Pentest

Een beveiliginsonderzoek of ook wel pentest (penetratietest) is een zeer effectieve manier om te achterhalen hoe het met de veiligheid van uw IT systemen gesteld is. Met een pentest gaan onze ethische hackers op realistische wijze aan de slag met het inbreken op uw systemen.

Om er zeker van te zijn dat u uw digitale beveiliging goed op orde heeft, is een penetratietest een must. Een penetratietest of pentest levert waardevolle inzichten waarmee uw organisatie de informatiebeveiliging kan versterken.

1 ONDERZOEK

Eén van de eerste stappen bij het starten van een pentest is het verkennen van het doelwit. Goed onderzoek kan de pentest maken of breken.

2 DOEL

Het doel is afhankelijk van de scope, maar eindigt vaak met toegang tot systemen, klantdata, of domain admin rechten.

3 PRAKTISCH

Een pentest is een praktische nulmeting op dat moment en brengt het huidige beveiligingsniveau in beeld.

Holistische aanpak

Een pentest richt zich doorgaans op één of meerdere onderdelen van uw IT infrastructuur. Pentests zijn eigenlijk een soort steekproeven. Onze analyse houdt daar echter niet op.

We combineren verschillende maatregelen, zowel geautomatiseerd als handmatig. Op die manier kunnen we beter maatwerk leveren en een hogere kwaliteit aanbevelingen doen en maatregelen aanbrengen.

Vragen?

Twijfelt u of uw omgeving wel veilig is of vraagt u zich af wat wij voor u kunnen betekenen? Neem vrijblijvend contact op kasperdewaard@kaaphoorn.net of bel op 0229 799 800.

Direct resultaat

Met een pentest achterhaal je direct het beveiligingsniveau op een bepaald punt binnen je IT infrastructuur.

- Onze ethische hackers brengen in kaart wat de risico's en gevolgen zijn.
- Direct actionbale data en een management rapport met aanbevelingen en praktische acties.
- Handvatten die u meteen kunt gebruiken om de IT security van uw bedrijf te verbeteren.

Intressant voor mij?

Met een pentest achterhaal je direct het beveiligingsniveau op een bepaald punt binnen je IT infrastructuur.

- Onze ethische hackers brengen in kaart wat de risico's en gevolgen zijn.
- Direct actionbale data en een management rapport met aanbevelingen en praktische acties.
- Handvatten die u meteen kunt gebruiken om de IT security van uw bedrijf te verbeteren.

Type pentests

In de wereld van cybersecurity kennen we de “aanvallende kant”, ook wel het “red team of pentester” genoemd, en de verdedigende kant, het “blue team”. Er is veel geschreven over het verschil tussen pentesten en red teaming, maar kort gezegd krijgt een pentester vaak een opdracht vanuit een vooraf bepaalde positie, terwijl een redteamer bijna alles moet doen om die positie te verkrijgen (denk hierbij aan phishing, social engineering, etc.). De red teamer moet dus ook vaak fysiek aan de slag.

Pentest

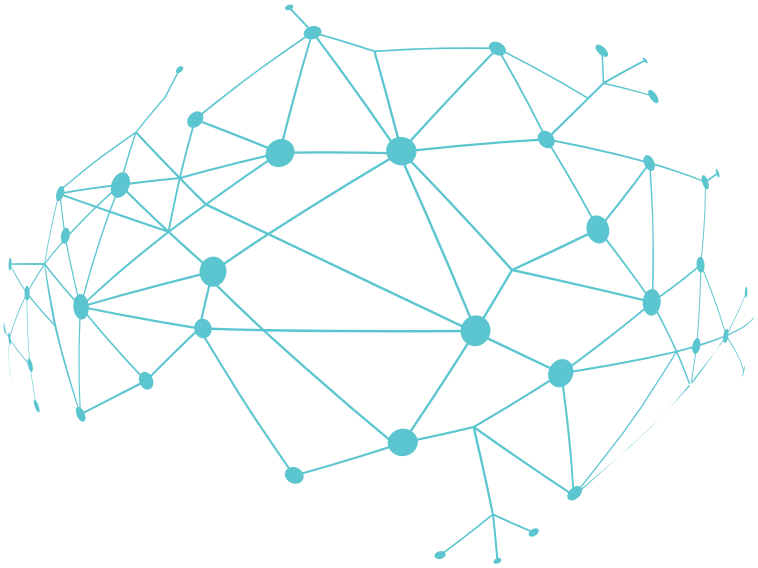
Het uitvoeren van een pentest kan op verschillende onderdelen van de organisatie.

- ### Netwerken & Infrastructuur
  Bij penetratietesten van de infrastructuur worden beveiligingszwakheden binnen je netwerk geïdentificeerd. Testers zoeken naar gebreken zoals verouderde software, ontbrekende patches, onjuiste beveiligingsconfiguraties, zwakke communicatiealgoritmes, commando-injecties, enzovoort.
- ### Wireless
  Hackers kunnen draadloze functionaliteiten benutten om een beveiligde omgeving van een organisatie te infiltreren, zelfs als er enkele toegangs- en fysieke beveiligingscontroles zijn geïmplementeerd.
- ### Web applicaties
  Web applicaties verwerken en/of bewaren vaak gevoelige informatie, waaronder creditcardgegevens, persoonlijk identificeerbare informatie (PII) en bedrijfseigen data. Door hun complexiteit en snelle ontwikkelingscycli zijn webapps vaak kwetsbaar. Daarom is ongeveer 40% van alle inbreuken gerelateerd aan webapps.

Methode

Een pentest kan ook op meerdere manieren worden uitgevoerd.

- ### Blackbox
  Bij een blackbox pentest simuleren we aanval op een netwerk van binnenuit waarbij de gedachte is dat een aanvaller is binnengedrongen via phishing of een kwetsbaarheid op het externe netwerk.
- ### Whitebox
  Bij een whitebox-aanpak worden vooraf login-gegevens verstrekt aan de pentester. Hierdoor kan een inzicht worden verkregen in de kwetsbaarheden die mogelijk uitgebuit kunnen worden door gebruikers die legitiem toegang tot een systeem, netwerk of applicatie hebben.



Een veilige omgeving begint met een 360-graden aanpak.

Over ons

We doen allemaal dat wat we het beste kunnen en voor ons is dat cyber security. Daarmee dragen wij ons steentje bij aan een prettigere en veiligere samenleving. Samen staan we sterk.

Contactgegevens

We leren u graag kennen om samen te bepalen wat we voor u kunnen betekenen. Voor een vrijblijvende kennismaking, bel of mail ons.

Telefoon: 0229 799 800
E-mail: kasperdewaard@kaaphoorn.net