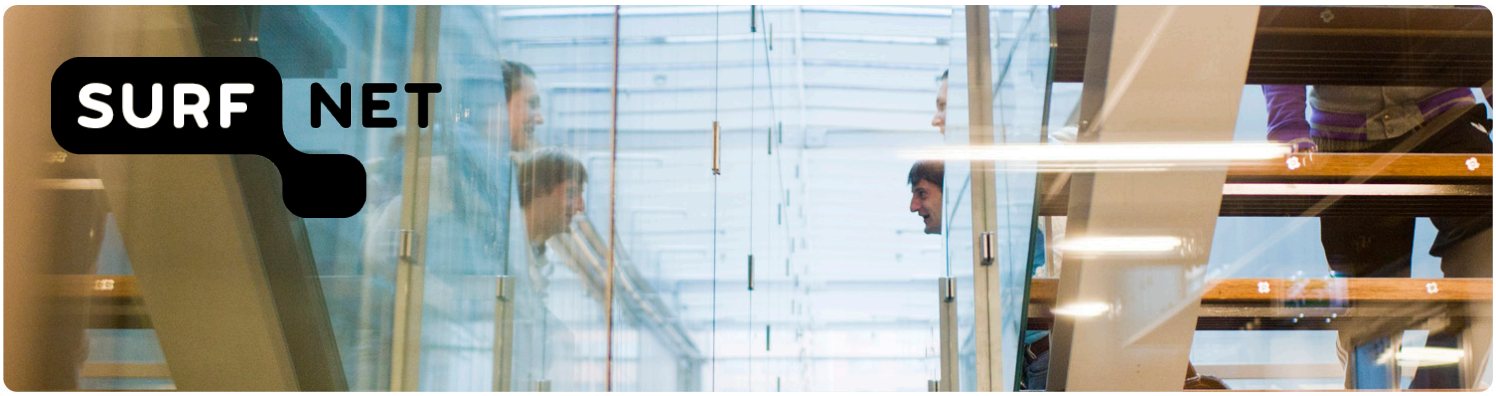


Whitepaper IT-beveiligingsonderzoeken

Auteur(s):	Madison Gurkha
Versie:	1.0
Datum:	18 maart 2016

Colofon

Dit document is geschreven door medewerkers van Madison Gurkha. Zij hebben vanuit hun specifieke functie kennis, praktijkervaring en voorbeelddocumenten ingebracht. Deze publicatie is mede mogelijk gemaakt dankzij: Walter Belgers, Tamara Brandt, Mark Braspenning, Arie van Boxsel, Ester van Dael, Remco Huisman, Arthur Korst en Arjan de Vet.

Inhoudsopgave

Managementsamenvatting

Dit document gaat in op verschillende aspecten van IT-beveiligingsonderzoeken. Hierbij is gekozen voor een pragmatische insteek waarbij theoretische kennis wordt gecombineerd met ervaringen uit de praktijk. De doelgroep van dit whitepaper zijn medewerkers van onderwijs- en onderzoeksinstellingen die betrokken zijn bij IT-projecten, zowel vanuit een operationele rol als een regiefunctie.

Waarom IT-beveiligingsonderzoek?

Wet- en regelgeving

Dit whitepaper gaat eerst in op redenen waarom instellingen technische IT-beveiligingsonderzoeken zouden willen of moeten uitvoeren. Er is wet- en regelgeving die dergelijke onderzoeken verplichten, zoals het DigiD normenkader. Als een instelling compliant wil zijn met normenkaders zoals ISO 27000, SURFaudit of NEN 7510/11, dan moeten periodiek beveiligingsonderzoeken worden uitgevoerd.

Risico's verlagen

Soms is er geen wettelijke verplichting, maar is het wel verstandig om te testen, bijvoorbeeld om het risico te verlagen om een datalek te moeten melden aan de autoriteit persoonsgegevens en wellicht een boete te krijgen.

Structurele aanpak

Het is aan te raden om te zorgen voor een structurele aanpak van IT-beveiligingsonderzoeken. In de praktijk blijkt vaak dat deze testen ad-hoc worden uitgevoerd of alleen periodiek (met een lage frequentie en beperkte scope). Het ontwikkelen van duidelijk beleid rondom IT-beveiligingstesten kan medewerkers houvast geven wanneer welke applicaties en IT-infrastructuren met welke frequentie en met welke methodiek zouden moeten worden getest. Naast deze periodieke testen moet ook worden nagedacht over het testen van nieuwe IT-projecten en Security by Design.

Lees meer in hoofdstuk 1.

Onderzoeksobjecten

Op welke onderzoeksobjecten zouden instellingen zich moeten richten bij IT-beveiligingstesten? De meeste aandacht gaat vaak uit naar IT-infrastructuur en (web)applicaties die vanaf het internet bereikbaar zijn. Er zijn echter meer risicogebieden. Het interne netwerk bijvoorbeeld en servers op dat netwerk met vertrouwelijke en/of privacygevoelige informatie. De meeste onderwijsinstellingen hebben een open karakter en het is erg moeilijk het interne netwerk fysiek te beschermen. Ook de mens - vaak de zwakste schakel - is een interessant onderzoeksobject.

Lees meer in hoofdstuk 2.

Soorten technisch onderzoek

Deze objecten zijn op verschillende manieren te onderzoeken. De bekendste test is de penetratietest. Hierbij wordt in een beperkte tijd gezocht naar bepaalde zwakheden en wanneer deze gevonden zijn, richt de tijd en energie zich in het gebruiken hiervan om zo diep mogelijk door te dringen (in een netwerk en/of applicatie). Black-, Grey- en Crystal-box onderzoeken brengen meer systematisch zoveel mogelijk zwakke plekken in kaart, zonder gericht te zijn op het misbruiken ervan. Bij de onderzoeken gebruiken testers veel tooling, maar zorgt hun ervaring en expertise voor meer

betrouwbare resultaten een meer gevonden risico's. Er kan ook puur automatisch "gescand" worden. Deze aanpak is geschikt voor (aanvullende) periodieke onderzoeken met een wat hogere frequentie.

Onderzoeken die gericht zijn op de mens staan bekend als social engineering. Instellingen kunnen met social engineering onderzoeken hoe medewerkers omgaan met USB-devices, phishing, telefonische verzoeken en hoe het gesteld is met de fysieke beveiliging. Een Red Teaming onderzoek gaat uit van de werkwijze van cybercriminelen: wat zijn de kroonjuwelen van een organisatie en hoe kunnen die worden bereikt met een mix van (geavanceerde) malware en social engineering. Een dergelijk onderzoek geeft een realistisch beeld van de kwetsbaarheid van een instelling, waarbij ook incident response en forensische paraatheid kan worden getest.

Lees meer in hoofdstuk 3.

Keuzehulp

In dit whitepaper is een keuzehulp opgenomen die instellingen ondersteunt bij het kiezen van bepaalde testen.

Lees meer in hoofdstuk 4.

Uitvoering van IT-beveiligingsonderzoek

Goede intake

Bij de uitvoering van testen komt het nodige kijken. In dit whitepaper wordt dit uitgebreid beschreven. Om een goed onderzoek uit te voeren, is allereerst een goede intake noodzakelijk. Bij dit whitepaper zijn intakeformuleren bijgevoegd die kunnen helpen bij het bepalen van de scope. De grootte en complexiteit van een omgeving in combinatie met het risicoprofiel bepalen hoeveel tijd aan een onderzoek zou moeten worden besteed. Bij het beoordelen van offertes van leveranciers van technische IT-beveiligingsonderzoeken speelt deze tijd een belangrijke rol. Hoe minder tijd, des te goedkoper het onderzoek maar ook hoe groter de kans op restrisico's. Het is aan te raden om leveranciers vooral ook te beoordelen op kwaliteitsaspecten.

Juridische afspraken

Vanwege het gebruiken van hacktechnieken tijdens beveiligingsonderzoeken, is het noodzakelijk om juridisch goede afspraken te maken tussen instelling en leverancier. Er moet expliciete toestemming door de instelling worden gegeven voor het onderzoek. Het uitvoeren van testen brengt bovendien kans op schade met zich mee, waar een leverancier niet voor aansprakelijk kan worden gesteld, behalve als er sprake is van grove nalatigheid en/of opzet. Als de te onderzoeken omgeving geen eigendom is van de instelling, maar van een derde partij, zoals een cloud- of SaaS-leverancier, dan moet ook deze derde partij expliciet toestemming geven en de leverancier te vrijwaren tegen schade. In dit white paper is een voorbeeld contract opgenomen die kan worden gebruikt tussen instelling en leverancier en een vrijwaringsverklaring voor derde partijen.

Rapportage over het onderzoek

Na uitvoering van het onderzoek volgt de rapportage. Eigenlijk begint het werk voor instellingen dan pas echt. De bevindingen uit het rapport moeten worden opgelost. Het is raadzaam dit goed te bewaken en het eindresultaat te laten hertesten of het herstel op de juiste manier is uitgevoerd en er een eindrapport ligt met een voldoende beoordeling.

Lees meer in hoofdstuk 5.

1 Waarom technische IT-beveiligingsonderzoeken?

In oktober 2014[1] is het Cyberdreigingsbeeld Sector Hoger Onderwijs en Wetenschappelijk onderzoek verschenen. In dit rapport worden 7 dreigingen onderscheiden.

- Verkrijging en openbaarmaking van informatie
- Identiteitsfraude
- Manipulatie van data
- Spionage
- Verstoring van ICT
- Overname en misbruik van ICT
- Bewust beschadigen imago

Het rapport geeft aan dat deze dreigingen reëel zijn en maakt de noodzaak voor preventieve, detectieve en reactieve maatregelen duidelijk. Het (laten) uitvoeren van technische IT-beveiligingsonderzoeken is een preventieve (en detectieve) maatregel waarmee IT-beveiligingsproblemen kunnen worden opgespoord zodat deze kunnen worden opgelost voordat bepaalde actoren hier misbruik van kunnen maken. Er kunnen verschillende actoren zijn, zoals eigen medewerkers, studenten, maar bijvoorbeeld ook andere (overheids)organisaties die spioneren of activisten.

Een organisatie of instelling zou in kaart moeten brengen welke IT-beveiligingsrisico's er zijn. Hierbij moet niet alleen gekeken worden naar de IT-middelen die reeds in gebruik zijn, maar ook naar de nieuwe IT-projecten die nog uitgevoerd gaan worden. Dit hoort bij goed bestuur en in veel gevallen ook bij wat gezien wordt als 'goed huisvaderschap' over vertrouwelijke en/of persoonlijke gegevens. Een student, patiënt of medewerker mag ervan uitgaan dat er zorgvuldig met zijn of haar gegevens wordt omgegaan. Ook mag een bestuur verwachten dat er zorgvuldig wordt omgegaan met onderzoeksresultaten uit R&D-inspanningen al dan niet in de vorm van "Intellectual Property".

In de praktijk blijkt het nog niet zo vanzelfsprekend dat organisaties intrinsiek gemotiveerd zijn om structureel IT-beveiligingsrisico's in kaart te brengen. Dit werd goed duidelijk tijdens Lektober in 2011. De maand oktober van dat jaar werd door Webwereld uitgeroepen tot Lektober. Hiermee werden IT-beveiligingsproblemen in veel websites aangekaart. Belangrijke doelwitten waren gemeentelijke DigiD websites, waarin bij veel gemeentes serieuze IT-beveiligingsproblemen aan het licht zijn gekomen. Lektober heeft ertoe geleid dat Logius de DigiD-audit in het leven heeft geroepen om daarmee een bepaald minimaal beveiligingsniveau af te dwingen. Elke organisatie die DigiD gebruikt voor de authenticatie op websites moet nu jaarlijks een DigiD-audit uit laten voeren (inclusief de benodigde technische IT-beveiligingsonderzoeken).

Audits en zelfscans worden vaak op basis van normenkaders uitgevoerd. Normenkaders zijn goed omdat ze houvast bieden en checklists geven om toe te werken naar een bepaalde mate van veiligheid. Het kan voor organisaties ook een valkuil zijn. Een organisatie met privacygevoelige gegevens in IT-systemen moet streven naar een zo veilig mogelijke omgeving. Het is mooi meegenomen dat dit ook een certificering en/of compliance met zich mee brengt. Gaat het echter alleen om het laatste, dan ligt de vinkjescultuur op de loer. Hoe gedegen een IT-beveiligingsonderzoek wordt uitgevoerd, des te groter is de kans dat er bevindingen zullen zijn. Die bevindingen kunnen certificering of compliance in de weg staan. De verleiding is dan groot om een

[1] Eind 2015 is een nieuwe versie van het cyberdreigingsbeeld verschenen.

minder goed onderzoek te laten uitvoeren door bijvoorbeeld een minder gespecialiseerde leverancier te kiezen en/of erg weinig tijd voor de onderzoeken vrij te maken. Dit is uiteraard een onwenselijk effect.

In Bijlage 1: Wet- en regelgeving en normenkaders toegelicht" worden de verschillende wet- en regelgeving op nationaal en Europees niveau kort belicht. Daarnaast worden normenkaders toegelicht waarin een verplichting tot het uitvoeren van technische IT-beveiligingsonderzoeken is opgenomen, dan wel onderdeel is van de norm. Tevens zijn in de bijlage een aantal technische normenkaders opgenomen die houvast kunnen bieden bij het veilig ontwikkelen en testen van applicaties en/of IT-infrastructuren.

