cuccibu WHITEPAPER

Reduce Risk, Create Value

Pentest: hoe goed is de beveiliging van jouw IT omgeving?

Auteurs: Jorrit Huitema & Joris Wijnen **Gepubliceerd**: 30 maart 2023

Introductie pentesten

Het uitvoeren van een penetratietest, afgekort pentest, is een essentieel onderdeel van de informatiebeveiliging in een organisatie. Een pentest wordt steeds vaker gebruikt om de kwetsbaarheid van bedrijfssystemen en netwerken te evalueren. In deze Whitepaper zal worden uitgelegd wat pentests zijn, hoe ze werken en waarom ze steeds belangrijker worden.

Wat is een pentest?

Een **pentest** is het opzettelijk proberen binnen te dringen in – een component van – de IT omgeving. Dit met het doel de beveiliging van de IT omgeving te testen. Tijdens een pentest doen de Cyber Security professionals zich voor als hackers. Zij gaan opzoek naar kwetsbaarheden en zullen deze ook daadwerkelijk misbruiken om een omgeving binnen te dringen of anderszins te compromitteren.

Het eindproduct van een pentest, zoals Cuccibu die uitvoert, is een adviesrapport met daarin de bevindingen uit het onderzoek. Elke bevinding wordt vertaald naar een concreet bedrijfsrisico met daarbij advies over hoe dit risico het beste te mitigeren is. Op deze manier kan de organisatie meteen, met de juiste prioritering, aan de slag met verbeteringen.

Een pentest? Hoe werkt dat?

Een pentest kan in verschillende vormen worden uitgevoerd en op verschillende componenten van een IT omgeving. Het object van onderzoek kan de infrastructuur zijn, maar ook een specifieke applicatie of webapplicatie. Deze wordt getest op kwetsbaarheden.

Zoals in onderstaande figuur staat beschreven begint een pentest inhoudelijk met het verzamelen van informatie over het doelwit, zoals de gebruikte software en hoe de netwerkinfrastructuur eruit ziet. Vervolgens wordt er binnen het systeem gezocht naar kwetsbaarheden, dit kan geautomatiseerd of handmatig gedaan worden. De gevonden kwetsbaarheden worden vervolgens geanalyseerd en geëxploiteerd.

Alle bevindingen worden gedocumenteerd. Bij sommige bevindingen wordt een score gegeven om hiermee het risico van de kwetsbaarheid aan te geven.

cuccibu WHITEPAPER

Reduce Risk, Create Value

Aanpak en techniek

Onze aanpak is gebaseerd op een in de praktijk bewezen effectieve methode om de kwetsbaarheden te identificeren en op een adequate manier te adresseren. Er zijn drie typen **pentesten** die uitgevoerd kunnen worden, namelijk:

- **Black box pentest**. Dit type pentest kan vergeleken worden met een echte aanval op een specifiek systeem, zoals hackers deze zouden uitvoeren. De pentesters starten met het binnendringen van de systemen zonder enige voorkennis van uw systemen en applicaties.
- **Grey box pentest**. Bij dit type pentest, proberen de pentesters de systemen binnen te dringen. Dit doen zij zowel met als zonder informatie over de systemen of applicaties. De combinatie van beide scenario's geeft een zo compleet mogelijk beeld van de kwetsbaarheden binnen systemen of applicaties van jouw organisatie.
- **White box pentest**. Bij dit type pentest wordt alle informatie voorafgaand aan de pentest gedeeld met de pentesters om op deze manier gericht opzoek te gaan naar kwetsbaarheden in de systemen of applicaties. Denk hierbij aan toegang tot het interne netwerk of gebruikersaccounts van applicaties.

De meerwaarde van een pentest

Ons advies is dat iedere organisatie minimaal één keer per jaar een pentest uitvoert. Hiermee wordt diepgaand inzicht in de status van de huidige beveiliging van de omgeving behouden. Daarnaast stelt het de organisatie in staat om de beveiliging up-to-date te houden. Het up-to-date houden van de beveiliging is van essentieel belang omdat er vaak nieuwe kwetsbaarheden worden ontwikkeld en misbruikt. Daarnaast is een pentest een middel om vast te stellen of ingevoerde beveiligingsmaatregelen effectief zijn.

Voor een minder diepgaand, maar algemener, inzicht raden wij aan om een **vulnerability assessment** uit te voeren. In onderstaand figuur worden de verschillende soorten security assessments toegelicht, inclusief de bijbehorende werkzaamheden.

	Vulnerability Scan	Vulnerability Analysis	Vulnerability Assessment	Pentest	Red Teaming
Scope bepaling	X	X	X	X	X
Rapportage	X	X	X	X	X
Eindbespreking bevindingen	X	X	X	X	X
Automatische scan	X	X	X	X	X
Verificatie bevindingen		X	X	X	X
Handmatig onderzoek			X	X	X
Exploitatie				X	X
Social Engineering					X
Fysieke beveiliging					X

Benieuwd naar de Cyber Security van jouw organisatie?

Heeft u interesse in of vragen over een pentest? Of wil je meer weten over één van de andere security asessments? Onze consultants en pentesters helpen u graag!

Naast het uitvoeren van een pentest kunnen wij ook de volgende **Cyber Security** dienstverlening bieden:

- Netwerk monitoring (SIEM/SOC)
- **Phishing** (Email, SMS, Voice)
- Mystery guest
- OSINT
- Red Teaming

Neem vrijblijvend **contact** met ons op en we vertellen je graag over de mogelijkheden. Wij zijn te bereiken via 085-3032984 of **info@cuccibu.nl**