PENTEST

UITGEBREIDE TEST VAN UW INFRASTRUCTUUR OF WEBAPPLICATIE/APP

Een penetratietest, kortweg pentest, is een gecontroleerde poging om in te breken in uw netwerk, wifi of (web)applicaties. Hiermee worden kwetsbaarheden geïdentificeerd die kunnen worden misbruikt door kwaadwillenden. Het doel van een pentest is om beveiligingsrisico's te identificeren en aanbevelingen te doen om deze risico's te verminderen.

WAAROM EEN PENTEST?

Een penetratietest is een cruciaal onderdeel van het beveiligen van uw bedrijfsnetwerk en gegevens. Door het proactief identificeren van kwetsbaarheden en het testen van uw beveiligingsmaatregelen, kunt u de beveiliging van uw bedrijf naar een hoger niveau brengen. Doordat u de sterktes en zwaktes van uw beveiliging in kaart heeft, kunt u ervoor zorgen dat uw bedrijf beter is beschermd tegen aanvallen van hackers. Met het uitvoeren van een penetratietest toont u ook aan dat u investeert in het beschermen van de gegevens van uw klanten en medewerkers.

Dit draagt bij aan het vertrouwen van uw klanten en een betere reputatie voor uw bedrijf. Daarnaast kunnen pentests vereist zijn voor compliance aan bepaalde regelgeving en normen, zoals ISO 27001/ NEN7510 en PCI-DSS.

WAT DOEN WE?

BIJ HET UITVOEREN VAN EEN PENTEST DOORLOPEN WE DE VOLGENDE STAPPEN:

Doelstellingen vaststellen
We stellen in overleg de doelstellingen vast. Hierbij wordt besproken wat we gaan testen (infrastructuur, wifi of (web)applicaties) en welke testen we gaan uitvoeren. Denk bij dit laatste aan inzet van phishing of social engineering om te kijken of we uiteindelijk rechten van een gebruiker kunnen overnemen. Daarnaast kunnen we zogenaamde black box- of grey box-testen uitvoeren.

Tijd is tijdens elke technische penetratietest een belangrijke factor. Over het algemeen kan worden gesteld dat meer testtijd meer resultaten oplevert. Zeker bij complexe omgevingen is het niet mogelijk om in een beperkte tijd een hoge mate van diepgang te creëren.

Informatieverzameling:
Voordat we starten met de test, verzamelen we informatie. Dit kan bijvoorbeeld informatie zijn over het netwerk, de systemen en/of de (web) applicaties. Deze informatie vormt de basis voor de volgende stappen van de test.

Vulnerability scanning
We scannen het doelwit op bekende kwetsbaarheden en verzamelen informatie over de beveiligingsarchitectuur en -configuratie. Hiervoor zetten onze ethisch hackers allerlei verschillende instrumenten in. De resultaten geven een beeld van aanwezige kwetsbaarheden en vormen de input voor het black box- en/of grey box-testen.

Black box-test
Met de in de eerste twee stappen verkregen kennis onderzoekt de ethisch hacker de omgeving op kwetsbaarheden. Hij of zij heeft geen speciale gebruikersrechten: het aanvalsscenario is dat van een kwaadwillende buitenstaander die toegang probeert te verkrijgen tot de omgeving die wordt getest.

Grey box-test
Met de kennis verkregen tijdens de eerdere fasen én met accountgegevens (zelf verkregen of verstrekt door de opdrachtgever) gaat de ethisch hacker op zoek naar kwetsbaarheden binnen het systeem. Hierbij wordt een scenario nagebootst van een kwaadwillende die de beschikking heeft over rechten binnen het te testen systeem.

Exploitatie
We proberen kwetsbaarheden te misbruiken om toegang te krijgen tot het doelwit en zoeken naar manieren om verder te komen.

Rapportage
We stellen een uitgebreid rapport op met de resultaten van de test, inclusief aanbevelingen voor verbetering van de beveiliging. Dit rapport wordt met u besproken en we kijken samen met u welke stappen er genomen kunnen worden om de beveiliging te verbeteren.

DE DRIE GROOTSTE VOORDELEN VAN EEN PENTEST

Identificeren van zwakke plekken
Een pentest helpt bij het identificeren van kwetsbaarheden in de systemen en applicaties die worden getest, waardoor u deze zwakke plekken kunt versterken voordat kwaadwillende hackers dat doen.

Inzet van gecertificeerd ethisch hackers
Onze ethisch hackers hebben jarenlange ervaring. Ze zijn in het bezit van internationale certificeringen zoals CISSP, Licensed Penetration Tester (LPT) of Certified Ethical Hacker (CEH).

Voldoen aan regelgeving
Veel organisaties zijn wettelijk verplicht om regelmatig pentests uit te voeren om aan bepaalde regelgeving te voldoen. Een pentest kan mogelijke boetes of andere sancties voorkomen.