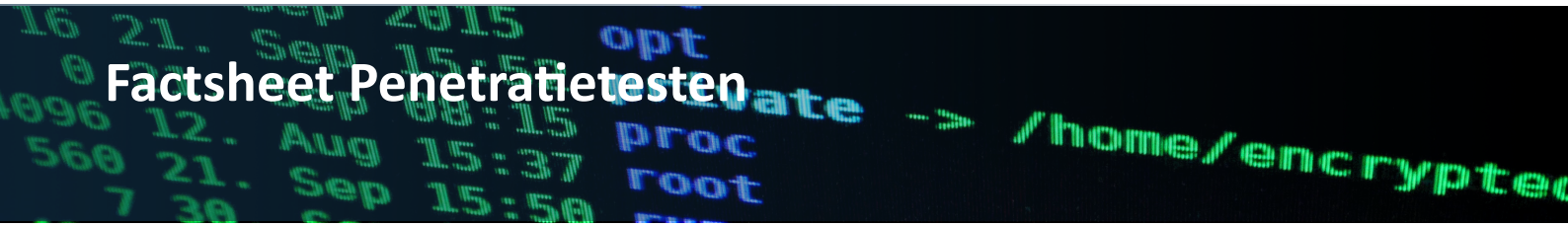
INFORMATIE
BEVEILIGINGS
DIENST



# Factsheet Penetratietesten

**Een penetratietest (pentest) is een van de manieren om beter inzicht te krijgen in de kwaliteit van de digitale beveiliging. Dit is een geautoriseerde poging om (digitale) zwakheden in kaart te brengen door ethische hackers. Door het in kaart brengen van de zwakheden kan bepaald worden waar aanvullende maatregelen nodig zijn. U verhoogt hiermee de digitale weerbaarheid en toont tegelijkertijd aan dat u informatiebeveiliging serieus neemt.**

## Vooraf

Om bij een pentest tot een goed resultaat te komen zullen verschillende zaken bepaald moeten worden: de scope, de opdracht en de communicatie. Zonder duidelijk plan en een definitie van de doelstellingen draagt een pentest mogelijk niet bij aan een planmatige en risicogestuurde aanpak van informatiebeveiliging. Een pentest is onderdeel van een groter proces om periodiek de risico's tegen het licht te houden en kwetsbaarheden in kaart te brengen.

### a. Scope bepalen

Ieder computernetwerk is verschillend. Om effectief te kunnen testen moet bepaald worden op welke onderdelen van het IT-landschap de test zal plaatsvinden. Als vuistregel geldt dat u een test het beste kunt laten uitvoeren op die onderdelen waar een incident de grootste impact zou hebben op de bedrijfsprocessen.

### b. Type onderzoek bepalen

Er bestaan diverse soorten penetratietests die zijn te onderscheiden naar de informatie die de onderzoeker vooraf ter beschikking heeft. Geeft u informatie over de ICT-infrastructuur (white-box), geeft u beperkte informatie (grey-box) of juist helemaal geen informatie (black-box)? Afhankelijk van het risico dat u wilt vaststellen kunt u het type test bepalen. Een black-box test simuleert een hacker die van buiten de organisatie een aanval uitvoert terwijl een white-box test een aanvaller met kennis van de organisatie, bijvoorbeeld een (ex-) medewerker, nabootst.

### c. Opdracht opstellen

Voor de inhuur dient een opdracht en een vrijwaringsverklaring te worden opgesteld. In de opdracht maakt u afspraken over het type test en 'hoe ver' de pentester mag gaan om zwakheden aan te tonen. Vaak zal een penetratietester al een standaard vrijwaringsovereenkomst hebben. U kunt tevens het model van de vrijwaringsovereenkomst in Bijlage 1 van de Handreiking penetratietesten van de IBD (zie lees meer).

### d. Communicatie plannen

Om goed voorbereid te zijn zal een communicatieplan opgesteld en gecommuniceerd moeten worden. Daarin wordt bepaald wie op de hoogste gesteld worden van de resultaten en bevindingen. Dan gaat het in ieder geval om proceseigenaren, pentestpartij, de eigen CISO en eventuele betrokken derde partijen (bijvoorbeeld de ICT-leverancier of dienstverlener of een ketenpartner).

## Uitvoering en opvolging

Nadat alle randvoorwaarden ingevuld zijn kan de penetratietest van start gaan. Tijdens de uitvoering van de penetratietest dient de verantwoordelijke manager en/of CISO door de penetratietester op de hoogte gehouden te worden over de voortgang en de gevonden resultaten. De bevindingen uit de penetratietest komen dienen beoordeeld te worden. Dit kan in eerste instantie door de pentester gedaan worden. De bevindingen die uiteindelijk voor de gemeente als onacceptabel risico worden bestempeld, vereisen maatregelen om deze risico's in te perken dan wel te voorkomen. In een verbeterplan wordt aangeven welke maatregelen noodzakelijk zijn op basis van de bevindingen. Hierdoor kan het risico, dat is aangetoond met de penetratietest, gemitigeerd worden. Aan de acties in het verbeterplan kan een eindverantwoordelijke en deadline gekoppeld worden.

## Checklist Penetratietest

- O Scope bepaald
- O Type onderzoek bepaald
- O Opdracht opgesteld
- O Vrijwaringsverklaring getekend
- O Communicatieplan opgesteld

## Lees meer

Voor meer informatie leest u de handreiking Penetratietesten van de IBD: https://www.informatiebeveiligingsdienst.nl/product/handreiking-penetratietesten-v1-0/

Heeft u nog vragen? Dan kunt u contact opnemen met de IBD via info@IBDGemeenten.nl of via telefoonnummer 070 - 373 8011

VNG Realisatie