BDO DIGITAL

# Versterk uw digitale veiligheid met ethical hacking

In een wereld waar cyberdreigingen steeds complexer en omvangrijker worden, is de bescherming van uw IT-infrastructuur essentieel. Onze ervaren ethische hackers versterken uw digitale weerbaarheid door security- en penetratietesten uit te voeren. Dit is niet alleen cruciaal voor het waarborgen van uw cybersecurity, maar voldoet ook aan (inter)nationale wet- en regelgeving en normenkaders zoals de BIO, AVG, ISO27001 en NIS2.

## Onze aanpak

Bij BDO geloven we dat effectieve security begint bij een helder inzicht in de huidige status van uw beveiliging. Om uw organisatie te beschermen tegen de nieuwste gevaren, zorgen we voor de juiste beveiligingsmaatregelen die altijd 'up-to-date' zijn. Onze aanpak is afgestemd op de specifieke behoeften van uw bedrijf, de risicobereidheid en de vereisten vanuit wet- en regelgeving. Hierbij fungeren onze experts als uw centrale aanspreekpunt, begrijpen uw bedrijf en de markt, en zorgen voor een naadloze integratie van cybersecurity in uw bedrijfsvoering.

## Diensten

Binnen onze ethical hacking dienstverlening bieden we een uitgebreid aanbod aan diensten om de cybersecurity van uw organisatie te versterken en te beschermen tegen potentiële cyberaanvallen. Op de volgende pagina vind u een overzicht van onze diensten. Onze ethical hackers zijn OSCP-gecertificeerd en worden tweejaarlijks gescreend.

## Wat leveren we op?

- Een gedegen test afgestemd op klantbehoefte, scope en dreigingen;
- Ondersteuning voor auditdoeleinden;
- Duidelijk rapport in begrijpelijke taal inclusief heatmap;
- Directe reactie op ernstige gedetecteerde kwetsbaarheden;
- Duidelijke en afgestemde risico rating en uitleg van impact;
- Verbeterpunten en helder advies inclusief management samenvatting.

## Wat is onze aanpak?

**1. Voorbereiding** - Deze fase richt zich op het definiëren van de testomvang inclusief de systemen die getest moeten worden en de testmethoden die gebruikt zullen worden. Het is belangrijk om duidelijke communicatiekanalen op te zetten, toestemmingen te verkrijgen en belanghebbenden op de hoogte te brengen. Zo verloopt de test op een gecontroleerde en legale manier.

**2. Reconnaissance** - Het doel is om zoveel mogelijk informatie te verzamelen over het doelgebied, zowel via passieve (publiekelijk beschikbare informatie) als actieve (directe interactie met het doelwit) methoden, om potentiële aanvalsvectoren te identificeren, zowel op netwerk- als applicatieniveau.

**3. Kwetsbaarheidsanalyse** - Deze fase omvat een grondige controle van geïdentificeerde aanvals-vectoren op kwetsbaarheden met behulp van geautomatiseerde tools en handmatige technieken.

**4. Exploitatie** - Gevonden kwetsbaarheden worden uitgebuit om de ernst en diepte te beoordelen. Het doel is om kwetsbaarheden te verifiëren en ervoor te zorgen dat er geen verkeerde risico-classificaties zijn.

**5. Documentatie** - Het resultaat is een gedetailleerd rapport dat inzichten biedt in de kwetsbaarheden, inclusief beschrijvingen, ernst, bewijs, en aan-bevelingen voor verbetering van de beveiliging.

# Dienstenoverzicht

## Penetratietesten

Ontdek en mitigeer risico's binnen uw IT-infrastructuur door onze grondige penetratietesten. Ons team voert uitgebreide testen uit op uw systemen, netwerken en applicaties om zwakke punten en beveiligingslekken te ontdekken. Na de testfase ontvangt u een uitgebreid rapport met gedetailleerde bevindingen, risicoclassificaties en praktische aanbevelingen om geïdentificeerde kwetsbaarheden aan te pakken.

## Red Teaming

Test de effectiviteit van uw beveiligingsmaatregelen met onze Red Teaming dienst. We simuleren realistische cyber-aanvallen gebaseerd op potentiële bedreigingen specifiek voor uw organisatie. Ons team ontwikkelt aanvalsscenario's om kwetsbaarheden in uw beveiligingsinfrastructuur bloot te leggen.

## Attack Surface Assessment

Krijg een continu en proactief overzicht van uw publieke dreigingsniveau met onze Attack Surface Assessment. We monitoren en analyseren uw gehele aanvalsoppervlak – digitaal, fysiek en sociaal – om risico's en potentiële aanvals-vectoren bloot te leggen. Dit stelt uw beveiligingsteam in staat om snel en efficiënt te reageren op opkomende kwetsbaarheden en bedreigingen.

## Vulnerability Management

Met onze dienst identificeren, evalueren en verhelpen we kwetsbaarheden in de IT-infrastructuur van onze klanten. Vanuit ons Security Operations Center in Utrecht werken we nauw samen met organisaties (of hun IT-leveranciers) om het beveiligingsniveau van de infrastructuur op een hoog niveau te houden. Onze service omvat dagelijkse scans, risicoanalyses, en prioritering van kwetsbaarheden, evenals ondersteuning bij de implementatie van effectieve beveiligingsmaatregelen. Zo creëren we een veiligere bedrijfsomgeving die bestand is tegen de laatste dreigingen.

**MEER INFORMATIE**

Maak uw digitale veiligheid sterker en bereid uw organisatie voor op de voortdurende ontwikkeling van cyberdreigingen. Samen met BDO kunt u de weg inslaan naar een veiligere digitale toekomst. Wilt u meer informatie of een vrijblijvend gesprek? Neem dan contact op met:

**Kees Plas**
Partner BDO Digital
T 06 - 535 98 513
E kees.plas@bdo.nl

**Chester van den Bogaard**
Senior Adviseur BDO Digital
T 06 - 316 81 172
E chester.van.den.bogaard@bdo.nl



05/2024 – AD2414