Goede cyberaanvallen

In een digitale wereld waarin cyberdreigingen aan de orde van de dag zijn, spelen penetratietesten en ethische hackers een cruciale rol in het beschermen van gevoelige informatie en systemen. Terwijl criminele hackers voortdurend nieuwe technieken en methoden ontwikkelen om systemen binnen te dringen, zijn het juist de pentesten en ethische hackers die werken aan het versterken van deze systemen.

Wat is een Penetratietest?

Penetratietesten, vaak simpelweg 'pentest' genoemd, is een gecontroleerde vorm van hacking waarbij ethische hackers, met toestemming, op allerlei manieren en met alle mogelijke middelen toegang proberen te krijgen tot de IT-omgeving. Op die manier leggen ze de zwakke plekken van je netwerk, applicatie of zelfs gehele IT-infrastructuur bloot.

Het doel is om zwakke plekken in de beveiliging te identificeren voordat kwaadwillende hackers dit doen.

Wie zijn Ethical Hackers?

Ethische hackers zijn professionals die dezelfde technieken en methoden gebruiken als kwaadwillende hackers, maar met de intentie om systemen te beschermen en te verbeteren. Ze werken doorgaans voor organisaties om hun beveiliging te testen en aan te scherpen.

De term 'ethische hacker' benadrukt de ethische verantwoordelijkheid van deze professionals om de informatie die ze tijdens hun tests ontdekken, vertrouwelijk te behandelen en niet te misbruiken.

De essentie van pentesten

De Good Practice Informatiebeveiliging van DNB verplicht financiële instellingen om pentesten uit te voeren. De eisen van DORA[1] gaan zelfs nog wat dieper. De essentie is dat een pentest de ultieme controle is of alle controles ook werken zoals je denkt. Pentesten gaan op zoek naar de zwakkere plekken die misschien aan de aandacht zijn ontsnapt of waar je je niet bewust van bent. Ze geven je belangrijke input voor je PDCA-cyclus van continue verbetering.

Pentest InAudit

Na het behalen van de ISO27001 certificering, pakt InAudit door om de informatiebeveiliging nog verder aan te scherpen. Voor InAudit is informatiebeveiliging niet alleen een kwestie aan het voldoen van de ISO27001 normen. Binnen InAudit gaat het erom dat wij onze gegevens beschermen en betrouwbaar zijn voor onze klanten en partners. We zijn volledig toegewijd aan het waarborgen van onze privacy en beveiliging van alle betrokken data en hebben daarom ook zelf een pentest laten uitvoeren.

Conclusie

In het huidige cyberlandschap is het niet langer een vraag óf een organisatie zal worden aangevallen, maar wanneer. Penetratietesten en ethische hackers zijn daarom essentiële middelen voor elke organisatie die serieus is over de bescherming van haar gegevens en systemen. Ze zorgen niet alleen voor een veiligere digitale omgeving maar helpen ook bij het opbouwen en behouden van vertrouwen bij klanten en partners.

1. Digital Operations Resilience Act: Europese verordening met als doel dat financiële organisaties hun IT-risico's beter gaan beheersen en daarmee weerbaarder worden tegen cyberdreigingen.