

Periodieke Penetratietest Informatiesystemen

Dienstbeschrijving Versie 1.2

Testen, testen en nog eens testen

Eén manier om inzicht te verkrijgen in de beveiliging van een informatiesysteem is het op gecontroleerde wijze te laten testen. Maar dan wel 'real-life': op een manier waarop een 'echte' aanvaller dat ook zou doen. Dit is een goed middel om nieuwe, of sterk gewijzigde, informatiesystemen te testen alvorens deze in productie te nemen. Het is evenwel van evengroot belang om gedurende de levensduur van een informatiesysteem met regelmaat te testen, zodat nieuwe kwetsbaarheden niet ongemerkt zorgen voor een verlaging van het veiligheidsniveau.

Specialisten van LBVD zijn thuis in deze dienstverlening middels de dienst Periodieke Penetratietest Informatiesystemen. Deze dienst is specifiek toegesneden op het veilig *opleveren* en veilig *houden* van (met name op maat ontwikkelde) informatiesystemen. Zoveel mogelijk wordt gewerkt met vaste doorlooptijden en derhalve vaste investeringen, opdat de testen optimaal in de projectplanning zijn op te nemen. In deze dienstbeschrijving wordt onze werkwijze toegelicht alsmede de mogelijkheden en kaders.

Standaard uitvoeringen

Om een consistent en herhaalbaar resultaat te behalen heeft LBVD de aanpak van haar (periodieke) penetratietesten gestandaardiseerd. Voor de Periodieke Penetratietest wordt de *Open Source Security Testing Methodology Manual* (OSSTMM) als leidraad gebruikt. Dit is een standaard op het gebied van penetratietesten welke tot stand is gekomen door de samenwerking van tientallen beveiligingsdeskundigen uit diverse landen (zie ook www.ise.com.org/osstmm). Daar waar het web-gebaseerde applicatie betreft maakt LBVD mede gebruik van de kennis en ervaring welke voortkomt uit het Open Web Application Security Project (OWASP).

Technische scope

Voor de goede orde: bij de Periodieke Penetratietest gaat het om het doorbreken van de *technische (ICT-)beveiliging* van het betreffende systeem. Er zijn evenwel meer zwakke plekken – zoals de mens die het informatiesysteem gebruikt. Ook hiervoor heeft LBVD mogelijkheden, denk bijvoorbeeld aan onze dienst MysteryGuest. Een MysteryGuest actie laat zich prima combineren met een (Periodieke) Penetratietest voor een breder zicht op de zaak en soms onvermoede bevindingen.

Doel van de Periodieke Penetratietest

De Periodieke Penetratietest heeft tot doel om, met een vooraf bepaalde frequentie, inzicht te krijgen en te houden in de mate waarin een bepaald informatiesysteem weerstand kan bieden aan pogingen om het te compromitteren.

Hierbij wordt een antwoord gezocht op de volgende specifieke vragen:

1. Is het mogelijk voor een willekeurig persoon om toegang tot het systeem te verkrijgen?
2. Is het mogelijk om, eenmaal binnengedrongen, toegang te verkrijgen tot vertrouwelijk materiaal of om anderszins schade aan te richten - al dan niet opzettelijk¹?
3. Kan een geautoriseerd persoon met beperkte toegangsrechten misbruik maken van de (wellicht meer uitgebreide) toegangsrechten van een ander geautoriseerd persoon?

Uitvoeringsvarianten

Een Periodieke Penetratietest kent verschillende uitvoeringsvarianten. Hierbij kan onder andere gedacht worden aan:

- Het perspectief van waaruit getest wordt: testen vanuit het perspectief van een interne medewerker (*privileged test*) of vanuit het perspectief van een aanvaller vanaf internet (*non-privileged*);
- De mate waarin de uitvoerend specialist informatie over het systemen krijgt: van *blackbox* (vrijwel geen voorinformatie) en *greybox* (enige voorinformatie) tot *crystalbox* (volledige openheid van zaken);
- *Intrusief*² of niet? M.a.w. als we een kwetsbaarheid of zwakke plek gevonden hebben, moeten we dan het feit noteren en onderzoeken naar de volgende, of wil de opdrachtgever dat we het lek ten volle proberen uit te buiten?

De exacte vorm waarin de test voor de opdrachtgever wordt uitgevoerd wordt vooraf tijdens een intakegesprek besproken. Uiteraard gebeuren acties welke de beschikbaarheid van informatiesystemen in gevaar kunnen brengen alleen in overleg met, en na toestemming van de opdrachtgever.

Aanpak

Start

De te onderhouden omgeving wordt door de opdrachtgever gedefinieerd in termen van IP adressen. Vervolgens inventariseert LBVD alle systemen en netwerk componenten (doelobjecten) in het aangegeven adresbereik en onderwerpt al deze componenten aan een eerste penetratietest. De resultaten van deze test worden aan de opdrachtgever gecommuniceerd en door LBVD bewaard.

¹In principe. Uiteraard zal worden getracht alleen het bestaan van de mogelijkheid aan te tonen, zonder daadwerkelijk schade aan te richten!

