PENETRATIETESTEN; WAAR OP TE LETTEN?

Om te weten of je als organisatie goed bent beschermd tegen digitale aanvallen van buitenaf ('hacks') is het verstandig om je bescherming periodiek te laten testen. Dit kan bijvoorbeeld door een vulnerability scan te laten uitvoeren of een penetratietest (ook wel 'pentest'). Er zijn veel aanbieders van dergelijke testen, maar waar moet je nu op letten? Wanneer heb je bijvoorbeeld een pentest laten uitvoeren waar je enige zekerheid uit mag halen?

Er wordt vaak gesproken in de volgende soorten van pentesten:

AUDITTYPEN:

- Black Box: de auditor heeft geen kennis van het systeem, behalve naam, IP-nummer etc. van de testomgeving. De tester moet als buitenstaander het interne systeem benaderen en technieken toepassen die een echte hacker ook zou gebruiken.
- Grey box: de auditor beschikt over een login en voorkennis van de te testen systemen en kent de resultaten van de black box. Hij heeft geen login van de beheerders. Hiermee wordt onder andere geprobeerd hogere privileges te behartigen.
- White box/Crystal box: de auditor heeft volledige voorkennis van de omgeving. Het voordeel daarvan is dat hij zo de gevonden kwetsbaarheden kan valideren en nadere verdieping kan aanbrengen (dit wordt soms ook wel een 'vulnerability scan' genoemd).

Vervolgens wordt met auditniveaus de diepgang van de pentest aangeduid:

AUDITNIVEAUS:

- Niveau 1 (basisbedreigingen test): deze test simuleert een eenvoudige aanval meestal met behulp van gratis beschikbare tools.
- Niveau 2 (opportunistische bedreigingtest): deze gaat uit van een ervaren hacker die op een eenvoudige, maar gerichte wijze met automatische en handmatige middelen aanvallen uitvoert op willekeurige systemen.
- Niveau 3 (doelgerichte bedreigingentest): deze test simuleert een doelgerichte aanval op systemen door een ervaren hacker. Dit is de meest gekozen diepgang voor onder andere penetratietesten.
- Niveau 4 (geavanceerde bedreigingentest): deze test simuleert een aanval door een zeer ervaren hacker met uitgebreide middelen en mogelijkheden.

De audits worden normaliter in fasen uitgevoerd. Meestal wordt gestart met een voorbereiding om een beeld te krijgen van de netwerken en apparaten, etc. Vervolgens vinden de meer specifieke toetsen plaats. Hierbij dient te worden uitgegaan van o.a. de ISO 27001 en de ISO 18028 (standaard voor netwerkbeveiliging), conform de PTES (Penetration Testing Execution Standard). Webapplicaties dienen getest te worden op kwetsbaarheden die zijn opgenomen in de OWASP- en WASC-TC standaarden, waaronder 'SQL-injection', 'cross-site-scripting' en configuratiefouten in de website. Er wordt normaliter getest op ten minste 300 mogelijke kwetsbaarheden.

Simpele vuistregel is dat de kwaliteit van een pentest sterk wordt beïnvloed door de duur van de test (over welke periode mag de test worden uitgevoerd) en welke software-tools de pentester gebruikt ('hoe meer' is in dit geval vaak ook 'hoe beter').

Nu je wat meer zicht hebt op de wijze waarop je een pentest kunt vormgeven, ben je wellicht ook beter in staat je af te vragen wat jij voor je organisatie nodig hebt en wat dus wanneer bij jouw behoefte aan zekerheid past!

Alex Klaassen, IT Risk organisatie NewDay
newdayriskservices.nl