KONZEPT ZUR ABSTIMMUNG

Security Radar

Vom Versionsstand zum Wartungsauftrag

Der Radar ergänzt Zabbix um eine Übersicht zum Updatebedarf und eine Frühwarnung für Server, Anwendungen, Virtualisierungshosts und Netzwerkgeräte.

1. Versionsstand und Support erfassen

Vorhandene Bestandsdaten kommen lesend aus Zabbix. Fehlende Paketrevisionen, Builds oder Update-Kanäle erfassen wir am System. Die Übersicht unterscheidet verfügbare Updates in der eingesetzten Produktlinie, größere Upgrades und Supportenden.

2. Kritische Meldungen im Portal bündeln

Das Portal zeigt vorrangig kritische Herstellerhinweise und bekannte Ausnutzung zu eingesetzten Produkten. Der Radar bündelt Mehrfachmeldungen und erfasst auch Herstellerwarnungen ohne CVE. Technische Schwere und Relevanz für unsere Systeme bleiben getrennt sichtbar.

3. Betroffenheit prüfen und Maßnahmen zuordnen

Feste Regeln vergleichen den installierten Stand mit dem Fix des jeweiligen Paketanbieters. Ein Debian-Backport kann die Lücke in einer älteren Paketversion schließen. Die KI erklärt die Zuordnung, benennt fehlende Angaben und schlägt einen Prüfschritt vor. Das Technikteam bestätigt die Einstufung.

Sofort handeln. Akuter Prüfbedarf geht per E-Mail an das Ticketsystem.
Nächste Wartung. Bestätigten Fall mit Termin und Begründung einplanen.
Bereits behoben. Installierte Paketrevision oder Build enthält den Fix.
Nicht relevant. Produkt, Version oder betroffene Funktion trifft nicht zu.
Noch zu prüfen. Fehlenden Build, Paketursprung oder Konfiguration benennen.

Pilot und Nutzen für Wartung und Vertrieb

Mit einer ausgewählten Systemgruppe starten. An früheren Fällen Quellen und Versionsabgleich prüfen. Bestätigte Befunde liefern für Kundengespräche den betroffenen Stand, den Herstellerbeleg und die empfohlene Maßnahme.

QUELLENÜBERSICHT

Quellen je Stufe

Sollstand, Frühwarnung und Nachweis der Betroffenheit

1. Versionsstand	2. Kritische Meldungen	3. Betroffenheit und Fix
Debian		
Debian-Paketsuche und eingerichtete Repositories je Release.	Debian Security Advisories und LTS Advisories	Debian Security Tracker (JSON) für Release und vollständige Paketrevision.
Plesk und PHP		
Plesk Changelog für Panel und Komponenten. PHP-Releases und PHP-Supportstatus je Zweig.	Plesk Security Alerts und PHP Security Advisories	Aktiven PHP-Handler und Paketquelle prüfen. Fix laut Plesk, Debian oder PHP. Panel und Handler separat abgleichen.
MikroTik RouterOS		
RouterOS Changelogs für Stable oder Long-term.	MikroTik Security für Herstellerwarnungen.	MikroTik Security nennt Fix-Versionen. Installierten Stand, Kanal und betroffene Funktion prüfen.
Proxmox VE		
Proxmox Release-Historie und eingerichtete APT-Repositories.	Proxmox VE Security Advisories und Debian Security Advisories für Basispakete.	Proxmox-Hinweise und Paket-Changelogs für Proxmox-Pakete. Debian Tracker für Basispakete. Laufenden Kernel prüfen.
Windows Server und Dynamics NAV / Business Central		
Windows Server Release Information für Builds und KBs. NAV 2018 als Beispiel und Business Central On-Premises für Anwendungsstände.	Microsoft Security Update Guide und offizielle Updatehinweise für NAV bzw. Business Central.	Microsoft Security Update Guide für betroffene Produkte und Updates. OS-Build und Anwendungsbuild separat abgleichen.

Ergänzende Warnsignale in Stufe 2. BSI / CERT-Bund WID für herstellerübergreifende Warnungen und CISA KEV für bekannte Ausnutzung. Der konkrete Fix ergibt sich aus der zuständigen Herstellerquelle.