

One-pager

Pentesten: laat je verantwoord hacken

Elk bedrijf – groot of klein – heeft zijn IT-omgeving in bepaalde mate beveiligd. Hoe goed of slecht, daar kom je vaak pas achter als het al te laat is. Dat is het probleem. Zou je je niet beter voelen als je zeker wist dat de IT-beveiliging van jouw bedrijf in orde is? Met Pen Testing kun je daar zeker van zijn. De pentest van Anderis biedt je een actueel inzicht in de zwakke plekken met concrete handvatten voor adequate maatregelen om kwetsbaarheden te verhelpen en schade te voorkomen.

Een pentest, ook wel penetratietest genoemd, is een gecontroleerde aanval – een hack – op de systemen van je organisatie. We proberen, legaal en met jouw toestemming, de beveiliging van de systemen te omzeilen en digitaal in te breken. Zo kunnen we kijken wat er allemaal mogelijk is met de informatie waar toegang toe verschaft wordt. Denk aan kopieën maken, het versleutelen of zelfs het aanpassen of verwijderen van informatie. Kortom: we kunnen zwakke plekken blootleggen voordat ze worden misbruikt door cybercriminelen.

Doel

Het doel van een pentest is het achterhalen van (potentiele) beveiligingsrisico's binnen de geteste omgeving. Zodat je stappen kunt ondernemen om je beveiliging te verbeteren.



Black-box

Bij deze methodiek word er vooraf geen informatie aan de pentester gegeven. Op deze manier krijg je een helder beeld van de veiligheid van je website, infrastructuur, applicaties of (web) apps.

Grey-box

Bij deze methodiek beschikt de pentester over beperkt verstrekte informatie. Ze krijgen de inloggegevens. Zo kan ook worden onderzocht of er kwetsbaarheden zijn die van belang zijn voor medewerkers. Kunnen bijvoorbeeld niet alle medewerkers gemakkelijk toegang krijgen tot de HR-gegevens?

White-box

Bij deze methodiek beschikt de pentester over bijna alle nodige informatie. Bij deze informatie kun je denken aan source code, de gedefinieerde scope, een rollen/rechtenmatrix en een lijst met functionaliteiten. Hierdoor kan er zeer gericht opgezocht worden wat de IT-risico's zijn van bijvoorbeeld een website, app of webapplicatie.

Verkenning

We vormen we ons een beeld van jouw IT-omgeving. Hierbij worden de infrastructuren en gebruikte systemen in kaart gebracht. Hierdoor krijgen we een duidelijk beeld van de mogelijke bedreigingen waarmee je bedrijf te maken kan krijgen.

De aanval

Na de verkenning begint het daadwerkelijk aanvallen van je systemen. We voeren een realistische aanval uit en proberen in te breken in je IT-omgeving.

Rapportage en advies

Zo snel mogelijk sturen we je een overzichtelijk rapport met de risico's. Dit is een helder rapport met daarin de belangrijkste conclusies en aanbevelingen waarmee de beveiliging van uw organisatie verbeterd kan worden. Vervolgens kunt u deze aanbevelingen vertalen in concrete acties.

Voordelen

De Anderis Pentest biedt u de volgende voordelen:

- Inzet van zeer ervaren en gecertificeerde pentesters
- Na elke pentest ontvang je een overzichtelijk rapport waarin we de risico's presenteren, met een toelichting in duidelijke taal.
- Anderis is sinds 1999 een gezonde Nederlandse IT-organisatie met een groot landelijk klantenbestand
- Eigen SOC (Security Operations Center)

Contact

Bent u geïnteresseerd of wilt u meer informatie? Neem dan gerust contact met ons op via e-mail op security@anderis.nl, of bel met ons:

Greg van Brussel: +31 6 18 98 19 11
Perry Liebrechts: +31 6 22 37 30 10

U kunt ook onze website bezoeken voor meer informatie: anderis.security

Weerbaar zoals
geen anderis



anderis

IT Security