knowit

Program för testning av digital motståndskraft

Det regulatoriska landskapet kräver att organisationer har ett riskbaserat och heltäckande program för att testa sin digitala operativa motståndskraft. Knowits erbjudande är utformat för att möta dessa krav, från exempelvis Dora-förordningen och NIS2-direktivet. Vårt fokus ligger på hotmodellering och teknisk testning, anpassat efter kundens verksamhet och riskprofil. Genom att identifiera de mest relevanta hoten säkerställer vi effektiv åtgärd av kritiska sårbarheter.

Planering och förberedelse

I denna inledande fas gör vi en kort genomgång av kundens befintliga riskanalys samt en bedömning av vad som är mest kritiskt hos era IKT-tjänster, system och informationstillgångar. Detta lägger grunden för vår hotmodellering.

Observera att detta testprogram förutsätter att kunden redan har ett ramverk för riskhantering inom informationssäkerhet. Saknas detta, erbjuder vi stöd för riskhanteringsarbete som en separat tjänst.

Metodik och utförande

Vår metodik för teknisk testning bygger på en transparent process som innehåller tre centrala steg:

Steg 1 – Hotmodellering
Vi kartlägger de mest relevanta hoten och sårbarheterna utifrån er verksamhets unika förutsättningar och det aktuella hotlandskapet.

Steg 2 – Teknisk testning
Utifrån hotmodelleringen genomför vi verifieringstjänster, exempelvis penetrationstester, anpassade efter kundens förutsättningar. Vi tillämpar vedertagen metodik och bästa praxis som PTES, CIS Benchmarks, NIST SP 800–115, samt OWASP Web Security Testing Guide, beroende på målbild och testmiljö.

Steg 3 – Rapportering och rekommendationer
Resultaten analyseras, sammanställs och prioriteras i en detaljerad rapport med åtgärdsförslag. Tillsammans med kunden utarbetas en handlingsplan med rekommendationer.

Leverans och uppföljning

Efter testningen levereras en omfattande rapport som dokumenterar:

- Identifierade hot samt genomförda tester
- Klassificering och prioritering av identifierade risker och sårbarheter
- Skräddarsydd handlingsplan med rekommenderade åtgärder
- Förslag på uppföljning för säkerställande av implementation av åtgärder

Fördelar med att samarbeta med Knowit

Bred expertis: Djupgående teknisk kunskap om aktuella hotbilder och sårbarheter samt juridisk spetskompetens.

Skräddarsydda lösningar: Tester och åtgärdsplaner anpassade efter era behov.

Helhetsstöd: Från förberedelse till uppföljning – vi är med er hela vägen.

Utbildning: Möjlighet till kompetenshöjande utbildning för er personal.

Kontakt

Kontakta oss för konsultation – tillsammans skapar vi en tryggare digital framtid för er verksamhet.

Knowit
Box 3383, 103 68 Stockholm
secure@knowit.se
knowit.se