Het is aan te raden dat organisaties zorgen voor een structurele aanpak van IT-security testen. In de praktijk blijkt vaak dat deze testen ad-hoc worden uitgevoerd of alleen periodiek (met een lage frequentie en beperkte scope). Het ontwikkelen van duidelijk beleid rondom IT-beveiligingstesten kan medewerkers houvast geven wanneer welke applicaties en IT-infrastructuren met welke frequentie en met welke methodiek zouden moeten worden getest. Naast deze periodieke testen moet ook worden nagedacht over het testen van nieuwe IT-projecten en Security by Design.

2 Onderzoeksobjecten

Instellingen maken vaak gebruik van een uitgebreide IT-infrastructuur. Deze bestaat niet uitsluitend uit een of meerdere koppelingen aan het netwerk, maar ook uit eigen netwerken, servers, laptops en steeds vaker andere mobiele apparatuur, maar in veel gevallen ook uit software die zelf ontwikkeld is of is aangekocht.

Om de veiligheid van (onderzoeks)gegevens te waarborgen geven we in dit hoofdstuk een overzicht van mogelijke onderzoeksobjecten die relevant kunnen zijn om (periodiek) aan een IT-beveiligingsonderzoek te (laten) onderwerpen.

2.1 IT-Infrastructuur

Er wordt onderscheid gemaakt tussen infrastructuur (netwerk, firewalls, generieke systemen) en applicaties, die gebruik maken van de infrastructuur. De grens is soms lastig te leggen. Hoort de Apache webserver bij de infrastructuur of de applicatie? Vaak zijn aparte groepen binnen organisaties verantwoordelijk voor de infrastructuur en applicaties en kan die scheiding ook bij beveiligingstesten aangehouden worden, zodat de rapportage gaat over het verantwoordelijkheidsgebied van maar één afdeling.

2.1.1 Intern netwerk

Voor veel instellingen is het erg moeilijk om de fysieke toegang tot het interne netwerk te beschermen. Universiteiten, Hogescholen en ziekenhuizen zijn namelijk organisaties met een ‘open’ karakter. Het is vrijwel niet uit te sluiten dat onbevoegden fysiek toegang krijgen tot het interne netwerk. Het is daarom aan te raden het interne netwerk te onderzoeken op IT-beveiligingsrisico’s.

Bij het onderzoek naar een intern netwerk is de premisse dat de aanvaller al toegang heeft tot dit netwerk (bijvoorbeeld door fysiek te koppelen, via wifi-verbindingen of via een geïnfecteerde werkplek). Bij aanvallen op het interne netwerk kan het gaan om een buitenstaander die fysiek toegang tot het interne netwerk heeft weten te krijgen, maar het kan ook gaan om gebruikers op het netwerk die ongeoorloofde acties uitvoeren, zoals bijvoorbeeld studenten die servers overnemen om illegale games en films uit te wisselen of die toegang willen krijgen tot de server met de studentendatabases.

Het doel van een onderzoek van een intern netwerk is om te kijken waar de zwakheden op het interne netwerk zich (voornamelijk) bevinden. Het is handig om vooraf te bedenken wat de 'kroonjuwelen' zijn die beveiligd moeten worden. Tijdens de test kan dat getracht worden deze kroonjuwelen te bemachtigen. Deze kroonjuwelen zijn bijvoorbeeld het studentvolgsysteem, het treasury systeem, intellectual property (bij universiteiten en onderzoeksinstituten) of de database met elektronische patiëntendossiers.

Het onderzoek kan vanuit verschillende uitgangspunten worden gestart, zoals:

- iemand met fysiek toegang tot het Kantoor Automatisering (KA) netwerk;
- iemand met een gebruikersnaam en wachtwoord voor het KA-netwerk;
- iemand met toegang tot een bepaald VLAN;
- iemand met remote toegang tot een werkstation.

2.1.2 Externe IT-infrastructuur/DMZ

De IT-infrastructuur die door middel van routeerbare IP-adressen op internet bereikbaar is, is een doelwit voor veel criminelen. Het is nuttig om na te gaan of de infrastructuur voldoende is gehardend, dus dat alle patches zijn aangebracht en geen onnodige services worden aangeboden. Bij dit onderzoek worden de IP-reeksen onderzocht die via internet bereikbaar zijn. De organisatie of instelling zal zelf de lijst met IP-reeksen moeten aanleveren. De juistheid van deze gegevens is bepalend voor een correcte scope (zie ook paragraaf 5.1). Bij de externe IT-infrastructuur is het verder van belang om na te gaan welke externe koppelingen er allemaal zijn. Dit zijn vaak niet alleen de IP-connecties. Uit het verleden zijn er vaak nog modemverbindingen, of een straalverbinding tussen 2 kantoren. Dit kunnen ook ingangen tot het interne netwerk zijn, die het overwegen waard zijn te onderzoeken.

2.1.3 Werkstations

Werkstations zijn door hun toegang tot het internet via de webbrowser erg kwetsbaar voor malware. Door het gebruik van verouderde software en bepaalde plug-ins voor de browser hoeft een besmette website alleen maar bezocht te worden om al een besmetting met malware op het werkstation op te lopen. Vanaf een besmet werkstation kan een aanvaller het interne netwerk bedreigen en heeft vanuit dat werkstation alle tijd om rustig op zoek te gaan naar de kroonjuwelen van een organisatie.

Hoe kwetsbaar is een werkstation gegeven de inrichting? Dit is een vraag die te beantwoorden is door een dergelijk systeem na te lopen op zaken zoals geïnstalleerde software, patch-level van alle software, gebruikerspermissies, opgeslagen wachtwoorden/hashes etc.

2.1.4 Wifi

Het gebruik van wifi biedt mensen toegang tot het netwerk. Zij hoeven hiervoor niet fysiek in het pand aanwezig te zijn. Voor gasten worden vaak aparte netwerken opgezet.

Er zijn verschillende vragen die bij het gebruik van wifi beantwoord moeten worden.

- Kan een gast verbinden met andere netwerken buiten het netwerk waar deze toegang toe zou moeten hebben?
- Kunnen gebruikers van het draadloze netwerk elkaar aanvallen?
- Kunnen ongeautoriseerde gebruikers toegang krijgen?
- Is het mogelijk gebruikers verbinding te laten maken met een door een aanvaller opgezet netwerk met als doel het bemachtigen van credentials?

Deze vragen kunnen worden beantwoord door een onderzoek waarbij deels gekeken wordt naar de configuratie van de wifi-componenten en deels door onderzoek dat wordt uitgevoerd met speciale wifi-apparatuur.

2.1.5 Mobiele devices

Mobiele devices worden steeds vaker ingezet om toegang te verkrijgen tot bepaalde netwerken en/of diensten. Wat nu, als een dergelijk device in verkeerde handen valt? Het is mogelijk te onderzoeken wat er aan gegevens achterblijft op een mobiel device en in hoeverre die gegevens misbruikt kunnen worden om toegang te krijgen. Dit geeft inzicht over het risico dat men loopt bij het gebruik van mobiele devices voor netwerktoegang.

2.1.6 Firewalls

Firewalls blokkeren bepaald verkeer. Om te zien of dit inderdaad werkt zoals verwacht, kan een onderzoek uitgevoerd worden. Daarbij kan de ruleset onderzocht worden. Er moet dan wel duidelijk

zijn welke verkeersstromen toegestaan zouden moeten zijn. Door deze review komen fouten, vergissingen, oude regels en dergelijke aan het licht. Daarnaast kan een netwerkscan gebruikt worden om te zien of de rulesets actief zijn en of de firewall correct omgaat met ongebruikelijk netwerkverkeer. Hiermee kan dus inzicht verkregen worden in hoe goed de firewall het werk doet waar hij voor bedoeld is.

2.2 Applicaties

2.2.1 Webapplicaties

Tegenwoordig worden de meeste applicaties als webapplicatie gebouwd. De fouten die hierin worden gemaakt zijn vaak invoervalidatiefouten (zie ook paragraaf 7.3.1 over OWASP), maar er zijn ook meer subtiele problemen. Dit zijn bijvoorbeeld logische problemen waar uitgebreid onderzoek voor nodig is om deze aan het licht te brengen. Een webapplicatieonderzoek kan met of zonder login-gegevens worden uitgevoerd. Typische webapplicaties die een IT-beveiligingsonderzoek verdienen zijn bijvoorbeeld:

- extranetportals (studenten/patiënten/leveranciers)
- interne webapplicaties (hrm/intranet)

2.2.2 Fat clients

Fat clients (veelal Windows en Java applicaties die vanaf de desktop opgestart worden) communiceren vaak met een back-end. (stand-alone applicaties zijn voor wat betreft beveiliging minder interessant.) Deze communicatie wordt in paragraaf 2.2.3 verder toegelicht. De fat client kan zelf ook nog gegevens opslaan, al dan niet versleuteld. Het onderzoek kan zich richten op deze gegevens en proberen om, met behulp van reverse engineering, uit te zoeken hoe goed de gegevens lokaal beveiligd worden.

2.2.3 Webservices

Communicatie tussen twee partijen of software gebeurt vaak via Webservices. Deze webservices (en fat clients) maken veelal gebruik van protocollen zoals SOAP of REST en datamodellen zoals XML en JSON. Het is interessant om te zien hoe de beveiliging in deze protocollen is geregeld. Aangezien het - vanwege het ontbreken van een user interface - lastiger is om de communicatie van webservices te onderscheppen en manipuleren, wordt hier vaak ook minder aan beveiliging gedaan. Afhankelijk van het gebruikte protocol is het meer of minder eenvoudig om het te onderzoeken door het verkeer aan te passen. Er kan dan (deels) ook naar de inrichting van de configuratie van de webservices software worden gekeken.

2.2.4 Mobiele applicaties

Bij mobiele applicaties is de communicatie met de back-end (via SOAP of REST) vaak een belangrijk onderdeel, zie paragraaf 2.2.3. Een interessante vraag is hoeveel data achterblijft op het mobiele device (zie ook paragraaf 2.1.5). Het is mogelijk voor een specifieke applicatie te testen welke gegevens achterblijven op smartphone of tablet. Dat kunnen interne databases zijn, maar ook tijdelijke gegevens en zaken zoals screenshots die het besturingssysteem maakt als een applicatie gepauzeerd wordt.

2.3 De mens

Er is een constante wapenwedloop aan de gang tussen aanvallers en verdedigers. Het punt is bereikt dat aanvallen op de mens vaak effectiever zijn dan die op de techniek. Zelfs zo effectief, dat de meeste van deze aanvallen uiteindelijk succesvol zullen zijn. De vraag is dan wat het nut is van een

dergelijk onderzoek, wanneer de uitkomst vooraf al bekend is? Het onderzoek is vooral relevant als een onderdeel van een bewustwordingscampagne, waarbij herhaald allerlei tests worden uitgevoerd. De mens kan op een aantal manieren worden aangevallen. Zo kan de mens gebruikt worden om bijvoorbeeld toegang te krijgen tot fysieke locaties, zoals kantoren of datacenters. Ook kunnen mensen worden uitgenodigd om te klikken op een link in een e-mail of zelfs hun netwerk credentials in te geven op een website. Op een vergelijkbare manier worden mensen verleid een USB device aan te sluiten op hun computer of om telefonisch meer informatie te geven dan verstandig is. Aanvallen op de mens staan bekend als social-engineeringaanvallen (zie ook paragraaf 3.8).

3 Soorten technische IT-beveiligingsonderzoeken

Technische IT-beveiligingsonderzoeken zijn er in verschillende vormen en maten en uit te voeren op verschillende onderzoeksobjecten (zie hoofdstuk 2). Het soort onderzoek hangt natuurlijk af van een aantal zaken, zoals wanneer het wordt uitgevoerd (als de omgeving al is opgeleverd of eerder), welk onderdeel of risico getest wordt (een hacker die het systeem aanvalt, of iemand die met behulp van social engineering een gebruiker aanvalt) en hoe uitgebreid/diep er onderzocht moet worden (met of zonder broncode) of toegang tot configuraties van systemen.

In dit hoofdstuk worden een aantal mogelijke aanpakken van IT-beveiligingsonderzoeken beschreven. Het hoofdstuk wordt afgesloten met een keuzehulp die kan helpen bij het vinden van de juiste aanpak.

3.1 Automatisch scannen

Tijdens een geautomatiseerde scan worden systemen getest door te achterhalen of er software met reeds bekende kwetsbaarheden draait. Hiertoe bevat de scansoftware een database met mogelijke kwetsbaarheden. Tests om te zien of die kwetsbaarheden daadwerkelijk aanwezig zijn, kunnen bestaan uit het opvragen van een versienummer of het uitvoeren van een 'exploit'. Voordat de tool gebruikt wordt, moet deze worden voorzien van de meest recente kwetsbaarheden-database.

Voordelen

- Snel
- Goedkoop

Nadelen

- Niet volledig
- Grote kans op false positives wanneer de resultaten niet met de hand worden nagelopen
- Een geautomatiseerde tool kan alleen (relatief) eenvoudige problemen kan detecteren. Problemen zoals met een logische flow in een webapplicatie kan door een geautomatiseerde scan vaak niet gedetecteerd worden.

