/ MAURISEC.DE

FIELD NOTES / CHECKLIST 08

Patchen mit Priorität: vom KEV-Treffer zum Nachweis

PRUEFEN. BELEGEN. NACHHALTEN.

Arbeitsliste für Schwachstellen- und Betriebsverantwortliche. Herstellerhinweise, betroffene Versionen und tatsächlich eingesetzte Komponenten müssen pro Befund geprüft werden.

Pruefbereich / Team:

Datum:

- [ ] **01 / Aktives Inventar mit Produkt, Version, Supportstatus, Standort, Exposition und fachlichem Eigentümer führen.**

  Nachweis: Abgleich zwischen Inventar, erreichbaren Diensten und eingesetzten Software-/Firmware-Versionen.

- [ ] **02 / Neue Herstellerhinweise und CISA-KEV-Einträge gegen das eigene Inventar prüfen; Produktnamen allein nicht als Betroffenheitsnachweis verwenden.**

  Nachweis: CVE, betroffene Version, technische Voraussetzung und zugeordnete eigene Systeme.

- [ ] **03 / Ausnutzung, Erreichbarkeit, Privilegiengewinn, Geschäftsfolgen und vorhandene Schutzmaßnahmen gemeinsam priorisieren; CVSS nicht isoliert verwenden.**

  Nachweis: Begründete Risikoeinstufung mit Verantwortlichem und intern festgelegter Frist.

- [ ] **04 / Korrektur direkt aus vertrauenswürdiger Herstellerquelle beziehen und Voraussetzungen, Integrität sowie Installationshinweise prüfen.**

  Nachweis: Herstellerreferenz, Paket-/Build-Bezeichnung und dokumentierte Integritätsprüfung, soweit angeboten.

- [ ] **05 / Für risikoreiche Änderungen repräsentative Tests, Betriebsfreigabe, Rückfallplan und erforderliche Sicherung vorsehen.**

  Nachweis: Testergebnis, genehmigter Ablauf und tatsächlich nutzbare Wiederherstellungsoption.

/ MAURISEC.DE

FIELD NOTES / CHECKLIST 08

- [ ] **06 / Rollout und gegebenenfalls Neustart ausführen; die wirklich laufende Version und nicht nur das installierte Paket prüfen.**

  Nachweis: Erfolgreicher Rollout plus Laufzeit-/Boot-/Firmware-Nachweis und erneute Schwachstellenprüfung.

- [ ] **07 / Kann noch nicht gepatcht werden, eine zum konkreten Befund passende Kompensation umsetzen und ihre Wirkung prüfen.**

  Nachweis: Beispielsweise belegte Zugriffsbeschränkung; befristete Risikoentscheidung mit erneutem Prüftermin.

- [ ] **08 / Bei möglicher vorheriger Ausnutzung zusätzlich Vorfallsprüfung und herstellerspezifische Wiederherstellungsschritte veranlassen.**

  Nachweis: Untersuchungsauftrag und gesicherte Befunde; Patchstatus und Kompromittierungsstatus getrennt dokumentiert.

- [ ] **09 / Befund erst mit Wirksamkeitsnachweis schließen; Ausnahmen, nicht erreichte Systeme und abgekündigte Produkte weiterverfolgen.**

  Nachweis: Abschlussbeleg, Restliste und aktualisiertes Inventar statt bloß eines erfolgreichen Verteilungslaufs.

GEGENPROBE / AUTORISIERTE TESTUMGEBUNG

Ein aktualisiertes Testsystem auf tatsächlich laufende Version und nötigen Neustart prüfen; zusätzlich eine nicht betroffene Inventarposition korrekt ausnehmen.

GRENZEN UND VORAUSSETZUNGEN

KEV dokumentiert bekannte Ausnutzung; das Fehlen einer CVE im Katalog beweist keine Harmlosigkeit. CISA-Fristen und US-Behördenvorgaben gelten nicht pauschal als gesetzliche Patchfristen für deutsche Privatunternehmen. Ein Update beseitigt nicht automatisch Persistenz, gestohlene Zugangsdaten oder andere Folgen einer vorherigen Kompromittierung.

PRIMAERQUELLEN / STAND 09.11.2026

NIST SP 800-40 Rev. 4: Enterprise Patch Management Planning
csrc.nist.gov

CISA: Known Exploited Vulnerabilities Catalog
www.cisa.gov

CISA: KEV-Priorisierung und Geltungsbereich der Behördenvorgaben
www.cisa.gov