One-pager

Pentesten: van kwetsbaar naar weerbaar

Weet u hoe uw IT security ervoor staat? Weet u waar de kwetsbaarheden zitten? De beveiliging van uw IT landschap is immers een dynamisch proces. Uw organisatie is continu in beweging en bovendien worden dagelijks nieuwe kwetsbaarheden ontdekt, waar aanvallers misbruik van kunnen maken. De pentest van Pinewood biedt u een actueel inzicht in de zwakke plekken met concrete handvatten voor adequate maatregelen om kwetsbaarheden te verhelpen en schade te voorkomen.

Een pentest is een gecontroleerde aanval op een systeem van buitenaf met als doel kwetsbaarheden van het systeem bloot te leggen. Er worden doorgaans dezelfde methoden en technieken gebruikt als bij een echte aanval, zodat een echte aanval zo realistisch mogelijk kan worden nagebootst. De pentest wordt echter uitgevoerd door een legitieme partij in overleg met de partij die eigenaar is van het systeem.

Daarnaast is een pentest niet destructief, zodat het geen invloed heeft op het correct functioneren van het doelsysteem. Een pentester simuleert een aanval en probeert op die manier kwetsbaarheden van het systeem te ontdekken en uit te buiten.

Pentesten zijn er in verschillende aanvalssenario's afhankelijk van de hoeveelheid kennis die de pentester over het aanvalsdoelwit heeft. Deze aanvalsenario's worden aangeduid als Black-box, Grey-box en White box.

De pentest vindt plaats op één of meerdere systemen, service of functie. Voorbeelden hiervan zijn het testen van de beveiliging van een website, het testen van de toegang tot een interne server of het evalueren van een webshop, inclusief de koppeling met een betalingssysteem.

Doel

Het doel van een pentest is het in kaart brengen van hetmbeveiligingsniveau van één of meerdere systemen. De bevindingen van een pentest bestaan uit kwetsbaarheden die op systemen gevonden zijn. In de pentesten uitgevoerd door Pinewood wordt het risico van een kwetsbaarheid geclassificeerd van "Laag" tot "Kritiek".

Black-box

Een Blackbox pentest houdt in dat de pentester nauwelijks voorkennis heeft van het doelsysteem (hooguit het IP-adres of domeinnaam). Deze test is uitermate geschikt om de veiligheid van de firewall, gebruikte serversoftware of publieke websites te testen.

Grey-box

Een Greybox pentest houdt in dat de pentester beschikt over beperkt verstrekte informatie. Een Greybox pentest is geschikt om te testen of achterliggende netwerken en systemen veilig zijn voor bijvoorbeeld geautoriseerde gebruikers. Hierbij krijgt Pinewood beperkte uitleg over het doelsysteem en bijvoorbeeld een gast- of medewerkersaccount.

White-box

Biedt een zeer nauwkeurige analyse van informatiebeveiliging. Bij een Whitebox heeft de pentester alle relevante informatie zoals netwerkarchitectuur, functionele en technische ontwerpen.

Type testen/vraagstukken die Pinewood o.a. uit kan voeren zijn:

- OSINT (open source intelligence vraagstukken)
- Insider attacks
- Testen van (web) applicaties
- AD Checks
- IoT testen

Aanpak

Tijdens de pentest wordt een aantal stappen doorlopen:

- Vulnerability scan;
- Exploitatie fase (door pentester);
- Rapportage en advies.

Vulnerability Scan

Allereerst wordt er algemene informatie verzameld over de betreffende systemen. Deze informatie wordt opgehaald uit databases en bevat informatie over IP adressering, eigenaarschap van de IP blocks en DNS informatie. Vervolgens wordt een breedte-scan uitgevoerd op de systemen, welke een indicatie geeft van de applicaties die door de systemen worden aangeboden. Aan de hand van deze informatie kan effici nt en effectief gezocht worden naar de kwetsbaarheden die hiervoor bekend zijn.

Exploitatiefase (door pentester)

Op basis van de vergaarde kwetsbaarheden voeren onze testers een realistische aanval uit en proberen in te breken in uw IT-omgeving. Dit doen ze onder andere door middel van exploitatie van de gevonden kwetsbaarheden, zodat de tester “ongeautoriseerde” toegang heeft tot het systeem of tot informatie op het systeem.

Rapportage en advies

Rapportage vindt zo snel mogelijk plaats na het onderzoek om eventuele kwetsbaarheden zo snel mogelijk te kunnen verhelpen. De pentester maakt uitgebreid verslag van de kwetsbaarheden die gevonden zijn en zal advies geven aan de organisatie hoe de kwetsbaarheden het beste verholpen kunnen worden. Niet alleen gericht op de techniek, maar ook op de processen en op de voor uw geldende normen voor uw organisatie. Daarnaast zal er een indicatie gemaakt worden van de urgentie van de kwetsbaarheid.

Voordelen

De Pinewood Pentest biedt u de volgende voordelen:

- Inzet van zeer ervaren en kundige pentesters met o.a. OSWE, OSCP en CEH certificeringen.
- De Pinewood Pentest onderzoekt o.a. op basis van de meest bekende testing frameworks (zoals OWASP Testing Guide en PCI Penetration testing guide).
- Na elke pentest ontvangt u een gedetailleerd adviesrapport met concrete verbeterpunten. U krijgt inzicht in de effectiviteit van reeds getroffen security maatregelen en detecteert risico’s nog voordat ze problemen veroorzaken.
- Pinewood is sinds 1994 een gezonde Nederlandse organisatie met 100% focus op informatiebeveiliging.
- Pinewood is ISO 27001 en NEN 7510 gecertificeerd.

Over Pinewood

Pinewood is al sinds 1994 een gevestigde naam in de dynamische wereld van de IT-beveiliging. Focus, kwaliteit en samenwerking zijn de kernelementen van onze filosofie. Pinewood focust zich niet exclusief op de technische kant van IT, maar legt altijd de link met uw business. Als zorginstelling betekent dit dat uw informatiebeveiliging in vakkundige en veilige handen is.

Bent u geïnteresseerd of wilt u meer informatie, neem dan contact met ons op via e-mail **info@pinewood.nl** of op telefoonnummer **015 251 36 36**.

We see risks
before they hurt