3.2 Design review (Security by Design)

Een design review is een onderzoek waarbij niet daadwerkelijk een werkend systeem wordt onderzocht. In plaats daarvan, wordt het ontwerp bekeken en beoordeeld. Bij deze aanpak wordt de ontwerpdocumentatie doorgenomen en worden daarna interviews afgenomen met architecten en/of ontwikkelaars. Dit, omdat het ontwerp vaak niet voldoende details bevat en ook niet altijd duidelijk maakt welke ontwerpbeslissingen er gemaakt zijn. Bij een design review wordt gekeken naar de inrichting van een systeem, een netwerk, een appliance, software etc. De toetsing vindt plaats aan de hand van best practices of van vooraf aangeleverde normen. Het betreft hier de beoordeling van de ‘opzet’ van een omgeving. Een design review kan worden uitgevoerd op zowel bestaande omgevingen als omgevingen die nog moeten worden gerealiseerd.

Security by design staat voor een benadering van IT-beveiliging waarbij getracht wordt vóór de bouw van een applicatie of een IT-omgeving de beveiliging van meet af aan mee te nemen, in plaats van te proberen het achteraf toe te voegen. Design reviews maken vaak deel uit van Security by Design en wordt vaak aangevuld met korte IT-beveiligingstesten tijdens het gehele bouwproces. Ook wordt tijdens een project vaak een IT-beveiligingsspecialist aangewezen die een goede IT-beveiliging moet borgen. De technische normenkaders zoals vermeld in paragraaf 7.2 kunnen hierbij worden gebruikt.

Voordelen

- In korte tijd kunnen beoordelen van relatief grote en complexe omgevingen.
- Preventief (voor omgevingen die nog gerealiseerd moeten worden).

Nadelen

- Een papieren onderzoek. Er vindt geen controle plaats van de werking van de omgeving.
- Het geeft geen uitsluitsel over de beveiliging van een omgeving.

3.3 Black-box

Bij een black-box-aanpak wordt vooraf geen enkele informatie verstrekt, met uitzondering van welk systeem (applicatie en/of infrastructuur) onderzocht moet worden. De consultants zullen alles zelf moeten uitvinden. Hierdoor geeft het onderzoek, in beginsel, een goed inzicht in wat een aanvaller vanaf het internet kan bereiken zonder verdere voorkennis en zonder legitieme toegang.

Black-box-tests worden vaak in een beperkte tijd uitgevoerd, een tijd die veelal korter is dan de tijd die aanvallers bereid zijn in een aanval te steken. Het gaat daarbij niet alleen om de daadwerkelijke inspanning, maar ook om de doorlooptijd. Een aanvaller zal bijvoorbeeld een kwetsbaarhedenscan heel langzaam kunnen laten verlopen, zodat bepaalde Intrusion Prevention-maatregelen niet in werking treden. Een consultant die maar een beperkte tijd heeft, kan hier niet omheen werken. In de praktijk worden dit soort maatregelen daarom vaak (tijdelijk) uitgeschakeld voor de consultants (zie ook paragraaf 5.6.4).

Voordelen

- Vaak een kortere doorlooptijd en kosten voor onderzoek dan bij de grey- of crystal-box-aanpak

Nadelen

- Mogelijk worden er minder kwetsbaarheden gevonden dan bij een grey- of crystal-box onderzoek.
- Kwetsbaarheden die zich achter een inlog-scherm bevinden kunnen niet gevonden/gerapporteerd worden. Denk hierbij aan sommige kwetsbaarheden zoals beschreven in de OWASP top 10 (zie paragraaf 7.3.1).

3.4 Grey-box

Bij een grey-box-aanpak worden vooraf login-gegevens verstrekt aan de consultants. Hierdoor kan een inzicht worden verkregen in de kwetsbaarheden die mogelijk uitgebuit kunnen worden door gebruikers die legitiem toegang tot een systeem, netwerk of applicatie hebben. Alle onderzoeken die in een black-box-aanpak worden uitgevoerd, worden eveneens in een grey-box-aanpak uitgevoerd. Hieronder valt bijvoorbeeld het onderzoek of het inloggen voor niet-geautoriseerde gebruikers te omzeilen is.

Voordelen

- Een applicatie kan beter beoordeeld worden op kwetsbaarheden dan bij de black-box-aanpak. Denk hierbij aan autorisatiecontroles, Cross-site-scripting, Cross-site-request-forgery, SQL-injectie, etc (zie paragraaf 7.3.1 OWASP top 10).

Nadelen

- Er is meer tijd nodig om de applicatie te onderzoeken dan bij een black-box onderzoek.

3.5 Crystal-box

Bij een crystal-box-aanpak wordt volledig inzicht gegeven in de werking van het te onderzoeken systeem. Er wordt dan bijvoorbeeld beheer-toegang verstrekt tot servers en de broncode van een applicatie wordt ter beschikking gesteld. Vragen over de inrichting worden door architecten, ontwikkelaars of beheerders beantwoord. Hierdoor kunnen die onderdelen van de omgeving beoordeeld worden, waar anders geen toegang tot zou zijn.

Voordelen

- Een beter inzicht in kwetsbaarheden in applicaties en systemen.
- Controle op backdoors.
- Door niet alleen de eerste laag van beveiliging te onderzoeken, maar ook onderliggende lagen, kan een crystal-box-onderzoek van onderliggende systemen ook een aanvulling zijn op applicatie-onderzoeken.

Nadelen

- Er is meer tijd nodig voor onderzoek dan bij een grey box aanpak.

3.6 Code review/inspectie

Tijdens een code review/inspectie wordt op basis van een controle van de beschikbaar gestelde broncode van een applicatie een oordeel geveld over de applicatie/code.

Tijdens een code inspectie wordt naast een werkende applicatie ook de broncode aangeleverd om zo op basis van de code eventuele bevindingen te kunnen verifiëren. Het betreft hier geen volledige code review, maar controle van (belangrijke) delen van de code.

De code kan ook volledig gereviewd worden. Vaak wordt dan bij (zeer) veel code handmatig bepaalde delen onderzocht en de volledige code met behulp van automatische tooling.

Voordelen

- Tijdens een code review/inspectie kan met grote zekerheid worden vastgesteld of kwetsbaarheden op de juiste manier worden voorkomen. Denk hierbij aan het gebruik van de juiste escaping bij alle invoervelden in de applicatie, het gebruik van geparametriseerde queries, etc.
- In plaats van het nemen van steekproeven kan de gehele code gecontroleerd worden op mogelijke kwetsbaarheden.

Nadelen

- Een volledige code review is vaak een tijdrovend onderzoek.

3.7 Penetratietesten

Bij een black/grey/crystal-box-onderzoek gaat het vooral om het vinden van zoveel mogelijk kwetsbaarheden en hierover te rapporteren. Tijdens een penetratietest is het de bedoeling om een of meer kwetsbaarheden te vinden en die ook daadwerkelijk uit te buiten.

Voordelen

- De opdrachtgever krijgt onomstotelijk bewijs dat een hacker kan inbreken/misbruik kan maken van de gevonden kwetsbaarheden.

Nadelen

- Het (laten) uitvoeren van een penetratietest kan gevolgen hebben voor de beschikbaarheid van systemen. Mogelijk kan een penetratietest productieverstoringen tot gevolg hebben.
- Het kan voorkomen dat een penetratietest niet succesvol blijkt binnen de vooraf afgegeven time-box. Dit wil niet zeggen dat de omgeving daadwerkelijk veilig is. Een penetratietest is er namelijk niet op gericht om volledig te zijn.

3.8 Social engineering

Een social engineering aanval richt zich niet direct op de techniek, maar op wat vaak de zwakke schakel in de keten is, namelijk de mens. Tijdens een aanval zal een hacker proberen toegang te krijgen tot vertrouwelijke informatie. Hier worden 4 verschillende soorten social engineering aanvallen/onderzoeken toegelicht:

3.8.1 Phishing

Phishing kan worden ingezet om grote groepen mensen in aanraking te laten komen met de test (die daarna in de bewustwordingscampagne gebruikt kan worden). In samenspraak met de organisatie of instelling wordt een scenario bedacht waarbij gebruikers een e-mail krijgen met daarin een link en/of een attachment. Er kan apart gerapporteerd worden over hoeveel mensen op de link hebben geklikt en hoeveel mensen op de bijbehorende website ook hun credentials hebben ingegeven.

3.8.2 Telefonisch

Bij deze vorm van social engineering wordt telefonisch contact opgenomen met een afdeling of specifieke personen. Het doel hierbij is om deze mensen over te halen om telefonisch gevoelige informatie te delen zoals gebruikersnaam en wachtwoord, maar het is ook mogelijk om te proberen bepaalde 'kroonjuwelen' te bemachtigen

3.8.3 USB

Hoe makkelijk is het om een interne PC te infecteren? Hiertoe worden USB-gadgets verspreid die een stuk elektronica bevatten die de PC proberen te infecteren. Hierbij worden USB-sticks op locatie achtergelaten of als gadget naar personen verstuurd. Zowel de USB-stick als het gadget zijn dusdanig geprepareerd dat als deze gebruikt worden in een PC of laptop dat er code execution plaats vindt. In de regel zal er slechts een verbinding worden opgezet in plaats van dat de PC geïnfecteerd wordt, dit in verband met het extra werk en risico dat daaraan gekoppeld is, terwijl in beide gevallen wordt aangetoond dat het kan.

3.8.4 Fysiek

Hoe makkelijk is het om ergens binnen te komen? Door middel van social engineering kan men onderzoeken of het lukt om de instelling in te komen of om te komen op plaatsen binnen een instelling die niet openbaar zijn, zoals bijvoorbeeld rekencentra, operatiekamers of onderzoekslaboratoria.

Onder fysieke social engineering worden alle acties verstaan die nodig zijn om lijfelijk toegang tot ruimtes met vertrouwelijk informatie te verkrijgen. Dit gebeurt onder meer door tailgating (met iemand door de beveiliging heen lopen) en het tijdelijk aannemen van een andere identiteit.

Voordelen

- Het IT-beveiligingsbewustzijn van grote groepen personen kan relatief eenvoudig worden getoetst.

Nadelen

- De effecten van de uitkomst van een social engineering aanval zijn van relatief korte duur.
- Voor een meer blijvend effect moeten de aanvallen op regelmatige basis worden herhaald.

3.8.5 Red teaming

Een red teaming onderzoek richt zich niet op een bepaalde applicatie of (deel van) een infrastructuur. Dit onderzoek richt zich juist op de kroonjuwelen van een organisatie. Er wordt hierbij gericht geprobeerd toegang te krijgen tot de belangrijkste bedrijfsgegevens door gebruik te maken van de weg van de minste weerstand, uitgaande van de denk en werkwijze van actoren die uit zijn op bepaalde kroonjuwelen van een organisatie.

Een red teaming onderzoek bestaat uit een combinatie van zowel technische (voornamelijk black-box) als social engineering onderzoeken. De te volgen scenario's worden vooraf overlegd met de opdrachtgever. De opdrachtgever bepaalt uiteindelijk hoe ver hij of zij wil gaan met het onderzoek.

Voordelen

- Het onderzoek wordt uitgevoerd op de wijze waarop een kwaadwillende hacker een aanval zou uitvoeren.
- Organisaties kunnen op basis van deze aanval ook meten hoe goed monitoring en detectie werken en wat er van de aanval in de verschillende systemen is terug te zien (forensic readiness).
- Een red teaming aanval kan gecombineerd worden met het oefen van het incident respons plan.

Nadelen

- De omgeving wordt niet volledig onderzocht en ook niet alle kwetsbaarheden zullen worden gevonden. Tijdens het onderzoek wordt namelijk alleen de weg van de minste weerstand gevolgd.

3.9 DigiD-audit

Logius heeft naar aanleiding van "lektober" in 2011 verplicht gesteld dat alle applicaties die gebruikmaken van DigiD getoetst moeten worden tegen een door Logius opgestelde norm. Deze norm bestaat uit 28 technische en procedurele punten. Tijdens een technisch IT-beveiligingsonderzoek kunnen een aantal van deze punten getest worden. Een EDP-auditor zal de overige (procedurele) punten toetsen en uiteindelijk een rapport opleveren aan de klant. Dit rapport wordt door de opdrachtgever opgeleverd aan Logius. Per DigiD aansluiting moet er één rapport worden opgeleverd. Zie ook paragraaf 7.1.3.

Opmerking:

Logius heeft (tot op heden) nog niet bepaald hoe er om wordt gegaan met groepsaansluitingen.

4 Keuzehulp voor de test

De onderstaande richtlijnen kunnen worden gehanteerd bij de keuze welk type onderzoek het beste past bij de te onderzoeken omgeving.

Dit white paper biedt twee manieren om vast te stellen welke soort onderzoek voor welke omgeving instellingen het beste kunnen kiezen. De eerste manier betreft een tabelvorm op basis waarvan de keuze kan worden bepaald. Dit is handig wanneer men de redenatie start vanuit (kwetsbare) data of gegevens met een bepaalde classificatie. De tweede vorm is een keuzeschema die start vanuit het doel en het systeem. Dit schema leidt instellingen met behulp van vragen naar een bepaalde test toe.

In beide gevallen betreft het globale richtlijnen, die slechts op hoofdlijnen helpen bij het maken van een keuze. Bij twijfel is het aan te raden om altijd te kiezen voor de beste test (als dat budgettair haalbaar is).

