

SECURITY TESTING CHECKLIST

preventie

TECHNOLOGIE

- ☐ Maak software-updates verplicht
- ☐ Implementeer single-sign-on (SSO)
- ☐ Herzie authenticatie- en toegangsprocedures
- ☐ Verwijder gevoelige gegevens en geheimen uit de code
- ☐ Implementeer encryptieprotocollen
- ☐ Pas veilige codeerpraktijken toe
- ☐ Integreer beveiligingstesten in de ontwikkeling •
- ☐ Voer penetratietesten uit op applicaties, API's en mobiele apps •
- ☐ Beveilig internet- en Wi-Fi-instellingen
- ☐ Installeer en configureer firewalls en eindpuntbescherming
- ☐ Monitor op verdachte activiteiten in systemen en netwerken
- ☐ Stel logging en monitoring in •
- ☐ Beveilig externe toegang (VPN, MFA, apparaatcontroles)
- ☐ Voer regelmatig netwerktesten uit •
- ☐ Maak back-ups van gegevens en test herstelprocedures
- ☐ Blijf op de hoogte van nieuwe kwetsbaarheden
- ☐ Voer continue kwetsbaarheidsbeheer uit

ORGANISATIE

- ☐ Stel een Security Officer aan (CISO of gelijkwaardig)
- ☐ Creëer een incidentresponsplan en -procedures voor beveiliging
- ☐ Beoordeel beveiligingsrisico's van leveranciers en derden
- ☐ Stem af op beveiligingsnormen (ISO 27001, NIS2, CIS Controls)
- ☐ Herzie en verbeter beveiliging jaarlijks op managementniveau
- ☐ Stel gecentraliseerde logging en monitoring in
- ☐ Zorg voor correcte procedures bij in- en uitdiensttreding

MENSEN

- ☐ Maak een lijst van alle medewerkers en koppel deze aan hardware (Asset Management)
- ☐ Organiseer phishing-simulaties •
- ☐ Bied beveiligingstrainingen aan voor al het personeel •
- ☐ Gebruik een wachtwoordmanager en sterke wachtwoorden
- ☐ Implementeer multi-factor authenticatie (MFA)
- ☐ Pas het principe van minimale rechten toe