

Penetratietest

Een penetratietest is een eenmalige, gecontroleerde test om te onderzoeken waar jouw organisatie kwetsbaar is. Dit kan gaan om netwerken, applicaties, systemen of apparaten. Onze ethische hackers voeren aanvallen uit die lijken op die van echte cybercriminelen. Zo ontdek je risico's voordat ze kunnen worden misbruikt.





Assessment

Penetratietest

Duur: 3 dagen, remote

Omschrijving

In het huidige cyberdreigingslandschap is het niet de vraag of je wordt aangevallen, maar wanneer. Door kwetsbaarheden op tijd te vinden en aan te pakken, verklein je de kans op datalekken, financiële schade en reputatieschade.

Deze dienst is bedoeld voor organisaties die zekerheid willen over de beveiliging van hun IT-omgeving. Of je nu moet voldoen aan compliance-eisen, vragen van klanten krijgt of simpelweg inzicht wilt in je beveiliging: met een penetratietest krijg je een onafhankelijk en professioneel beeld van je huidige beveiligingsstatus.

We werken met erkende methodieken zoals OSSTMM, OWASP, NIST, PTES en OSCP. Zo weet je zeker dat onze testen voldoen aan internationale standaarden.

Doelstellingen

- ☉ Kwetsbaarheden identificeren
- ☉ Risico's inzichtelijk maken
- ☉ Beveiligingsmaatregelen testen
- ☉ Compliance en regelgeving

Uitkomsten

- ☉ Gedetailleerd rapportage met bevindingen, risico-inschatting en praktische aanbevelingen.

Methode

Het traject begint met een intakegesprek waarin we jouw wensen, doelen en testomgeving bespreken. Daarna plannen we een scopingssessie. Hierin bepalen we welke onderdelen we testen, welke testvorm het beste past (blackbox of greybox), en hoeveel tijd daarvoor nodig is.

Vervolgens voeren onze ethische hackers de penetratietest uit.

Na afloop ontvang je een duidelijk rapport* met onze bevindingen, een inschatting van de risico's en praktische aanbevelingen. Wil je extra toelichting? Dan bieden we een optionele Q&A-sessie aan, waarin we het rapport samen doornemen en al je vragen beantwoorden in begrijpelijke taal.

Ook kun je kiezen voor een hertest. Daarbij controleren we of de aangepaste onderdelen nu goed zijn beveiligd.

**het rapport wordt in het Engels opgeleverd*

Voorwaarden

Om de penetratietest veilig en effectief uit te voeren, gelden de volgende voorwaarden:

- ☉ De klant neemt deel aan een intake- en scopingssessie.
- ☉ Een ondertekende vrijwaringsverklaring is verplicht voordat wij starten met testen.
- ☉ Toegang tot systemen, gebruikersaccounts en technische documentatie moet tijdig worden aangeleverd.
- ☉ De omgeving moet stabiel en beschikbaar zijn op het moment van de test.



Assessment

Penetratietest

Overzicht

Rollen & Verantwoordelijkheden

Wat wij doen:

- Leveren van gecertificeerde ethische hackers.
- Voorbereiden en uitvoeren van de penetratietest volgens de afgesproken scope.
- Opleveren van een begrijpelijk rapport met verbeterpunten.
- (Optioneel) Geven van een toelichting en beantwoorden van vragen.
- (Optioneel) Uitvoeren van een hertest om opgelost bevindingen te controleren.

Wat jij doet:

- Levert tijdig de benodigde informatie en accounts aan.
- Zorgt voor beschikbaarheid tijdens intake en scope.
- Ondertekent de vrijwaring.
- Neemt actie op basis van de bevindingen in het rapport.

Assessment en kennisoverdracht

Scoping

Scoping

- Scoping call om de vereisten en structuur van de opdracht door te nemen en te helpen bij het kiezen van de bijpassende soort test en dagen te bepalen.

Start pentest

Uitvoeren van de penetratietest

- Uitvoeren van de penetratietest volgens de afgesproken scope.

Rapportage

Opleveren rapportage

- Oplevering rapportage met verbeterpunten.
- Oplevering gebeurd via een beveiligde manier.

Optioneel

Q&A, hertest

- Q&A meeting indien gewenst, word er een eind meeting opgesteld om vragen te beantwoorden m.b.t. de rapportage en uitkomsten ervan.
- Hertest indien gewenst: word er na het oplossen van de bevindingen, opnieuw gericht getest of de bevindingen nog aanwezig zijn.



**Meer informatie? Neem
contact met ons op**

✉ info_nl@ek.co

🌐 www.ekco.nl

☎ 088 – 070 0600