4.1 Risicoprofielen

Applicatie en infrastructuren kunnen worden ingedeeld in een 6-tal risicoprofielen. Risicoprofiel 1 is het profiel met het hoogste risico en risicoprofiel 6 het laagste. Bij risicoprofiel 1 is het risico groot vanwege een of meer factoren die een rol kunnen spelen, bijvoorbeeld als er sprake is van bijzondere persoonsgegevens. Bijzondere persoonsgegevens betreffen informatie over onder andere iemands ras, godsdienst of gezondheid. Ook afbreukrisico's, imagoschade de grootte van gebruikersgroepen spelen een rol. Applicaties waarin niet ingelogd hoeft te worden bevatten daarnaast meestal ook geen vertrouwelijke gegevens.

Veel organisaties hanteren ook een zogenaamde BIV classificatie. BIV staat voor: Beschikbaarheid, Integriteit en Vertrouwelijkheid. Een score van B:3, I:3 en V:3 betekent dat Beschikbaarheid, Integriteit en Vertrouwelijkheid zeer veel aandacht verdient, dit in tegenstelling tot een score van: B:1 I:1 en V:1. Ook indicatieven BIV scores zijn in onderstaande tabel opgenomen.

Risicoprofiel 1: Hoog	**Risicoprofiel 2: Hoog**	**Risicoprofiel 3: Hoog**
Bijzondere persoonsgegevens	Privacy gevoelige gegevens	Privacy gevoelige gegevens
Groot afbreukrisico	Groot afbreukrisico	Laag afbreukrisico
Grote Imagoschade	Grote Imagoschade	Imagoschade
Multi-tenant	Grote groepen gebruikers	Grote groepen gebruikers
Grote groepen gebruikers	Applicatie Login	Applicatie Login
Applicatie Login	BIV: 1/2/3,2,3	BIV: 1/2/3,2,2
BIV: 1/2/3,3,3		

Risicoprofiel 4: Midden	Risicoprofiel 5: Laag	Risicoprofiel 6: Laag
Privacy gevoelige gegevens Laag afbreukrisico Weinig Imagoschade Kleine groepen gebruikers Applicatie Login BIV: 1/2/3,1,2	Laag afbreukrisico Weinig Imagoschade Geen Applicatie Login BIV: 1/2/3,1,1	Geen afbreukrisico Geen Imagoschade Geen Applicatie Login BIV: 1/2/3,1,1

4.2 Applicatieonderzoeken

Voor nieuwe applicaties (inclusief bijhorende IT-infrastructuur) met hoge risicoprofielen is het aan te raden deze te onderzoeken met de methode waarmee de meeste risico's geïdentificeerd kunnen worden: de Crystal box aanpak, waarbij de code ook beschikbaar is. Applicaties met een gemiddeld risicoprofiel kunnen eventueel ook onderzocht worden met de Grey box aanpak. Is er geen sprake van een login, dan is de Black box aanpak over het algemeen voldoende. Voor grote en complexe applicaties met een hoog risicoprofiel kan het raadzaam zijn om een design review uit te voeren.

Risicoprofiel	Black box	Grey box	Crystal box	DR/SbD*
Profiel 1 (Hoog)			X	X
Profiel 2 (Hoog)			X	X
Profiel 3 (Hoog)		X	X	X
Profiel 4 (Midden)		X		
Profiel 5 (Laag)	X			
Profiel 6 (Laag)	X			

* Design Review/ Security by Design

Bovenstaande indeling kan in ieder geval gebruikt worden voor nieuwe applicaties. Het is raadzaam om bestaande applicaties ook periodiek te (laten) onderzoeken. Het is afhankelijk van de aard en hoeveelheid van de wijzigingen en toevoegingen welke methodiek het beste kan worden gebruikt. Voor de risicoprofielen 1, 2 en 3 blijft een crystal box onderzoek aan te bevelen, tenzij er hoegenaamd niets aan een applicatie is gewijzigd in een bepaalde periode.

4.3 Infrastructuuronderzoeken

Voor IT-infrastructuren die nieuw worden opgeleverd kan eenzelfde indeling worden gebruikt zoals hiervoor vermeld voor applicaties. In veel gevallen zal er ook sprake zijn van een integraal project waarbij zowel een nieuwe applicatie wordt ontwikkeld als de bijhorende IT-infrastructuur. Voor hogere

risicoprofielen moet dan echt naar de inrichting van systemen worden gekeken en dus de Crystal box methode worden toegepast.

Bij bestaande infrastructuur die vanaf het internet bereikbaar is, is het aan te raden om periodiek onderzoek te laten verrichten via de Black box methodiek eventueel gecombineerd met automatische scanning met een wat hogere frequentie.

Het interne netwerk kan periodiek worden onderzocht door middel van een penetratietest en Black box test van de infrastructuur eventueel gecombineerd met automatische scanning.

Samenvattend:

Target	**Onderzoek**
Internetfacing ip-adressen	Black-box-infrastructuuronderzoek Automatische scanning
Inrichting van systemen/DMZ	Crystal-box-infrastructuuronderzoek
Onderzoek intern netwerk	Penetratietest van het intern netwerk Black-box-infrastructuuronderzoek Automatische scanning

4.4 Overige onderzoeken

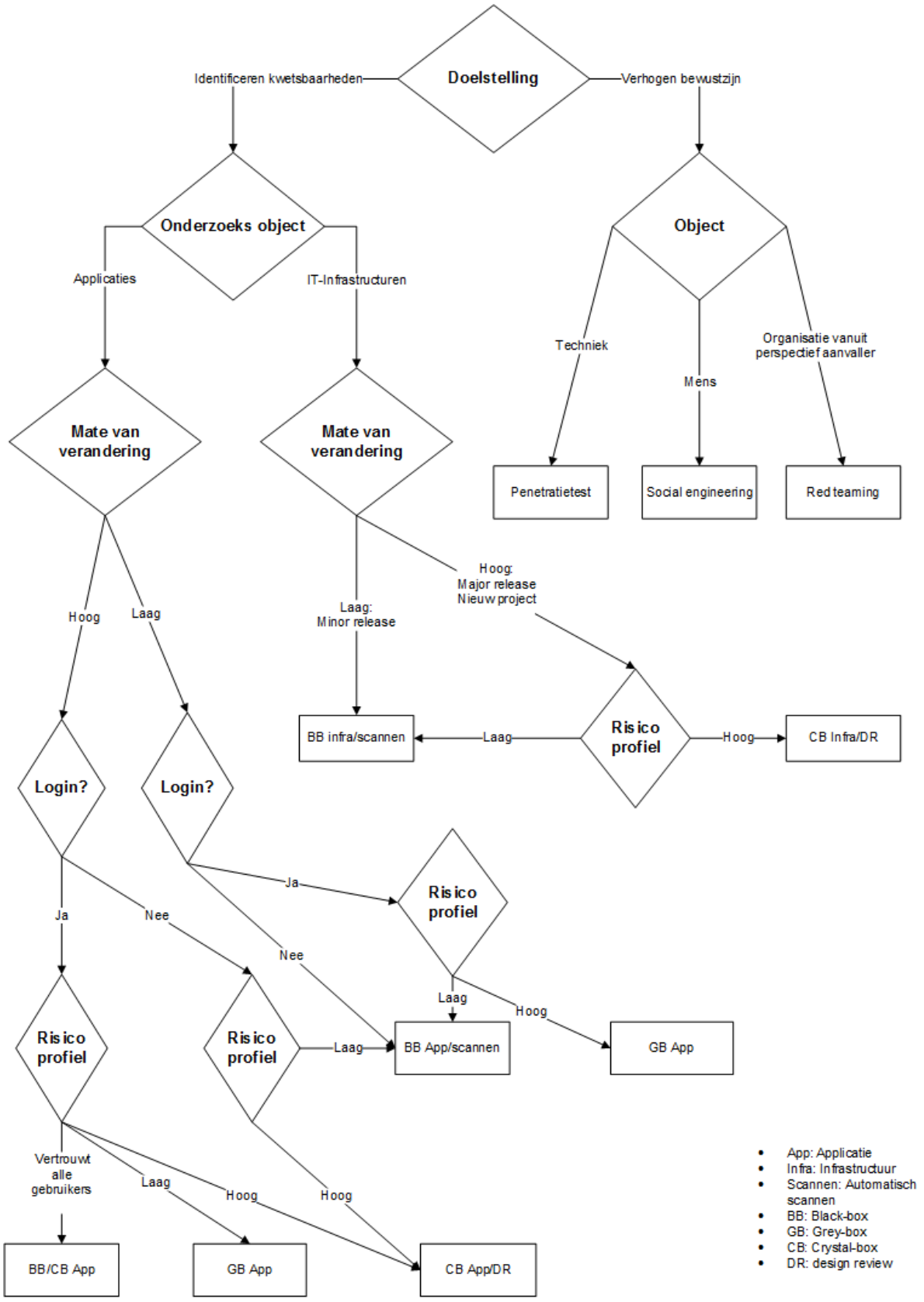
Voor het onderzoeken van de mens als zwakke schakel is een social engineering onderzoek geschikt. Er kan dan een keuze worden gemaakt tussen fysieke, USB, phishing en telefonische social engineering. Zoals al gezegd, is het verstandig om social engineering onderzoeken te combineren met een bewustwordingscampagne.

Het is het overwegen waard om een keer in de paar jaar een Red Teaming onderzoek uit te laten voeren. Hiermee test uw organisatie hoe een aanval vanuit het perspectief van een of meer actoren gericht op de kroonjuwelen van de organisatie zou kunnen verlopen. Losse testen op verschillende onderzoeksobjecten zijn buitengewoon nuttig, maar kennen toch een zeker beperking, die niet speelt bij een Red Teaming onderzoek.

Maakt uw organisatie gebruik van DigiD, dan moeten de volgende onderzoeken periodiek (jaarlijks) worden uitgevoerd:

- DigiD-audit
- Penetratietest
- Black box scan

4.5 Keuzeschema



In bovenstaande figuur is een alternatieve manier opgenomen om te assisteren bij de keuze voor een bepaalde test. In dit keuzeschema speelt ook bovenstaande tabel met de risicoprofielen een rol.

Allereerst wordt gevraagd naar de doelstelling. Als de doelstellingen is het verhogen van de het bewustzijn, dan komt men uit bij testen als Red Teaming, Social Engineering en Penetratietesten. Deze testen inventariseren namelijk geen kwetsbaarheden in de breedte, maar laten zien hoe een of meer kwetsbaarheden kunnen worden uitgebuit. De uitkomst hiervan kan worden gebruikt om het veiligheidsbewustzijn van medewerkers te verhogen.

Is het de doelstelling om systematisch alle kwetsbaarheden in kaart te brengen, dan maakt het schema vervolgens onderscheidt tussen IT-infrastructuren en applicaties. Vervolgens wordt in beide gevallen gevraagd naar de mate van verandering. Een project dat volledig nieuwe gerealiseerd wordt, moet beter worden onderzocht, dan een bestaande situatie waarin maar een kleine wijziging wordt doorgevoerd. Soms zijn de aard en het aantal van de wijzigingen weer dusdanig, dat feitelijk kan worden gesproken van een nieuwe situatie, die dus ook passende testen verdient.

Bij applicaties is het vervolgens de vraag of er sprake is van een login naar een besloten gedeelte van de site of niet. Als er sprake is van een besloten site, is het vrijwel altijd een goed idee om te testen met credentials (ook wel grey box; zie paragraaf 3.4).

Bij zowel applicaties als IT-infrastructuren is het vervolgens de vraag welk risicoprofiel het betreft. Als er sprake is van een laag risico is, kan worden volstaan met een eenvoudige test en hoe meer risico, des te beter de test moet zijn. Het is dan ook aan te bevelen al in het ontwerp echt rekening te houden met IT-security aspecten (Security by design / Design review; zie paragraaf 3.2). Voor het bepalen van het risico, kan bovenstaande tabel als uitgangspunt worden genomen.

5 Uitvoering van testen

Dit hoofdstuk beschrijft wat er komt kijken bij het laten uitvoeren van IT-beveiligingsonderzoeken door externe leveranciers. Het hele proces vanaf de intake en het bepalen van de scope tot het uitvoeren van het onderzoek, het herstellen van de bevindingen en de eventuele heronderzoeken wordt behandeld.

5.1 Intake en bepalen van de scope

Bij de uitvoering van IT-beveiligingsonderzoeken is het bepalen van de juiste scope erg belangrijk.

Dat begint allereerst bij de organisatie of instelling zelf. Wanneer de organisatie of instelling verzuimt bepaalde onderzoeksobjecten binnen scope te plaatsen, of er is onduidelijkheid over, dan worden deze objecten niet meegenomen tijdens het IT-beveiligingsonderzoek. Dit klinkt triviaal, maar kan toch tot gemiste kwetsbaarheden leiden. Voor sommige organisaties is ‘asset’ management een uitdaging. Wanneer je niet weet dat je iets hebt, kun je het ook niet testen. Iets dergelijks doet zich bijvoorbeeld al snel voor bij grote organisaties waarbij bijvoorbeeld de inbelverbindingen getest moeten worden of wanneer er gekeken moet worden naar alle externe IP-koppelingen. Organisaties moeten zich er van vergewissen dat de scope volledig is.

