

Ethical Hacking

In onze visie moeten organisaties en hun medewerkers veilig kunnen werken in een digitale wereld en alle kansen benutten die technologie en digitalisering biedt. Onze aanpak is er daarom op gericht om klanten te helpen technologie maximaal te benutten waarbij continuïteit en veiligheid van de digitale omgeving gewaarborgd moet blijven. Met onze ethical hacking dienstverlening krijgt u inzicht en concrete oplossingen en kunt u veilig blijven ondernemen. Nu en in de toekomst.

Cyber Security is een prioriteit

Een adequaat basis beveiligingsniveau voor uw digitale omgeving is vanwege de toenemende digitalisering en cyber criminaliteit essentieel. Cyberdreigingen groeien bovendien voortdurend in omvang en complexiteit. Ethical Hacking, het gecontroleerd testen en onderzoeken van de veiligheid & degelijkheid van een digitale omgeving, is daarom essentieel om de werking van beschermingsmaatregelen te testen.

Security- en penetratietests door ervaren ethische hackers zijn een goede manier om efficiënt en onafhankelijk zicht te krijgen op hoe het daadwerkelijk gesteld is met de security van de IT-infrastructuur en het applicatielandschap en netwerkinfrastructuur. Verder is een security test vaak een verplicht onderdeel van specifieke (inter)nationale wet- en regelgeving en normenkaders. Dit zijn bijvoorbeeld de AVG, WBNI, BIG en BIR, DigiD, ISO27001, NIST en industrie-standaarden zoals PCI DSS.

Sygnius' visie

In onze visie moeten mensen en organisaties veilig kunnen werken in een digitale wereld en alle kansen benutten die technologie en digitalisering biedt. Deze digitale wereld raakt websites, app's, cloud, webapplicaties en webshops maar tevens fysiek het bedrijf, de kantooromgeving, maar ook thuiswerkplekken en onderweg. Overal waar data over de organisatie en haar klanten beschikbaar en toegankelijk is, is passende digitale beveiliging belangrijk.

Het adequaat beveiligen van deze IT-omgeving is geen sinecure. Zeker als het uw bedrijfskritische applicaties en websites betreft. Een perfecte uitvoering door goed gebruik van de juiste tools, inzet van juiste methodieken en ervaring is daarbij essentieel. Kwetsbaarheden moeten in een onderzoek worden geïdentificeerd, terwijl tegelijkertijd bedrijfsgegevens zorgvuldig worden behandeld en beschermd. Testresultaten mogen nooit publiek bekend raken en de uitvoering moet nauwgezet aangepakt worden om elke kans op schade aan de bedrijfsvoering uit te sluiten.

Ethical Hacking vormt ook een belangrijk onderdeel bij het lanceren of updaten van een website, webshop of onlinedienst. U kunt daarmee vol vertrouwen de markt met een nieuwe dienst of website betreden of uw succes vergroten.

De juiste expertise

Onze securityspecialisten zijn gecertificeerde professionals met internationale ervaring die samenwerken om zo telkens de meest geschikte expertise in te kunnen zetten. Dit kan zowel op afstand, of in overleg op klantlocatie als gecombineerd worden uitgevoerd.

Afhankelijk van de behoefte, specialiteit en complexiteit, worden alle elementen door de juiste experts onderzocht. Van IT-infrastructuur, servers en netwerken tot standaard (web)applicaties of zeer specifieke omgevingen. Ongeacht of dit nu in (publieke) Cloud-omgevingen, datacenters of op klantlocatie staat.

Van inzicht naar bescherming

Testvormen

Black Box	Grey Box	White Box	Maatwerk
In een Black Box-onderzoek is vooraf geen informatie over het te testen systeem bekend en wordt getest zonder kennis vooraf van de omgeving. Hierbij is onderdeel van de test om meer informatie over het te onderzoeken object te vinden. Gemiddelde duur van een test is 4 dagen.	Grey Box-tests worden uitgevoerd op basis van op voorhand bekende informatie zoals functies van systemen of inloggegevens van applicaties, waardoor specifiek op bepaalde elementen kan worden getest, zoals de business logica. Gemiddelde duur van een test is 5 dagen.	White Box-tests geven alle mogelijke informatie voor aanvang van de test. Testers hebben toegang tot de kennis van (systeem)beheerders en inzicht in de volledige broncode van applicaties. Gemiddelde duur van een test is 7 dagen.	Voor specifieke wensen, bijvoorbeeld voor gevoelige omgevingen of multidisciplinaire opdrachten zoals Red of Purple Teaming, stellen wij in overleg een op maat gemaakt voorstel op.

Sygnius methodiek

- 🔑 Heldere afstemming van de scope en doelstelling van de security test, rekening houdend met specifieke branche-, bedrijfs- en omgevingskenmerken. Vastgelegd in een scoping document geaccordeerd door u.
- 🔑 Test uitvoering afgestemd op de specifieke omgevingen, zoals zoeken naar gevoelige informatie financiële data of IP, toegankelijke systemen, netwerk infrastructuur, bepaalde applicaties, etc.
- 🔑 Toepassing van best practices, juiste tools en specifieke expertise, volgens (internationale) standaarden zoals OWASP, NIST 800-115 of specifieke kaders zoals DigiD of PCI DSS.
- 🔑 De security tests kunnen zowel eenmalig als in abonnementsvorm periodiek worden uitgevoerd.
- structuur wordt voorzien van een certificering.
- 🔑 Duidelijk onderbouwde en afgestemde risico inschatting van onze bevindingen en geconstateerde kwetsbaarheden met uitleg van de impact.
- 🔑 Verbeterpunten in de vorm van een helder advies dat u kunt gebruiken om uw website of IT-omgeving verder te beschermen. Desgewenst helpen wij u bij de implementatie daarvan.
- 🔑 Direct contact met onze ethical hackers wanneer er kritische kwetsbaarheden of ernstige onvolkomenheden worden gevonden.
- 🔑 Naast het rapport een managementrapportage, waarbij niet alleen technisch de bevindingen beschreven staan, maar juist ook wat die bevindingen betekenen voor de bedrijfsvoering waarbij de focus op continuïteit en beschikbaarheid ligt.

Wat leveren we op?

- 🔑 Een gedegen penetratietest afgestemd op de klantbehoefte, inclusief scoping en inventarisatie van (potentiele) risico's en dreigingen, dit alles uitgevoerd volgens de bewezen Sygnius methodiek.
- 🔑 Rapport met gedetailleerde bevindingen in begrijpelijke taal en in een helder werkbaar overzicht. Dit rapport kent een standaard Sygnius

Prijsstelling

- 🔑 Door onze ervaring, bewezen werkwijze gecombineerd met hoge mate van automatisering kunnen wij zeer kosteneffectief werken.
- 🔑 Als richtprijs hanteren wij € 3.200,- excl. BTW per test. Hier gaan wij uit van een gemiddelde test duur van 4 dagen. Uiteraard is de testduur afhankelijk van de scope van de test.

Meer weten?

In onze visie moeten mensen en organisaties veilig kunnen werken in een digitale wereld en alle kansen benutten die technologie en digitalisering biedt. Met behulp van de beste experts & technologie en brengen wij de nieuwste oplossingen in de praktijk om dat te realiseren. Wij vertellen u graag in een persoonlijk en vrijblijvend gesprek wat onze dienstverlening voor uw organisatie kan bieden. Neem voor meer informatie contact met ons op via: info@sygnius.nl of 06 8115 2826

Van inzicht naar bescherming