Vom CVE-Eingang zum geschlossenen Fall.

Nicht jede Meldung braucht eine Prüfung. Jede Meldung braucht einen Owner, eine Frist und ein Ende: einen ausgerollten Fix oder eine begründete Entscheidung.

1 · DIE EINE FRAGE AN DEN OWNER

Können Sie innerhalb der Frist aktualisieren?

Ja, der Regelfall
Aktualisieren, ausrollen, schließen. Der Nachweis ist die ausgerollte Version.

Nein
Bewerten, mitigieren oder befristet akzeptieren, mit Begründung und Ablaufdatum. Der Fall bleibt beim Owner.

2 · BEWERTET WIRD NUR IN DREI FÄLLEN

1
Kein Fix verfügbar
Nichts zu aktualisieren. Das Risiko sinkt anders: abschalten, abschotten, konfigurieren.

2
Update in der Frist nicht möglich
Major-Upgrade, Herstellersoftware oder Wartungsfenster. Bis dahin: Mitigation oder befristete Ausnahme.

3
Aktiv ausgenutzt
Im KEV-Katalog der CISA. Zählt auch, ob das System schon exponiert war: Incident Response.

3 · DIE STATUS EINES FALLS

Eingegangen
In einer Liste, nicht in Postfächern.

Zugeordnet
Produkt und Owner aus der Owner-Liste.

Beim Owner
Die eine Frage, mit Frist.

Behoben
Ausgerollt, oder Ausnahme mit Ablaufdatum.

Geschlossen
Erscheint im Monatsbericht an die IT-Security.

4 · FRISTEN: EIN STARTPUNKT

Klasse	Kriterium	Antwort des Owners	Update oder Mitigation
Aktiv ausgenutzt	Im KEV-Katalog oder nachweislich ausgenutzt. Von außen erreichbare Systeme zuerst.	1 Arbeitstag	7 Tage
Hoch	CVSS ab 7,0 oder hoher EPSS-Wert (Schwelle legen Sie fest).	5 Arbeitstage	nächstes Release, spätestens 30 Tage
Übrige	Komponente kommt bei Ihnen vor.	kein Einzelfall	im regulären Update-Rhythmus
Nicht vorhanden	Komponente kommt in keinem Produkt vor.	keine	schließen, ohne Weiterleitung

Ein Vorschlag; verbindlich legt Ihre Leitung die Fristen mit der IT-Security fest. EPSS: geschätzte Wahrscheinlichkeit einer Ausnutzung in 30 Tagen (FIRST).

5 · DIE OWNER-LISTE

Anwendung	Owner	Vertretung	Rollt aus
Kundenportal BEISPIEL	Team Portal	A. Muster	Plattform
Abrechnung BEISPIEL	B. Beispiel	C. Probe	Team Abr.

6 · DIE FALL-LISTE: EINE ZEILE JE MELDUNG

`CVE` `Komponente` `Produkt` `Owner` `Klasse` `Status` `Frist` `Entscheidung` `Begründung` `geschlossen am`

Chat und Meeting dürfen entscheiden. Festgehalten wird in der Liste. Owner ist, wer das System ändern darf, nicht wer koordiniert.

7 · DAMIT „UPDATE ZUERST“ SICHER BLEIBT

- Neueste Patch-Version der unterstützten Release-Linie, nicht blind „latest“.
- Einige Tage Abstand zu ganz neuen Releases, außer bei aktiver Ausnutzung.
- Automatisierte Tests sichern das Update ab. Fehlen sie, ist das die erste Baustelle.

8 · MONATLICH AN DIE IT-SECURITY

- Wie viele Meldungen zutrafen und wie viele nicht.
- Was behoben ist und was offen, mit Alter und Owner.
- Welche Ausnahmen laufen und wann sie enden. Damit kann die IT-Security künftig vorfiltern.