Of een organisatie nu een uitvraag doet, of een leverancier een intake, er zal duidelijk moeten worden hoe groot, complex en risicovol een onderzoeksobject is. Dat is, in combinatie met de gebruikte onderzoeksmethodiek (zie hoofdstuk 3), bepalend voor de hoeveelheid tijd die er aan een onderzoek moet worden besteed.

Om de juiste scope te bepalen, moeten in ieder geval de volgende vragen worden beantwoord voor een onderzoek van applicaties:

Algemeen
Wat is de naam van de applicatie?
Geef een kort beschrijving van de applicatie
Welke methodiek moet bij het onderzoek worden gebruikt? (black/grey/crystal-box of penetratietest?)
Welke gegevens moeten worden beschermd en welke risico's ziet de organisatie zelf?

Indicatie van de omvang/complexiteit
Hoeveel schermen telt de applicatie (indicatief)?
Hoeveel formulieren (indicatief)?
Hoeveel velden (indicatief)?
Welke rollen kent de applicatie en welke moeten worden getest?

Indicatie van de omvang/complexiteit
Is het een webapplicatie? Of kent het een andere interface, bijv. Soap, fat client, silverlight, flash, etc.
Hoe wordt met het systeem verbonden? Is dit HTTP(S) (website), SOAP (API) of iets anders?
Is er buiten de standaard web browser nog iets anders benodigd? Zoals Flash, Silverlight, Java, of een fat client.
Moet ook de server waarop de applicatie draait worden onderzocht?
Maakt de onderliggende infrastructuur deel uit van het onderzoek?

Als ook de broncode onderzocht moet worden (optioneel)
In welke taal is de applicatie geschreven en van welke frameworks wordt gebruik gemaakt?
Uit hoeveel regels code bestaat de applicatie (excl. Html, commentaar en eventuele frameworks)

In de bijlage is een intake formulier voor (web)applicatietesten opgenomen waar ook ingegaan wordt op randvoorwaarden die van belang zijn bij de uitvoering van een test (zie ook paragraaf 5.6).

Om de juiste scope te bepalen moeten in ieder geval de volgende vragen worden beantwoord voor een onderzoek van de IT-infrastructuur:

Algemeen
Betreft het een onderzoek vanaf het internet of op locatie op een intern netwerk/dmz?
Welke methodiek moet bij het onderzoek worden gebruikt?
Moet een eventueel heronderzoek meegenomen worden in het voorstel?
Welke gegevens moeten worden beschermd en welke risico's ziet de organisatie zelf?

Indicatie van de omvang/complexiteit (black-, grey-box of penetratietest)
Welke IP adressen / ranges moeten worden onderzocht? Indien niet bekend, of niet gewenst nu te verstrekken, graag een indicatie van het aantal te onderzoeken IP adressen?
Hoeveel systemen zijn vanaf het internet benaderbaar?

Indicatie van de omvang/complexiteit (crystal box)
Hoeveel systemen moeten er worden onderzocht?

Indicatie van de omvang/complexiteit (crystal box)
Geef van elk te onderzoeken systeem het operating systeem en de primaire functie (indien gewenst kan ook een infrastructuur ontwerp worden bijgevoegd

In de bijlage is een intake formulier voor infrastructuurtesten opgenomen waar ook ingegaan wordt op randvoorwaarden die van belang zijn bij de uitvoering van een test (zie ook paragraaf 5.6).

Het is niet altijd mogelijk om alle informatie op een volledige manier uit te vragen. In deze situatie is een goede dialoog tussen de organisatie of instelling en de leverancier noodzakelijk. Dat geldt zeker voor testen die buiten de ‘standaard’ applicatie en infrastructuur onderzoeken vallen, zoals social engineering en red teaming.

Wanneer een organisatie een schriftelijke offerte aanvraag wil sturen naar verschillende leveranciers, dan is het sterk aan te raden om al in de aanvraag de (bovenstaande) benodigde informatie met betrekking tot de scope op te nemen in de aanvraag. Dat scheelt veel vragen van leveranciers. Leveranciers kunnen op basis van de informatie in de aanvraag een passende offerte uitbrengen.

5.2 Offerte

Als een organisatie of instelling nog geen vaste partner heeft voor het uitvoeren van IT-beveiligingsonderzoeken verdient het aanbeveling om bij meerdere leveranciers offertes op te vragen. Op deze manier is het mogelijk verschillende partijen met elkaar te vergelijken zodat de beste leverancier gekozen kan worden. De onderstaande criteria kunnen helpen bij het maken deze keus.

Prijs

Prijs speelt altijd een rol bij het beoordelen van offertes. De prijs van IT-beveiligingsonderzoeken bestaat uit 2 componenten: het (dag/uur) tarief en de tijd die is begroot voor het onderzoek. Het is belangrijk om deze beide componenten te kunnen beoordelen. De tijd die een leverancier begroot voor een onderzoek is een belangrijke factor voor de kwaliteit van het onderzoek. Hoe meer tijd, des te beter en duurder het onderzoek. Uiteraard is ook hier sprake van de wet van de afnemende meeropbrengsten. Op een gegeven moment voegt meer tijd relatief weinig extra kwaliteit toe. Een IT-beveiligingsonderzoek uitvoeren in te weinig tijd zorgt er voor dat er mogelijk veel restrisico's zijn omdat bijvoorbeeld alleen met kleine steekproeven kan worden gewerkt, er minder diepgang kan zijn, minder handmatig wordt onderzocht en er wellicht veel vertrouwd wordt op tooling.

Er moet een goede afweging worden gemaakt door de leverancier (en opdrachtgever) tussen de investering en de beoogde risicoreductie. Het verdient daarbij aanbeveling om ook het belang/risico van het systeem (en de data erin) en de ontwikkelkosten in de afweging mee te nemen.

Neem ook in ogenschouw dat leveranciers die weten dat ze in concurrentie aanbieden de neiging zullen hebben om de factor tijd af te stemmen op de concurrentie en dus wellicht minder tijd zullen begroten dan eigenlijk wenselijk is voor de kwaliteit van het onderzoek.

Ervaring/specialisatie leverancier

Er bestaan geen certificeringen voor leveranciers van IT-beveiligingsonderzoeken. Hoe kan dan vastgesteld worden of een leverancier de beoogde kwaliteit zal leveren? Men mag verwachten dat een organisatie die al vele jaren gespecialiseerd is in het uitvoeren van IT-beveiligingsonderzoeken bepaalde expertise heeft opgebouwd. Dat zal minder het geval zijn bij relatief jonge organisaties of

organisaties die het er (recent) bij (zijn gaan) doen. Dat laatste is een duidelijk zichtbare trend van de laatste jaren. Er is veel vraag naar IT-beveiligingsdiensten met als gevolg dat veel organisaties zich richten op deze groeiende markt.

Duidelijkheid offerte/aanpak

In de offerte moet duidelijk beschreven staan welke aanpak een leverancier kiest en ook op basis van welk normenkader en/of best practices de test wordt uitgevoerd. In een goede offerte gaat een leverancier in op de specifieke situatie van de organisatie of instelling die de aanvraag heeft ingediend. Ook zal de leverancier aangeven wat er van de organisatie of instelling verwacht mag worden en welke randvoorwaarden er zijn voor een goed onderzoek.

Referenties

Referenties kunnen een belangrijk criterium vormen om offertes/leveranciers met elkaar te vergelijken. Kan een leverancier toonaangevende referenties bieden? Is het mogelijk om contact op te nemen met de referenties om navraag te doen naar de ervaringen met de leverancier. Heeft de leverancier ervaring met en referenties binnen de instellingen aangesloten bij SURFnet? Veel instellingen delen een aantal eigenschappen en is het praktisch dat een leverancier daar de nodige ervaring mee heeft.

Voorbeeld rapportage

Van de meeste onderzoeken is het eindresultaat een rapport. Aan dit dure stuk papier mogen de nodige eisen gesteld worden (zie ook paragraaf 5.8). Om een goed beeld te kunnen krijgen van de verschillende rapportages is het belangrijk om voorbeeld rapportages op te vragen en deze goed te vergelijken.

CV's van testers

Het is te overwegen om ook CV's op te vragen van de tester of het team van testers dat de opdracht zal uitvoeren. Cv's zijn echter niet altijd goed bruikbaar als selectiecriterium. Hoe zeker is het bijvoorbeeld dat diegenen van wie het CV wordt gestuurd, ook echt de test gaan uitvoeren? Omdat veel projecten vertrouwelijk zijn, kan er vaak weinig informatie over op CV's worden opgenomen.

Certificeringen zoals Certified Ethical Hacker (CEH) of CISSP geven een minimaal niveau van kennis aan, maar niet zozeer de kwaliteit en ervaring van een tester. Een tester zonder CEH certificering die tientallen of honderden testen heeft uitgevoerd voor een of meer gerenommeerde leveranciers is beslist te prefereren boven een CEH of CISSP consultant met beperkte ervaring.

Een goede leverancier zal zorgen voor één of meer goede testers die passen bij het onderzoeksobject en het risicoprofiel. Er is voor de leverancier immers ook sprake van een afbreukrisico als bepaalde (triviale) risico's niet worden gevonden.

Leveranciers die testen uitvoeren volgens het 4-ogen principe kunnen extra kwaliteit leveren. Door het 4-ogen principe kunnen testers elkaar corrigeren en aanvullen. Het brengt de foutgevoeligheid naar beneden en introduceert creativiteit in het testproces. Door dit principe structureel toe te passen kunnen testers in verschillende teams veel van elkaar leren en zullen ze steeds beter worden in hun vakgebied.

Beschikbaarheid

Als een test voor een bepaalde tijd moet zijn afgerond, speelt het criterium of de leverancier de test tijdig kan uitvoeren een grote rol. Het verdient aanbeveling om, indien mogelijk, flinke tijd te nemen tussen het gunnen van een opdracht en de daadwerkelijke uitvoering. De kans is dan groter dat een leverancier de benodigde capaciteit heeft. Zeker wanneer er sprake is van ingewikkelde testen op

uitdagende onderzoeksobjecten is de expertise vaak schaars. Bovendien is het zo dat wanneer gunning en uitvoering erg dicht op elkaar zitten, leveranciers vaak niet bereid zijn om capaciteit vrij te houden, als niet zeker is dat daar ook gebruik van gemaakt zal worden.

5.3 Planning

Na het bepalen van de scope en het gunnen van de opdracht zal het IT-beveiligingsonderzoek worden ingepland. Welke wensen zijn er ten aanzien van de planning? Moet er bijvoorbeeld rekening worden gehouden met de datum waarop de livegang plaatsvindt? Of heeft de organisatie instelling te maken met een audit waarvan het onderzoek deel uitmaakt? Het is goed om deze wensen in een zo vroeg mogelijk stadium kenbaar te maken. Het is wenselijk om bij de planning rekening te houden met een periode waarbinnen er nog tijd is om (indien noodzakelijk) de gevonden risico's weg te nemen en vervolgens een heronderzoek te laten uitvoeren. Het is daarom onverstandig om een technisch IT-beveiligingsonderzoek vlak voor een geplande 'livegang' uit te laten voeren.

Een planning moet ook niet te optimistisch zijn. Wanneer er een IT-beveiligingsonderzoek uitgevoerd moet worden moet er wel een werkende omgeving zijn. Dit zou zelfs een omgeving moeten zijn die functioneel getest is, zodat er na de IT-beveiligingsonderzoeken vrijwel niets meer wijzigt. Elke functionele wijziging kan immers een nieuw IT-beveiligingsprobleem introduceren.

Het laten uitvoeren van onderzoeken op een niet (goed) werkende omgeving kan kostbaar zijn. Als de resultaten niet betrouwbaar zijn, of de consultants hebben niet efficiënt kunnen onderzoeken, dan kan het zijn dat wellicht het hele onderzoek opnieuw uitgevoerd moet worden. De kosten voor het opnieuw uitvoeren van het onderzoek komen in deze gevallen voor rekening van de opdrachtgever.

Aan de hand van de gewenste planning zal de leverancier, gebaseerd op de afgesproken scope, bepalen welk team van specialisten het beste kan worden ingezet. Op basis van beschikbaarheid wordt er vervolgens samen met de leverancier een definitieve planning vastgelegd.

Door ruim van tevoren de planningsafspraken vast te leggen kunnen alle betrokken partijen tijdig de juiste voorbereidingen treffen voor het gewenste onderzoek. Alle partijen weten op welke dagen de onderzoeken gaan plaatsvinden en wat er tijdens deze dagen verwacht mag worden.

De ervaring leert dat veel IT-beveiligingsonderzoeken in het vierde kwartaal van het jaar worden uitgevoerd. Als gevolg hiervan is de capaciteit bij de testbedrijven vaak erg beperkt. In deze periode is het verstandig om tijdig een offerte uitvraag te doen, anders bestaat de kans dat het onderzoek niet in de gewenste periode uitgevoerd kan worden. Als het mogelijk is, kan men (voor bijvoorbeeld periodieke onderzoeken) beter een andere periode kiezen voor het uitvoeren van de onderzoeken.

