vertrouwen hebben in uw infrastructuur is goed, maar uw kwetsbaarheden kennen is beter

Hoffmann penetratietesten

Cybercriminaliteit neemt naar verwachting fors toe de komende jaren. Criminelen, spionnen en activisten die een digitale aanval gebruiken om aan belangrijke informatie of geld te komen. Een penetratietest (pentest) laat zien of uw infrastructuur voldoende weerbaar is.

Het is belangrijk dat u regelmatig checkt of uw informatiesystemen voldoende veilig zijn. Zeker als u nieuwe systemen aan uw ICT infrastructuur toevoegt, maar ook omdat er dagelijks nieuwe kwetsbaarheden worden ontdekt in bestaande hard- en software. Een penetratietest geeft u inzicht in de kwetsbaarheden, en de gevolgen daarvan, in uw informatiesystemen. Niet alleen van uw website(s), maar ook uw interne netwerk, systemen en (zelfontwikkelde) applicaties.

Zichtbare impact

Onze specialisten doen bij de start een eerste scan van de mogelijkheden tot het verkrijgen van toegang tot uw systemen. Ze proberen zo snel mogelijk rechten te verkrijgen waarmee zij toegang hebben tot privacy- of bedrijfsgevoelige informatie of tot belangrijke bedrijf kritische processen.

In onze rapportage maken wij inzichtelijk hoe wij de kwetsbaarheid hebben gevonden, zodat uw ICT'ers dit kunnen reproduceren en repareren. Wij gaan bovendien waar mogelijk tijdens de test via de kwetsbaarheid uw systemen binnen en maken daarmee de gevolgen inzichtelijk. Want laten zien dat bepaalde gevoelige informatie voor ons beschikbaar is, heeft veel meer impact dan simpelweg vertellen dat het kan.

Richtlijnen en vrijwaring

Vanzelfsprekend doen wij dit zo voorzichtig dat uw kritieke processen daar geen hinder van hebben en houden we ons bij het testen aan voor uw sector belangrijke normen en richtlijnen. U geeft ons vooraf, door middel van een vrijwaring, toestemming om uw informatie-systemen te testen. Dit om te voorkomen dat wij ons schuldig maken aan computervredebreuk.

Blackbox, Greybox of Whitebox?

Onze onderzoekers voeren verschillende onderzoeken uit:

- Blackbox: In dit geval vallen onze onderzoekers uw systemen aan zonder enige voorkennis. Deze werkwijze benadert de aanval zoals een cybercrimineel dit ook zou doen.
- Greybox: Wij krijgen in dit geval een beperkte toegang tot de systemen van waaruit wij verder de kwetsbaarheden onderzoeken. Dit scenario komt overeen met een hacker die op enige wijze reeds toegang heeft tot uw systemen. Hierbij kunt u denken aan malware of een geslaagde phishing-actie. Dit is een reëel scenario waarbij bijvoorbeeld een medewerker van uw organisatie (onbedoeld) betrokken is bij een cyberaanval.
- Whitebox: In dit geval bestuderen wij ook de ontwerpen, broncode, documentatie en andere beschikbare informatie om u te kunnen adviseren over een betere beveiliging. Hierdoor kunnen op een efficiënte wijze kwetsbaarheden worden opgespoord.

Meer weten?

Zijn uw informatiesystemen (weer eens) toe aan een penetratietest?
Neem contact met ons op via info@hoffmannBV.nl of 088-2986600.