SWIFT CSCF v2026 · Control 7.3A

Checklist voor gereedheid van de penetratietest voor SWIFT CSCF v2026 Control 7.3A

1. Bepaal de afbakening op basis van gevolg

- ☐ Het SWIFT-landschap is geïnventariseerd: beveiligde zone, berichteninterface, werkstations van operators, de verbinding met het netwerk en de back-officesystemen die deze voeden.
- ☐ Aanvalspaden worden gerangschikt op het gevolg van een compromittering, niet op het gemak van testen.
- ☐ De afbakening wordt bepaald ten opzichte van de beveiligde zone en de vertrouwensgrenzen ervan, zodat de test aantoont dat een aanvaller niet kan pivoteren vanuit de back-office naar de berichtenlaag.
- ☐ Het testen is gepland over de scenariocyclus van drie jaar, met dekking van paden via applicatie, infrastructuur en mensen.

2. Kader met dreigingsinformatie

- ☐ Actuele informatie over actoren die financiële berichtgeving als doelwit hebben, voedt de testscenario's.
- ☐ Scenario's repeteren plausibele, met naam genoemde inbraakpaden in plaats van generieke kwetsbaarheidsklassen.
- ☐ De informatiebasis is gedocumenteerd, zodat de test kwalificeert als dreigingsgestuurd onder DORA en OSFI B-13.

3. Voer uit volgens de strengste norm

- ☐ De test wordt zowel van binnen als van buiten de grenzen van de systemen uitgevoerd, waarmee aan de verwachting van NYDFS Part 500 wordt voldaan.
- ☐ De test wordt uitgevoerd door een bekwame en voldoende onafhankelijke partij.
- ☐ De spelregels, de autorisatie en de veiligheidsmaatregelen voor het testen van productiesystemen zijn gedocumenteerd en goedgekeurd.
- ☐ Er wordt een vastgelegde frequentie bepaald en geregistreerd, die zowel het jaarlijkse NYDFS-minimum als de SWIFT-cyclus samen vervult.

4. Meet uw eigen verdediging

- ☐ De oefening meet of de monitoring de gesimuleerde inbraak heeft gedetecteerd, niet alleen wat er werd gevonden.
- ☐ De prestaties op het gebied van respons en indamming worden geregistreerd ten opzichte van de functies Detecteren en Reageren.
- ☐ Detectiekloven worden op zichzelf als bevindingen geregistreerd.

5. Sluit de cyclus en leg het bewijs vast

- ☐ Bevindingen komen in een gevolgde herstelcyclus met eigenaren en datums.
- ☐ De afsluiting van het herstel wordt aangetoond, niet slechts beweerd.
- ☐ Het volledige dossier (afbakening, scenario's, aanvalsverhaal, bevindingen, herstel, detectieprestaties) wordt één keer vastgelegd op de ruggengraat van het NIST Cybersecurity Framework 2.0.
- ☐ Het enkele dossier wordt aan elk regime gekoppeld: SWIFT 7.3A, DORA, NYDFS Part 500, OSFI B-13.