5.4 Contract

Na de keuze van een leverancier moeten er contractuele afspraken worden gemaakt. Als basis voor het contract met algemene voorwaarden (AV) kunnen de gebruikelijke contracten en AV voor IT-dienstverlening als basis dienen. Bij het opstellen van een contract voor het uitvoeren van een IT-beveiligingsonderzoek zijn er wel de volgende specifieke aandachtspunten:

- Toestemming en vrijwaring (zie verder paragraaf 5.5.1 en 5.5.2) en het goed vastleggen van de (technische) scope van de opdracht via url's, IP-adressen en/of netwerkranges.
- Geheimhouding: het is voor alle partijen van belang dat (de resultaten van) het IT-beveiligingsonderzoek zeer vertrouwelijk behandeld wordt.

- Beperking aansprakelijkheid: het is gebruikelijk om de aansprakelijkheid van beide partijen te beperken tot een omvang gerelateerd aan de opdrachtgrootte. Een goed voorbeeld hiervan is artikel 21.3 van de ARVODI 2014.

Zie bijlage 2 voor een voorbeeldcontract zoals gebruikt wordt door Madison Gurkha.

5.5 Toestemming en Vrijwaringen

Vanwege de bijzondere aard van IT-beveiligingsonderzoeken, en de daarmee gepaard gaande risico's voor zowel opdrachtgever als leveranciers, moeten toestemming en vrijwaring goed geregeld zijn.

5.5.1 Toestemming

In Nederland en vele andere landen is het "ongeautoriseerd binnendringen van een geautomatiseerd werk" een strafbaar feit. Hoewel de opdrachtverstrekking tot het doen van een IT-beveiligingsonderzoek als impliciete toestemming gezien kan worden, is het raadzaam de toestemming toch expliciet te maken.

Dit kan bijvoorbeeld door een tekst zoals deze op te nemen in het contract:

Het analyseren en/of binnendringen van en/of in het geautomatiseerd werk van de opdrachtgever, waarbij de beveiliging van het systeem wordt geanalyseerd en/of doorbroken en/of de toegang wordt verworven met behulp van valse signalen of een valse sleutel dan wel een valse hoedanigheid wordt aangenomen, een en ander zoals bedoeld in Artikel 138a Wetboek van Strafrecht, dan wel iedere poging daartoe geschiedt in opdracht van en op uitdrukkelijk verzoek van de opdrachtgever.

5.5.2 Vrijwaringen

Als er opdracht gegeven wordt tot het uitvoeren van een IT-beveiligingsonderzoek wordt aan de leverancier gevraagd te onderzoeken welke schade een kwaadwillende hacker zou kunnen aanrichten, maar dan liefst zonder die schade daadwerkelijk aan te richten.

Het is gezien de aard van de testwerkzaamheden en de vaak beperkte tijd onmogelijk te garanderen dat er nooit en te nimmer schade (downtime, verlies/verminking van gegevens) zal optreden. Als de leverancier hiervoor aansprakelijk gesteld kan worden zal niemand een dergelijk IT-beveiligingsonderzoek willen uitvoeren.

Daarom is het noodzakelijk dat de opdrachtgever de leverancier vrijwaart tegen schadeclaims die gerelateerd zijn aan het testen van de beveiliging.

Dit kan bijvoorbeeld door een tekst zoals deze op te nemen in het contract:

> *Opdrachtnemer is niet aansprakelijk voor enige schade, gevolgschade daaronder begrepen, en is in geen geval gehouden tot vergoeding van bedrijfsschade, winstderving, schade voortvloeiende uit aanspraken van derden jegens de opdrachtgever of welke andere schade dan ook, veroorzaakt door het analyseren en/of binnendringen dan wel iedere poging tot het analyseren en/of binnendringen van het geautomatiseerde werk van de opdrachtgever. Deze handelingen voltrekken zich onder de uitdrukkelijke voorwaarde dat opdrachtnemer uitsluitend de beveiliging tracht te analyseren, te doorbreken en/of toegang tracht te verwerven tot door de opdrachtgever aangegeven onderdelen van het geautomatiseerd werk.*

Deze vrijwaring is alleen van toepassing op het testen van de IT-beveiliging. Niet voor andere zaken die aansprakelijkheid kunnen veroorzaken (schending intellectuele eigendomsrechten of geheimhouding, te late oplevering, opzet en/of grove nalatigheid, etc.).

5.5.3 Derde partijen

In veel gevallen zullen behalve de opdrachtgever zelf, ook een of meer derde partijen betrokken zijn bij het beveiligingsonderzoek. Dit is het geval als de opdrachtgever zaken heeft uitbesteed aan bijvoorbeeld hosting- of beheerpartijen. Omdat deze partijen ook mogelijk schade kunnen lijden, moeten zij ook toestemming en vrijwaring geven. Deze vrijwaring is juridisch gezien alleen noodzakelijk wanneer de derde partij eigenaar is van de systemen die onderzocht moeten worden. Zo'n situatie doet zich vaak voor in het geval van (shared) webhosting of wanneer de volledige IT van een organisatie is uitbesteed middels een outsourcingscontract. Wanneer een

De vrijwaring kan op een aantal manieren geregeld worden.

In de meest simpele vorm sluiten de derde partij en leverancier een losse vrijwaringsovereenkomst die alleen toestemming, vrijwaring en geheimhouding omvat. De derde partij geeft toestemming en vrijwaart hierbij de leverancier. De geheimhouding moet dan zo zijn dat leverancier resultaten binnen de scope van de opdracht wel met opdrachtgever mag delen maar andere zaken (zoals andere klanten van de derde partij) niet.

Zie bijlage 1 voor een voorbeeldvrijwaring derde partijen zoals Madison Gurkha die gebruikt.

Vaak wil de opdrachtgever en/of derde partij meer vastleggen, bijvoorbeeld omdat de derde partij zelf ook gevrijwaard wil worden door de opdrachtgever. In dat geval is een driepartijen vrijwaringsovereenkomst aan te bevelen. Hierin kunnen de drie partijen dan specifieke afspraken maken over bijvoorbeeld:

- de vrijwaring door opdrachtgever van derde partij en leverancier voor schadeclaims;
- geen of verminderde service levels van de diensten gedurende de beveiligingstest;
- de kosten voor medewerking en eventueel het uitvoeren van herstelwerk door de derde partij;
- de procedure met betrekking tot oplevering conceptrapportage; hoor- en wederhoor;
- definitieve rapportage;
- Etc.

De verantwoordelijkheid van het regelen van de toestemming en vrijwaring van de derde partijen ligt bij de opdrachtgever. De opdrachtgever heeft (als het goed is) contractuele afspraken met deze derde partijen, de leverancier heeft die niet en kan daarom ook geen medewerking afdwingen. Het is daarom verstandig bij outsourcing-contracten goede afspraken over het houden van IT-beveiligingsonderzoeken te maken.

5.5.4 Beperking van risico’s op schade bij IT-beveiligingsonderzoeken

Hoewel schade nooit geheel uit te sluiten is, is het wel mogelijk om de risico’s op (grote) schade drastisch te beperken door een of meerdere van de volgende maatregelen:

- voer het IT-beveiligingsonderzoek uit op een acceptatie- of testomgeving;
- gebruik speciaal voor het IT-beveiligingsonderzoek aangemaakte testaccounts om mee te testen zodat schade aan productieaccounts en -data zo veel mogelijk voorkomen wordt;
- zorg voor recente, en vooral ook geteste(!), backups inclusief de procedures om deze snel terug te kunnen zetten.

5.6 Werkvoorbereiding

Het doel van de werkvoorbereiding is om alles gereed te hebben zodat een IT-beveiligingsonderzoek succesvol kan worden uitgevoerd.

5.6.1 Doel van de test

Het vaststellen van het doel heeft een tweeledige functie.

Aan de ene kant dwingt tot nadenken over het doel van het onderzoek. Welke risico's ziet de instelling? Waar wil de instelling zich tegen beschermen? Wat valt allemaal wel en niet binnen de scope van het onderzoek? Welke vragen moeten beantwoord worden? Het doel van het onderzoek kan ook voortkomen uit een wettelijke verplichting of compliancy (zie hoofdstuk 1).

Aan de andere kant geeft het de consultant handvatten om het onderzoek uit te voeren. Hoe ver moet de consultant doorgaan op één bepaalde zwakheid in het systeem? Of moeten er toch zoveel mogelijk zwakheden worden gevonden en hoeven deze niet allemaal aantoonbaar uitgebuit te worden? (zie ook hoofdstuk 3 over de verschillende soorten IT-beveiligingsonderzoeken). Hieruit kan een nieuw doel geformuleerd worden voor een eventueel vervolgonderzoek.

Wanneer er aan het begin van het traject een heldere vraagstelling is, is het vervolgens ook eenvoudiger deze vraagstelling duidelijk te beantwoorden.

5.6.2 Targets

Wanneer het doel van het IT-beveiligingsonderzoek is vastgesteld, kan er vervolgens worden bepaald welke targets in scope zijn. Welke URL's of IP-adressen moeten exact worden onderzocht? Betreft het acceptatie- of productieomgevingen?

Bij het bepalen van de targets is het erg belangrijk om secuur te zijn. Targets die niet in scope verklaard zijn kunnen IT-beveiligingsrisico's bevatten die de leverancier niet onderzoekt (zie ook 5.1).

Bij een IT-beveiligingsonderzoek op een productieomgeving moet er scherp worden gelet op het feit dat consultants mogelijk in aanraking komen met productiedata. Dit is als het geen privacygevoelige gegevens betreft meestal niet erg, maar bij privacygevoelige gegevens dient dat omdat dit door de Autoriteit Persoonsgegevens niet toegestaan is. Aan de andere kant is de productieomgeving vaak het meest representatief op het gebied van IT-beveiliging. Wanneer er gebruik gemaakt wordt van specifieke test-accounts is contact met productiedata vaak te vermijden. Het risico op productieverstoringen blijft echter wel bestaan. Het is daarom aan te raden om applicaties te onderzoeken in een acceptatieomgeving, met testdata en accounts. Eventueel in scope zijnde infrastructuur kan ook worden getest in de productieomgeving. Bij het onderzoeken op een acceptatie -of testomgeving is het noodzakelijk dat deze representatief is voor de productieomgeving.

Bij het testen van DigiD webapplicaties is het niet mogelijk deze op productieomgevingen te onderzoeken met test-DigiD accounts. Daarom moeten deze onderzoeken altijd in een testomgeving worden uitgevoerd. Deze onderzoeken uitvoeren op een productieomgeving met echt DigiD accounts is in verband met de privacy zeer sterk af te raden.

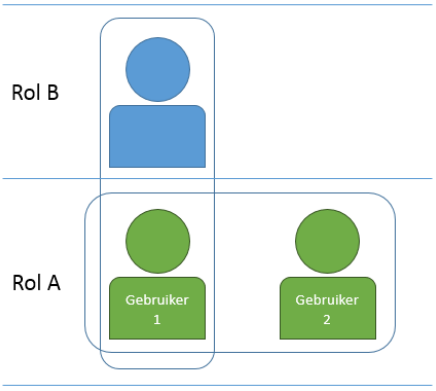
Zodra de targets bekend zijn kan bepaald worden of er vrijwaringen van derde partijen noodzakelijk zijn (zie ook paragraaf 5.5.3). Voor het bepalen of vrijwaringen noodzakelijk zijn, voeren leveranciers vaak een zogenaamde whois-check uit. Daarmee kan worden vastgesteld wie eigenaar is van de IP-adressen. Eigenaars van IP-adressen zijn vaak ook eigenaar van de servers die via die adressen

bereikbaar zijn. Belangrijke uitzondering hierop is colocatie waarbij een organisatie eigen servers heeft ondergebracht in een datacenter van een derde partij.

5.6.3 Credentials

Afhankelijk van het soort onderzoek dat wordt uitgevoerd, heeft de leverancier credentials nodig. Het kan hierbij gaan om bijvoorbeeld alleen een gebruikersnaam met wachtwoord. Het ook zijn dat er sprake is van two-factor authenticatie. Denk hierbij aan DigiD, certificaten, SMS-authenticatie, pasjes of calculators. Afhankelijk van de gekozen oplossing zal dat ook ingericht moeten zijn bij de test-credentials.

Omdat er zowel horizontale als verticale autorisatie controles worden uitgevoerd, is het noodzakelijk dat er per te onderzoeken rol in de applicatie twee sets test-credentials beschikbaar zijn.



Bij de horizontale autorisatiecontrole zal bepaald worden of gebruiker 1 met rol A zaken kan bekijken of zelfs wijzigen die alleen toegankelijk moeten zijn voor gebruiker 2 met rol A.

Bij de verticale autorisatie controle wordt vervolgens vast stellen of gebruiker 1 met rol A bepaalde functionaliteiten kan uitvoeren die eigenlijk alleen beschikbaar zijn voor gebruikers met rol B.

Vanwege die verticale autorisatie controles is het soms raadzaam dat in geval van een black-box-onderzoek (zie paragraaf 3.3) toch een set credentials opgeleverd wordt. Er kan dan worden ingelogd om vast te stellen welke functionaliteiten beschikbaar zijn. Vervolgens kan dan zonder de autorisaties geprobeerd worden om ook die functionaliteiten uit te voeren.

5.6.4 WAF/IDS/IPS

In de hele beveiligingsketen speelt het Intrusion Prevention Systeem (IPS), Intrusion Detection Systeem (IDS) of de Web Application Firewall (WAF) een (zeer) nuttige rol. Echter, een kwaadwillende hacker met voldoende tijd en middelen (bijvoorbeeld IP-adressen die ingezet kunnen worden voor scans) zal zodanig zijn aanval uitvoeren dat dit niet door deze middelen herkend wordt. Een deel van de aanvallen zal worden afgeslagen, maar het vormt geen 100% garantie.

