setzt stattdessen am Gerätebestand an, den Sie ohnehin für Wartung und Ersatzteilplanung pflegen, und bettet den Abgleich in dieselbe On-Premises-Appliance ein, die auch Störungen erkennt und Ihr Team alarmiert – ein Prozess, eine Historie, ein Ansprechpartner, statt Schwachstellenmanagement als isoliertes Zusatzprojekt.

Lizenzierung

Die CVE-Überwachung ist ein Lizenzmodul (1.900 €/Jahr, flatrate – unabhängig von der Anzahl überwachter Geräte) und wird pro Organisation aktiviert. Ohne aktives Modul sind CVE-Monitore und Findings nicht verfügbar.

Für das Gespräch mit Ihrer IT-Abteilung

Typische Rückfragen einer IT- oder Sicherheitsabteilung – Datenfluss im Detail, Authentifizierung, Update-Prozess der Appliance selbst, Rollen- und Rechtekonzept – beantworten wir Ihnen gerne direkt, auch gemeinsam mit Ihrer IT-Abteilung. Sprechen Sie uns an.