SWIFT CSCF v2026 · Control 7.3A

Checkliste zur Penetrationstest-Bereitschaft fuer SWIFT CSCF v2026 Control 7.3A

1. Nach Auswirkung abgrenzen

- ☐ Der SWIFT-Bestand ist inventarisiert: sichere Zone, Messaging-Schnittstelle, Bediener-Arbeitsplaetze, die Verbindung zum Netzwerk und die Back-Office-Systeme, die ihn speisen.
- ☐ Angriffspfade werden nach der Auswirkung einer Kompromittierung eingestuft, nicht nach der Leichtigkeit des Testens.
- ☐ Der Umfang ist gegen die sichere Zone und ihre Vertrauensgrenzen definiert, sodass der Test belegt, dass ein Angreifer nicht vom Back-Office in die Messaging-Schicht uebergehen kann.
- ☐ Der Test ist ueber den dreijaehrigen Szenariozyklus geplant und deckt Anwendungs-, Infrastruktur- und menschliche Pfade ab.

2. Mit Bedrohungsaufklaerung rahmen

- ☐ Aktuelle Erkenntnisse ueber Akteure, die auf Finanznachrichten abzielen, fliessen in die Testszenarien ein.
- ☐ Szenarien proben plausible, benannte Einbruchspfade statt generischer Schwachstellenklassen.
- ☐ Die Aufklaerungsgrundlage ist dokumentiert, sodass der Test als bedrohungsgesteuert im Sinne von DORA und OSFI B-13 gilt.

3. Nach dem strengsten Standard ausfuehren

- ☐ Der Test laeuft sowohl von innerhalb als auch von ausserhalb der Systemgrenzen und erfuellt damit die Erwartung von NYDFS Part 500.
- ☐ Der Test wird von einer kompetenten und hinreichend unabhaengigen Partei durchgefuehrt.
- ☐ Einsatzregeln, Autorisierung und Sicherheitskontrollen fuer das Testen von Produktivsystemen sind dokumentiert und genehmigt.
- ☐ Eine festgelegte Taktung wird bestimmt und festgehalten, sodass das jaehrliche NYDFS-Minimum und der SWIFT-Zyklus gemeinsam erfuellt werden.

4. Die eigenen Abwehrmassnahmen messen

- ☐ Die Uebung misst, ob die Ueberwachung den simulierten Einbruch erkannt hat, nicht nur, was gefunden wurde.
- ☐ Die Leistung von Reaktion und Eindaemmung wird gegen die Funktionen Erkennen und Reagieren festgehalten.
- ☐ Erkennungsluecken werden als eigenstaendige Befunde erfasst.

5. Den Kreis schliessen und die Nachweise sichern

- ☐ Befunde gelangen in einen nachverfolgten Behebungszyklus mit Verantwortlichen und Terminen.
- ☐ Der Abschluss der Behebung wird nachgewiesen, nicht nur behauptet.
- ☐ Der vollstaendige Datensatz (Umfang, Szenarien, Angriffsverlauf, Befunde, Behebung, Erkennungsleistung) wird einmalig entlang des Rueckgrats des NIST Cybersecurity Framework 2.0 abgelegt.
- ☐ Der einzelne Datensatz wird jedem Regelwerk zugeordnet: SWIFT 7.3A, DORA, NYDFS Part 500, OSFI B-13.