Daarnaast is het zo, dat het bij bijvoorbeeld webapplicaties van belang is dat onderzocht wordt hoe veilig de applicatie zelf is, en niet hoe goed de WAF functioneert. Door het testen van de applicatie zelf kunnen de risico's daarin worden verminderd. De WAF zorgt vervolgens voor een extra verdedigingslaag. Deze situatie is wenselijker dan een situatie waarin de risico’s voor een webapplicatie (hopelijk) worden tegengehouden door de WAF.

Door de beperkte tijd waarin het onderzoek uitgevoerd moet worden kan het worden herkend als een aanval. In het geval van een IPS worden dan het onderzoek sterk bemoeilijkt. Daarom is het zaak dat de bij een IT-security scan betrokken IP-adressen worden gewhitelist. Op deze manier loopt het onderzoek geen vertraging op en onterechte conclusies vermeden.

5.6.5 Contactpersoon (ten behoeve van escalatie)

Tijdens het IT-beveiligingsonderzoek is het van belang dat er verschillende contactpersonen telefonisch beschikbaar zijn.

De volgende drie rollen kunnen daarbij benoemd worden, soms neergelegd bij één persoon.

Ten eerste de persoon die het uiteindelijke rapport ontvangt. Vervolgens is het van belang dat er iemand stand-by is die op de hoogte is van technische aspecten van de omgeving. Mocht het bijvoorbeeld voorkomen dat er tijdens het IT-beveiligingsonderzoek een systeem niet meer online is, kan er direct afstemming plaatsvinden om het systeem weer beschikbaar te maken. Daarnaast is het tijdens grote applicatieonderzoeken raadzaam dat er een functioneel deskundige beschikbaar is. In complexe applicaties is het voor een consultant namelijk niet altijd vanzelfsprekend hoe de applicatie zou moeten functioneren, of wat geldige waarden zijn om naar een volgende stap te kunnen komen in het proces. Hierbij is de hulp van die deskundige erg waardevol.

5.7 Tijdens de test

Op de eerste dag van het onderzoek nemen de consultants – indien gewenst - telefonisch contact op om aan te geven dat het IT-beveiligingsonderzoek van start gaat. De voorkeur hiervoor kan tijdens de offerte- en/of contractfase kenbaar gemaakt worden.

Tijdens de werkvoorbereidingsfase zijn er afspraken gemaakt over het escalatietraject als er gedurende het IT-beveiligingsonderzoek een probleem ontstaat of er onduidelijkheden zijn (zie paragraaf 5.6.5). Wanneer het voorkomt dat tijdens het onderzoek op de afgesproken omgeving een risico wordt aangetroffen dat zo groot is dat deze geclassificeerd zal worden als een ‘hoog risico’, dan wordt de opdrachtgever daarvan direct op de hoogte gesteld. De afspraken over de terugkoppeling van deze eventuele ‘hoge risico’s’ zullen ook tijdens het voortraject worden afgestemd.

Aan het einde van de laatste onderzoeksdag wordt er veelal opnieuw contact opgenomen door de consultants. Enerzijds om zich af te melden, anderzijds om eventuele bijzonderheden door te spreken.

Tijdens het onderezoek is het van groot belang dat de omgeving, waarop het IT-beveiligingsonderzoek wordt uitgevoerd, ongewijzigd blijft. De redenen daarvoor zijn onder andere dat de onderzoeksresultaten onbetrouwbaar kunnen worden of niet meer reproduceerbaar zijn. Het is niet verstandig om tijdens het onderzoek op de testomgeving updates uit te voeren, nieuwe versies te lanceren of andere, bijvoorbeeld functionele, onderzoeken uit te laten voeren. Het laten uitvoeren van perfomancetesten tegelijkertijd met het IT-beveiligingsonderzoek is helemaal af te raden omdat de omgeving onbereikbaar kan worden of erg traag kan reageren.

5.8 Rapportage

Na afloop van het IT-beveiligingsonderzoek rapporteren de consultants uitgebreid over alle bevindingen die tijdens het onderzoek zijn gedaan. In een rapportage is het raadzaam de volgende zaken duidelijk op te laten nemen:

- De scope van het onderzoek
- Uitvoeringsdata van het onderzoek
- Onderzoekers
- De aangetroffen risico’s

- Beschrijving van het risico
- Bewijs van het risico
- Classificatie van het risico
- Advies over te nemen maatregelen

- Managementsamenvatting
- Conclusie op basis van de aangetroffen risico's

Een belangrijke eis die gesteld kan worden aan een rapportage is de 'reproduceerbaarheid'. Bevindingen die de leverancier heeft gedaan wil de instelling (laten) herstellen. Het is hiervoor noodzakelijk dat deze bevindingen weer 'gevonden' kunnen worden alvorens herstelacties mogelijk zijn. Van belang is hierbij dat in de rapportage minimaal vastgelegd staat waar een bepaald risico precies is gevonden en welke tool (inclusief versienummer) en parameters/instellingen van de tool hiervoor gebruikt zijn.

Voorafgaand aan het IT-beveiligingsonderzoek zijn duidelijke afspraken over de vorm van oplevering van de rapportage gemaakt. Een eerste versie in conceptvorm is raadzaam zodat eventuele feedback hierin verwerkt kan worden. Na goedkeuring door de opdrachtgever volgt het definitieve rapport. Ook worden er afspraken gemaakt over de manier waarop het rapport wordt aangeleverd, hierbij moet men zich bewust zijn van het feit dat het rapport mogelijk bedrijfsgevoelige en –kritische informatie bevat.

Afspraken over de onderzoek data zijn eveneens van belang. Te denken valt hierbij aan:

- de bewaartermijn van de data;
- op welke wijze en binnen welke termijn deze moet worden vernietigd.

Hierbij moet rekening gehouden worden met een mogelijk periodiek onderzoek of een eventueel heronderzoek.

5.9 Opvolging bevindingen

Zodra het rapport door de consultants is opgeleverd is het belangrijk dat de resultaten nauwkeurig worden bestudeerd. Hierop kunnen vervolgacties worden gedefinieerd. De meest positieve uitkomst van het IT-beveiligingsonderzoek en het rapport is dat er geen bevindingen zijn. In de praktijk blijkt vaak echter het tegendeel. Voor iedere bevinding moet vastgesteld worden wat de impact voor de organisatie is en wat de kosten zijn om de bevinding te mitigeren. Voor bevindingen met een hoog risiconiveau is de keus vaak helder, maar voor gemiddelde en met name lage risico's moet een organisatie een gedegen afweging maken. Dit kunnen procedurele veranderingen zijn, maar bijvoorbeeld ook een opdracht aan ontwikkelaars en/of netwerkspecialisten om zodanige veranderingen aan te brengen dat het risico en/of impact van een bevinding wordt gereduceerd – bij voorkeur tot nul, maar in ieder geval tot een voor de organisatie of instelling aanvaardbaar niveau.

Wanneer er de beschikking is over een eigen IT-afdeling komen de inspanningen/kosten voor het mitigeren van de bevindingen doorgaans ook voor eigen rekening. Hoe gaat dit echter wanneer het bouwen van bijvoorbeeld een (web)applicatie is uitbesteed aan externe partij? Als er vooraf geen afspraken zijn gemaakt met leveranciers over het gewenste IT-beveiligingsniveau of een IT-beveiliging SLA, is het mogelijk dat de organisatie of instelling de kosten voor benodigde herstelwerkzaamheden zelf moet dragen. De leverancier kan zich op het standpunt stellen dat er geen expliciete afspraken zijn gemaakt en dat het meerwerk betreft. Het is dus buitengewoon belangrijk dat er expliciete IT-beveiligingseisen worden gesteld aan software of IT-infrastructuur die bij derden wordt afgenomen. Hierdoor kan geëist worden dat tekortkomingen kosteloos worden hersteld (zie ook paragraaf 7.2).

5.10 Heronderzoeken

Na het uitvoeren van een onderzoek en het oplossen van de bevindingen verdient het aanbeveling om te laten controleren of dit op de juiste manier is gebeurd. Soms is er zelf een vereiste om een heronderzoek te laten uitvoeren, zoals bij DigiD omdat er anders geen goedkeuring komt en afsluiting dreigt.

Afhankelijk van de hoeveelheid aanpassingen die zijn gedaan om de bevindingen op te lossen een deelonderzoek worden uitgevoerd, maar er kan ook een volledig nieuw onderzoek nodig zijn om te onderzoeken of maatregelen die zijn getroffen geen nieuwe kwetsbaarheden hebben veroorzaakt. Een volledig heronderzoek is aan te raden als er meerdere maanden verstreken zijn sinds de uitvoering van het oorspronkelijk onderzoek. Hierbij is namelijk een grotere kans dat niet alleen bevindingen zijn opgelost, maar dat er ook andere aanpassingen zijn gedaan en functionaliteit is toegevoegd of verwijderd.

Bij een heronderzoek moet een leverancier altijd controleren of bepaalde bevindingen structureel zijn opgelost of dat er hier en daar een pleister is geplakt. In de praktijk wordt er veel aan symptoombestrijding gedaan, zonder de werkelijke oorzaak aan te pakken, met alle (toekomstige) risico's van dien.

Wanneer er tot een heronderzoek besloten wordt is het van belang dat er in detail gecommuniceerd wordt welke bevindingen bij het heronderzoek betrokken zijn. Het is mogelijk dat niet alle bevindingen zijn opgelost of dat sommige bevindingen door de instelling als aanvaardbaar zijn aangemerkt. Overigens is het zo dat als een organisatie vindt dat een risico aanvaardbaar is, er nog steeds sprake kan zijn van een technisch risico dat de leverancier in zijn rapportage handhaaft.

6 Bronnen

https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2014/cyberdreigingsbeeld-sector-hoger-onderwijs-en-wetenschappelijk-onderzoek.pdf

https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wbp-naslag/hoofdstuk-2-voorwaarden-voor-de-rechtmatigheid-van-de-verwerking-v-23

https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken.pdf

https://www.logius.nl/fileadmin/logius/ns/diensten/digid/assessments/120221_norm_ict-beveiligingsassessments_digid.pdf

https://www.eerstekamer.nl/eu/europeesvoorstel/com_2012_11_voorstel_voor_een/document/f=/viwze2lerprf.pdf

https://www.surf.nl/diensten-en-producten/surfaudit/normenkader-surfaudit/index.html

https://www.sambo-ict.nl/wp-content/uploads/2015/02/IBBDOC3-MBO-Toetsingskader-Informatie-Beveiliging-versie-1.0-Creative-Commons.docx

https://www.werkenmetnen7510.nl

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

https://www.owasp.org/images/6/67/OWASPApplicationSecurityVerificationStandard3.0.pdf

https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

http://www.cip-overheid.nl/downloads/grip-op-ssd/

https://www.securesoftwarefoundation.org/FrameworkSecureSoftware.html

http://www.sans.org/

http://www.nist.gov/cyberframework/index.cfm

https://www.microsoft.com/en-us/sdl/default.aspx

https://www.microsoft.com/en-us/download/details.aspx?id=34276

http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

7 Bijlage 1: Wet- en regelgeving en normenkaders toegelicht

7.1 Wet- en regelgeving

7.1.1 Wet bescherming persoonsgegevens

Zeer veel organisaties maken niet alleen gebruik van persoonsgegevens maar wisselen deze ook uit. Dit geldt ook voor veel leden die aangesloten zijn bij SURF. De belangrijkste regels voor de omgang met persoonsgegevens zijn in Nederland vastgelegd in de Wet bescherming persoonsgegevens.

De Wet bescherming persoonsgegevens (Wbp) is de Nederlandse uitwerking van de Europese richtlijn bescherming persoonsgegevens (95/46/EG). De Wbp is sinds 1 september 2001 van kracht.

In deze wet is in artikel 13 het volgende opgenomen:

"De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen."

In dit wetsartikel staan een aantal interessante zaken: passende maatregelen en stand van de techniek. Elke organisatie moet zich afvragen in hoeverre de maatregelen passend zijn en of er rekening wordt gehouden met de stand van de techniek. Het (laten) uitvoeren van technische IT-beveiligingsonderzoeken kan een aanzienlijke bijdrage leveren om deze vragen te beantwoorden.

Meer informatie:

https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wbp-naslag/hoofdstuk-2-voorwaarden-voor-de-rechtmatigheid-van-de-verwerking-v-23

7.1.2 Meldplicht datalekken

Op 1 januari 2016 is de meldplicht datalekken van de Autoriteit Persoonsgegevens (AP) van kracht geworden. Het AP zegt over deze wet op haar website:

"Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. En soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt)."

Onder deze meldplicht vallen veel verschillende soorten datalekken, uiteenlopend van het verliezen van usb-sticks tot websites die gehackt worden. Dit document gaat alleen in op de nut- en noodzaak van het uitvoeren van technische IT-beveiligingsonderzoeken en de meldplicht datalekken. Het is voor elke organisatie of instelling belangrijk om na te gaan wat de meldplicht voor hen betekent en hoe om te gaan met mogelijke IT-beveiligingsincidenten (die onder de meldplicht vallen).

