Nach dem Patch: verbliebene Angriffswege wirklich schließen

PRUEFEN. BELEGEN. NACHHALTEN.

Für einen eigenen Dienst nach einer kritischen Schwachstelle mit möglicher vorheriger Ausnutzung. Richtwert: 120 Minuten für eine erste belegte Prüfung eines Dienstes; Forensik, Bereinigung und Wiederaufbau benötigen zusätzliche Zeit. Bei konkretem Verdacht den Vorfallsprozess aktivieren.

Pruefbereich / Team:

Datum:

- [ ] **01 / Expositionszeitraum, betroffene Instanzen und erreichbare Schnittstellen einschließlich Replikaten und Administrationspfaden abgrenzen.**

  Nachweis: Zeitlinie aus Inventar, Herstellerhinweisen und Erreichbarkeitsdaten; unbekannte Zeiträume ausdrücklich markiert.

- [ ] **02 / Vor Bereinigung untersuchungsrelevante Logs und Zustandsdaten nach Vorfallsplan sichern; Aufbewahrung und Zugriffsrechte festlegen.**

  Nachweis: Gesicherte Artefakte mit Herkunft, Zeitbezug und Integritätsnachweis; dokumentierte Erfassungslücken.

- [ ] **03 / Die vom Hersteller geforderte korrigierte Laufzeit auf allen Instanzen einschließlich Neustart- oder Konfigurationsanforderungen belegen.**

  Nachweis: Laufende Builds, aktive Komponenten und Abschluss der produktspezifischen Nacharbeiten statt nur Installationsstatus.

- [ ] **04 / Bei möglichem Geheimniszugriff betroffene Zugangsdaten und ausgegebene Sitzungen bestimmen; Widerruf und Ersatz koordiniert ausführen.**

  Nachweis: Betroffenheits- und Widerrufsliste mit Zeitpunkten, geprüfter Restgültigkeit und funktionierenden abhängigen Diensten.

- [ ] **05 / Für das Produkt passende Persistenzflächen gegen einen vertrauenswürdigen Ausgangsstand prüfen: Konten, App-Berechtigungen, Schlüssel, Startaufgaben und Fernzugänge.**

  Nachweis: Datierter Soll-Ist-Abgleich und Untersuchung jeder nicht erklärten Änderung; Herstellerindikatoren ergänzend ausgewertet.

/ MAURISEC.DE

FIELD NOTES / CHECKLIST 14

- [ ] **06 / Die ursprüngliche Zugriffskette zusätzlich begrenzen: unnötige externe Verwaltung, direkte Backend-Zugänge und überbreite Dienstrechte überprüfen.**

  Nachweis: Aktuelle Pfad- und Rechteübersicht mit belegten Erlaubnis- und Sperrentscheidungen.

- [ ] **07 / Bei nicht belastbar bereinigbarem System einen Wiederaufbau aus vertrauenswürdiger Quelle entscheiden und Wiederherstellungsdaten vor Nutzung prüfen.**

  Nachweis: Begründete Bereinigungs- oder Neuaufbauentscheidung; Integritätsprüfung von Images, Konfigurationen und Rücksicherungen.

- [ ] **08 / Wiederanbindung an technische und fachliche Abnahmekriterien sowie befristete verstärkte Beobachtung knüpfen.**

  Nachweis: Freigabe durch Dienst- und Vorfallsverantwortliche, überprüfte Funktion und Zuständigkeit für erneute verdächtige Zugriffe.

GEGENPROBE / AUTORISIERTE TESTUMGEBUNG

Von genau einem autorisierten Testclient im nun ausgeschlossenen Netz einen harmlosen Verbindungsversuch zum eigenen, vorher benannten Verwaltungsport ausführen. Bestehen: Die erwartete Netzsperre greift und ihr Protokoll nennt Quelle, Ziel und Ergebnis. Kein Exploit und kein Scan weiterer Ziele; ein HTTP-Loginfehler allein belegt keine Netzsperre.

GRENZEN UND VORAUSSETZUNGEN

Ein negativer Scan oder fehlende bekannte Indikatoren beweist keine Kompromissfreiheit. Patchen widerruft weder gestohlene Geheimnisse noch Anwendungssitzungen und beseitigt nicht automatisch Persistenz. Art und Umfang der Prüfung folgen Produkt, Exposition und Befunden; US-Behörden-Playbooks begründen keine pauschalen Pflichten für andere Organisationen.

PRIMAERQUELLEN / STAND 09.11.2026

CISA: Incident and Vulnerability Response Playbooks
www.cisa.gov

NIST SP 800-61 Rev. 3: Incident Response Recommendations
nvlpubs.nist.gov

Microsoft Learn: Containment, eradication, and recovery
learn.microsoft.com

OWASP: Secrets Management Cheat Sheet
cheatsheetseries.owasp.org