SQUR

Checkliste: Autonome Pentests für Energieversorger

Zum Fachbeitrag "Autonome Pentests für Energieversorger: Sicherheit im Takt Ihrer Releases". Autor: Adam Lundqvist, SQUR · **squr.ai**

Für jeden Anbieter. Die Verweise beziehen sich auf den Fachbeitrag "Autonome Pentests für Energieversorger: Sicherheit im Takt Ihrer Releases".

1. Erste Anwendung und Bestand (Kapitel 2)

- ☐ Für die erste Anwendung sind Verantwortlicher, Freigabe des Betreibers, Testumgebung, Testidentitäten und der Umgang mit Befunden geklärt; der erste Lauf ist terminiert, bevor Inventar und Stufung fertig sind.
- ☐ Alle Webanwendungen und APIs sind inventarisiert, auch die von Konzern-IT und Dienstleistern betriebenen, mit benanntem Betreiber; die von außen sichtbaren Hosts sind per Attack-Surface-Scan abgeglichen.
- ☐ Je Anwendung sind Änderungsrate (Releases je Jahr aus den Pipeline-Daten) und Schadenswirkung (Datenklasse, Geld, Steuerungsnähe, Mandanten, Erreichbarkeit, Regime) festgehalten.
- ☐ Jede Anwendung hat eine Stufe A bis D und ein maximal tolerierbares Zeitfenster zwischen Änderung und Prüfung. Für fremdbetriebene Anwendungen ist der Weg zum Nachweis festgelegt.
- ☐ Auslöser sind im Change-Prozess verankert: wesentliche Änderung, Vorfall im Umfeld, neue Angriffsform.

2. Befugnis und Regeln (Kapitel 3)

- ☐ Der Betreiber jedes Zielsystems hat den Test schriftlich freigegeben.
- ☐ Freigabeliste mit Host, Port und Betriebsart je Adresse; zerstörerische Handlungen sind ausgeschlossen; die Betriebsarten des Anbieters sind auf die vier Stufen des BSI-Rasters abgebildet.
- ☐ Zwei bis drei Testidentitäten je Rolle und eigene Testobjekte sind bereitgestellt; schreibende Tests und Steuerbefehle gelten nur dort, nie im Produktivbetrieb.
- ☐ Verbotene Handlungen stehen im Vertrag: Ansprache von Personen, Datenabfluss über den minimalen Beweis hinaus, Wiederverwendung von Zugangsdaten, Persistenz.

3. Abnahmetest vor dem Ausbau auf Produktivsysteme (Abschnitt 3.3)

- ☐ Köder-Host (verboten eingetragen, jede Verbindung protokolliert): eigenes Protokoll leer, Protokoll des Anbieters zeigt den blockierten Versuch.
- ☐ Stoppmessung für beide Abbruchwege; beide Zeiten stehen im Abnahmeprotokoll.
- ☐ Gegenlogging: Quelladressen und Zeitfenster des Anbieters stimmen mit dem eigenen Protokoll überein; Abweichungen sind erklärt.
- ☐ Ein Lauf mit gescheiterter Anmeldung wird als unvollständig gemeldet, nicht als "keine Befunde".
- ☐ Aufbewahrungs- und Löschfristen, Schwärzungsregel und Verarbeitungsorte stehen im Vertrag.

4. Behebung und Nachweis (Kapitel 4)

- ☐ Jeder Befund trägt fünf Felder: Schwachstelle, Beweis (Anfrage-Antwort-Paar mit Gegenprobe), Frist und Verantwortlicher, Behebung, Retest-Ergebnis. Die Kennung bleibt über alle Läufe gleich.
- ☐ Für die Behebung gelten Fristen je Schweregrad und ein Verantwortlicher je Anwendung; der Retest folgt direkt auf die Korrektur.
- ☐ Ein Quartalsbericht mit vier Kennzahlen liegt der Geschäftsleitung vor: Abdeckung je Stufe, offene Schwachstellen nach Schwere und Alter, mittlere Behebungszeit, Retest-Quote.
- ☐ Jede Anwendung hat eine Regimespalte (BSIG, § 5c EnWG, nicht erfasst), von der Rechtsabteilung bestätigt.
- ☐ Ein Programmdokument mit Stufung, Takt und Begründung liegt vor, bevor jemand danach fragt (§ 30 Abs. 1 Satz 3 BSIG, § 5d EnWG).

Rechtsstand 8. November 2026. Keine Rechtsauskunft. Ersten Lauf vereinbaren: ***squr.ai/meeting***