²Intrusief: op een wijze waarbij, al dan niet met gebruik van hulpmiddelen, wordt gepoogd kwetsbaarheden en/of zwakke plekken te benutten of uit te buiten, teneinde het bestaan onomstotelijk aan te tonen. Hoewel LBVD bij het testen zeer voorzichtig en zorgvuldig te werk gaat teneinde schade te vermijden, geeft intrusief testen een extra kans op storing en mogelijk schade.

vervolgcyclus

Daarna ontstaat een cyclus waarbij met een afgesproken regelmaat (bijvoorbeeld 1x per kwartaal) alle geïdentificeerde doelobjecten opnieuw worden getest. Hierbij wordt dan bepaald of:

- 1) alle eerder gevonden beveiligingslekken afdoende zijn gedicht;
- 2) er m.b.v. inmiddels nieuw ontwikkelde technieken of nieuw ontdekte kwetsbaarheden nieuwe beveiligingslekken zijn te vinden.

Keuring alvorens een nieuw systeem op te nemen

Indien een nieuw systeem (of verzameling systemen) wordt toegevoegd aan de te onderhouden omgeving of wanneer een systeem substantieel veranderd, doorloopt dit systeem eerst een initiële “keuring”, alvorens het mee kan lopen in de reguliere cyclus. Deze keuring bestaat uit een vast aantal checks en wordt uitgevoerd binnen een vast tijdbestek.

Afhankelijk van de aard en complexiteit van het systeem en/of de bevindingen van de keuring geeft LBVD al dan niet een “verklaring van geen bezwaar”. Deze verklaring geeft aan dat LBVD voldoende zekerheid heeft dat tijdens de keuring alle op het moment van keuren aanwezig zijnde gebreken gevonden zijn³.

Indien een “verklaring van geen bezwaar” wordt afgegeven kan het systeem direct mee gaan lopen in de periodieke cyclus. Indien LBVD geen “verklaring van geen bezwaar” afgeeft is aanvullend onderzoek nodig.

Opdrachtgever kan er voor kiezen om dit aanvullende onderzoek niet uit te laten voeren – evenwel accepteert zij daarmee het risico dat er nog (triviale) kwetsbaarheden in het systeem zitten die bij verder onderzoek bekend zouden kunnen worden. Hierbij vervalt op dat moment dan ook elke vorm van aansprakelijkheid jegens LBVD aangaande dat systeem.

Rapportage

Van iedere (deel)test ontvangt de opdrachtgever een testrapport. Hierbij wordt gewerkt met een gestandaardiseerde rapportage vorm, zodat de rapporten steeds goed vergelijkbaar zijn. Achtereenvolgens komt hierin aan bod:

1. Een beschrijving van de doelobjecten;
2. Een beschrijving van de uitgevoerde testen;
3. Per doelobject:
 - een statusoverzicht;
 - een beschrijving van de gevonden kwetsbaarheden;
 - aanbevelingen om deze kwetsbaarheden aan te pakken;
4. Een geconsolideerd overzicht van kwetsbaarheden, gerangschikt naar ernst.

Plaats van uitvoering

Afhankelijk van het doelobject zal uitvoering gedeeltelijk plaats moeten vinden op locatie van Opdrachtgever.

³Voorzover deze ontdekt zouden kunnen worden met tijdens het moment van keuren ter beschikking staande kennis en middelen.

Beperkingen

Een dergelijke test kent enkele beperkingen waar een 'echte' aanvaller zich doorgaans niet aan hoeft te storen. Wij hechten er belang aan de opdrachtgever hierop te wijzen, ook al laten sommige 'concullega's' dat liever achterwege. Denk hierbij aan de volgende aspecten:

Momentopname

LBVD kan slechts een uitspraak doen over de gesteldheid en 'fitness' van het doelobject cq. de doelobjecten ten tijde van de test. Het bevindingenrapport kent derhalve een beperkte geldigheid. Een kwaadwillige hacker zal zijn moment van toeslaan mede laten afhangen van het beschikbaar komen van informatie over nieuw ontdekte kwetsbaarheden en – mogelijk zelf ontwikkelde – hulpmiddelen om deze zwakke plekken uit te buiten. Zijn kans van slagen hangt af van de conditie van de systemen op dat moment.

Dit punt is natuurlijk vooral van belang voor éénmalig uitgevoerde testen. Dit is onder anderen de reden voor de ontwikkeling van een Periodieke Penetratietest. Voor dit product geldt dit punt in belangrijk mindere mate.

Opdrachtgever is met dit product behoorlijk meer **'in control'**

Beschikbaarheid middelen

Tijd is geld. De opdrachtgever betaalt onze tijd en dat budget is vaak beperkt. Daarmee is ook de tijd die wij aan het 'hacken' van systemen kunnen besteden beperkt. Een kwaadwillige echter, die niet door dit factoren gehinderd wordt, kan sporen volgen die LBVD gedwongen door de tijdbepanking (nog) onvoldoende aandacht heeft kunnen schenken.

Garantie

Een ieder die beweert harde garanties te kunnen geven omtrent de veiligheid van de systemen, dient de opdrachtgever met argwaan tegemoet te treden. Deels vloeit dit voort uit de vorige twee punten: de momentopname en de beperking van middelen. Maar belangrijker nog: het is simpelweg onmogelijk om aan te tonen dat iets niet kan.

Het is slechts mogelijk om met zekerheid aan te tonen dat iets *wel* mogelijk is: *door het te doen*. En daar doen wij onze uiterste best voor – dat garanderen wij, en onze tevreden opdrachtgevers. Vraag naar ons ervaringen overzicht.