Heeft een organisatie of instelling een datalek en wordt dit onterecht niet aan de AP gemeld, dan kan een boete tot maximaal 810.000 euro volgen (en in de toekomst zelfs nog hoger, afhankelijk van voorgenomen veranderingen in het wetboek van strafrecht). Deze boete volgt alleen na het onterecht niet melden van een datalek en niet voor het incident zelf. Wel kan de AP een verplichting opleggen om de betrokkenen te informeren bij een datalek.

Er is onder de meldplicht datalekken geen verplichting opgenomen voor het (periodiek) laten uitvoeren van technische IT-beveiligingsonderzoek. Toch kan de meldplicht datalekken een extra motivator zijn om dit wel te doen. Bij vrijwel alle bij SURFnet aangesloten instellingen is er sprake van persoonsgegevens, zoals patiënten-, studenten- en uiteraard ook gegevens van medewerkers. Het laten uitvoeren van technische IT-beveiligingsonderzoeken verlaagt de kans op mogelijke datalekken en daarmee ook de kans dat deze gemeld moeten worden. Het is wel belangrijk om deze onderzoeken uit te voeren voordat een bepaalde IT-oplossing in gebruik wordt genomen. Het laten uitvoeren van een IT-beveiligingsonderzoek op een productie-omgeving, zoals een bestaande website, kan ook aanleiding geven tot het moeten melden van een incident. Stel dat een IT-beveiligingsonderzoek op een studentenportaal uitwijst dat er sprake is van een ernstige vorm van SQL- injectie waardoor de inhoud van de studentendatabase door onbevoegden (gedurende lagere tijd) uitgelezen kon worden of er wordt zelfs kwaadaardige software op de database server aangetroffen. Ook dergelijke bevindingen uit een IT-beveiligingsonderzoek kunnen onder de meldplicht vallen.

Er is nog een tweede reden om IT-beveiligingsonderzoeken uit te willen voeren. Als een organisatie of instelling namelijk kan bewijzen dat er geen misbruik is gepleegd, dan is er geen meldplicht van een IT-beveiligingsincident. Organisaties of instellingen kunnen (in samenwerking met een beveiligingsleverancier) bijvoorbeeld aan de hand van betrouwbare logfiles bewijzen dat onbevoegden geen toegang tot de gegevens hebben gehad of dat de gebruikte encryptie zodanig betrouwbaar is, dat misbruik vrijwel kan worden uitgesloten. Het is als organisatie daarom te overwegen om ook na te (laten) gaan hoe betrouwbaar logging, monitoring en encryptie zijn.

Meer informatie:

https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken en

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken.pdf

7.1.3 DigiD Audit

In de inleiding van dit hoofdstuk is al gerefereerd aan Lektober en de daaruit voortgekomen DigiD-audit van Logius. Elke organisatie of instelling die DigiD gebruikt als authenticatiemechanisme voor haar websites moet bij ingebruikname en daaropvolgend jaarlijks een DigiD-audit laten uitvoeren. Veel instellingen aangesloten bij SURFnet gebruiken SURFconext, maar met name in de medische sector (bijvoorbeeld (academische) ziekenhuizen) wordt DigiD gebruikt voor het ontsluiten van onder andere patiëntenportalen.

Het niet (tijdig) laten uitvoeren van een DigiD-audit kan leiden tot het afsluiten van DigiD.

De DigiD-audit wordt uitgevoerd door een geregistreerde EDP-auditor (deze is lid van ISACA of Norea) die de aansluiting toetst tegen het DigiD normenkader. Deze auditor mag in dienst zijn van de organisatie zelf en hoeft niet onafhankelijk te zijn. Het normenkader is gebaseerd op een subset van ICT-beveiligingsrichtlijnen voor webapplicaties van NCSC (zie verder 7.3.2).

In het normenkader zijn een aantal technische IT-beveiligingsnormen opgenomen die alleen vast te stellen zijn door het (laten) uitvoeren van een technisch IT-beveiligingsonderzoek. Een tweetal normen gaat ook expliciet over het periodiek laten uitvoeren van een penetratietest (B0-8) en een black-box-scan (B3-15) (zie ook hoofdstuk 3 over de verschillende soorten testen).

Het volledige normenkader is te vinden op de website van Logius:

https://www.logius.nl/fileadmin/logius/ns/diensten/digid/assessments/120221_norm_ict-beveiligingsassessments_digid.pdf

7.1.4 Europese richtlijnen

Ook op Europees niveau is wetgeving in de maak. Deze wetgeving werd in concept in december 2015 door een commissie in de Eerste Kamer behandeld. De verwachting is dat deze wetgeving in de loop van 2016 ingevoerd zal worden.

In de concept wetgeving zijn in ieder geval artikelen opgenomen die stellen dat er sprake moet zijn van een ‘passende beveiliging’ van privacy gevoelige gegevens. De vraag hierbij rijst dan op: ‘wat is passend?’. In een (juridische) discussie die wellicht ooit daarover ontstaat, heeft een organisatie in ieder geval een sterkere positie als zij kan aantonen dat er structureel IT-beveiligingsonderzoeken worden uitgevoerd en de daaruit voortvloeiende uitkomsten ter harte neemt.

In deze wetgeving is ook een vergelijkbare meldplicht opgenomen als die van de Autoriteit Persoonsgegevens inclusief mogelijk zeer aanzienlijke boetes.

Meer informatie:

https://www.eerstekamer.nl/eu/europeesvoorstel/com_2012_11_voorstel_voor_een/document/f=/viwze2lerprf.pdf

7.1.5 Overige Wet- en Regelgeving

Er is voor organisaties in bepaalde sectoren of voor beursgenoteerde organisatie ook wet- en regelgeving van belang waarin verplichtingen zijn opgenomen voor het (onafhankelijk) laten uitvoeren van technische IT-beveiligingsonderzoeken. Voor de bancaire sector zijn dat bijvoorbeeld regels van De Nederlandsche Bank en voor beursgenoteerde bedrijven in de Verenigde Staten (Sarbanes Oxley). Omdat deze wet- en regelgeving voor de instellingen van SURFnet weinig relevant is, wordt hier verder niet op ingegaan.

7.2 Normenkaders

Door het bestaan van wet- en regelgeving (zoals de Logius DigiD norm) kan er een verplichting zijn tot het uitvoeren van technische IT-beveiligingsonderzoeken. In andere situaties is het verstandig om een dergelijk onderzoek uit te voeren, denk hierbij aan de Wet bescherming persoonsgegevens of de meldplicht datalekken. Naast deze wet- en regelgeving zijn er normenkaders op het gebied van informatiebeveiliging waar de aanbeveling of ‘verplichting voor het uitvoeren van technische IT-beveiligingsonderzoeken im- of expliciet zijn opgenomen.

7.2.1 ISO 27K

Een van de bekendste normenkaders op het gebied van informatiebeveiliging betreft ISO 2700X. Deze staat in Nederland ook wel bekend als Code voor Informatiebeveiliging. Dit normenkader is zeer breed van opzet en gaat in op veel aspecten van informatiebeveiliging zoals beleid, personeel, cryptografie, toegangscontrole, communicatie, incident management etc. Richtlijnen en/of eisen die betrekking hebben op het uitvoeren van technische IT-beveiligingsonderzoeken maken slechts voor een zeer beperkt deel uit van de ISO 2700X familie.

In de praktijk wordt gebruik gemaakt van zowel de ISO 27001 als de ISO 27002. Op hoofdlijnen is het verschil tussen deze varianten dat de ISO 27001 normatief is, en organisaties er zich tegen kunnen certificeren. ISO 27002 is niet-normatief en bevat best-practices voor de implementatie van

informatiebeveiliging. Van deze ISO normen zijn de nodige afgeleide normenkaders gemaakt, waarvan de voor de onderwijsinstellingen twee belangrijkste varianten worden behandeld:

- SURFaudit
- NEN 7510/11

7.2.2 SURFaudit

Het normenkader SURFaudit is gebaseerd op ISO27002:2013 en is verdeeld over 6 clusters.

- Cluster 1: Beleid en organisatie.
- Cluster 2: Personeel, studenten en gasten.
- Cluster 3: Ruimten en apparatuur.
- Cluster 4: Continuïteit.
- Cluster 5: Toegangsbeveiliging.
- Cluster 6: Controle en logging.

In het normenkader wordt op een aantal plaatsen (zijdelings) ingegaan op het (laten) uitvoeren van technische IT-beveiligingsonderzoeken.

- **4.8**: Beheer van technische kwetsbaarheden: Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt wordt tijdig verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden wordt geëvalueerd en er worden passende maatregelen genomen om het risico dat ermee samenhangt aan te pakken.
- **6.5**: Testen van systeembeveiliging: Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest. Tijdens ontwikkelactiviteiten wordt de beveiligingsfunctionaliteit getest.
- **6.7**: Monitoring en beoordeling van dienstverlening van leveranciers: Organisaties monitoren, beoordelen en auditen regelmatig de dienstverlening van leveranciers.
- **6.10**: Beoordeling van technische naleving: Informatiesystemen worden regelmatig beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.

Op basis van het normenkader heeft SURFnet ook een toetsingskader (voor het MBO) ontwikkeld. Daarin wordt op een 5-punts schaal van het Capability Maturity Model (CMM) per niveau aangegeven waaraan een organisatie moet voldoen.

Het normenkader SURFaudit vereist - afhankelijk van het gewenste CMM niveau - het structureel (laten) uitvoeren van technische IT-beveiligingsonderzoeken om kwetsbaarheden in systemen (infrastructureel en applicatief) op te sporen.

Meer informatie:

https://www.surf.nl/diensten-en-producten/surfaudit/normenkader-surfaudit/index.html

https://www.sambo-ict.nl/wp-content/uploads/2015/02/IBBDOC3-MBO-Toetsingskader-Informatie-Beveiliging-versie-1.0-Creative-Commons.docx

7.2.3 NEN 7510/11

Net als SURFaudit is de NEN 7510 gebaseerd op ISO 27K. Daar waar SURFaudit is toegespitst op de instellingen aangesloten bij SURFnet is de NEN 7510/11 gericht op instellingen in en/of gerelateerd aan de zorg. Aangezien een deel van de eerder genoemde instellingen actief is in deze sector, wordt de NEN7510 norm kort behandeld. Naast de NEN 7510 zijn er ook nog de NEN 7512:2015 en NEN

7513:2010. De NEN 7512 heeft betrekking op de uitwisseling van gegevens terwijl de NEN 7513 de logging van acties op patiëntendossiers behandelt.

Het gebruik van de NEN7510/11 is niet verplicht voor zorginstellingen. Het is echter wel aan te raden deze norm te gebruiken. De Inspectie voor de Gezondheidszorg (IGZ) gebruikt de NEN 7510 om te toetsen of zorginstellingen de juiste maatregelen treffen voor adequate informatiebeveiliging.

Net als in het geval van SURFaudit zijn in de NEN7510 diverse verwijzingen aan te treffen die het (laten) uitvoeren van (periodieke) IT-beveiligingstesten op netwerken en applicaties vereisen.

Meer informatie:

https://www.werkenmetnen7510.nl

7.3 Technische normenkaders

Naast de bovengenoemde brede normenkaders voor informatiebeveiliging zijn er veel technische richtlijnen en normenkaders die kunnen dienen als leidraad voor het technisch veilig opzetten van (web)applicaties en IT-infrastructuren. Ook kunnen deze richtlijnen gebruikt worden om tegen te toetsen. In de praktijk wordt echter ook vaak getest op basis van best practices van leveranciers van IT-beveiligingsonderzoeken.

7.3.1 OWASP (Top 10 en ASVS)

OWASP staat voor "The Open Web Application Security Project". Dit is een non-profit instelling die er op gericht is om het beveiligingsniveau van (web) applicaties te verbeteren. Het is belangrijk te beseffen dat de OWASP richtlijnen niet ingaan op de risico's van IT-infrastructuren.

OWASP Top 10

De OWASP top 10, is een van meest eenvoudige en pragmatische manieren om websites veiliger te (laten) ontwikkelen en te (laten) toetsen. De OWASP top 10, de naam zegt het eigenlijk al, bevat de 10 meest voorkomende technische IT-beveiligingsproblemen in webapplicaties (versie 2013).

- A1 Injection.
- A2 Broken Authentication and Session Management.
- A3 Cross-Site Scripting (XSS).
- A4 Insecure Direct Object References.
- A5 Security Misconfiguration.
- A6 Sensitive Data Exposure.
- A7 Missing Function Level Access Control.
- A8 Cross-Site Request Forgery (CSRF).
- A9 Using Components with Known Vulnerabilities.
- A10 Unvalidated Redirects and Forwards.

Webapplicaties die deze fouten niet bevatten kunnen over het algemeen als veilig worden beschouwd. Honderd procent beveiliging bestaat echter niet en ook kan er nog sprake zijn van infrastructurele problemen.

OWASP ASVS

De OWASP Application Security Verification Standard (ASVS) vormt een basis voor het testen van webapplicaties, maar het kan uiteraard ook gebruikt worden als input om veilige software te (laten) bouwen.

ASVS kent drie niveau's.

- ASVS Level 1 is voor alle software.
- ASVS Level 2 is voor applicaties die gevoelige informatie bevatten en die bescherming behoeft.
- ASVS Level 3 is voor de meest kritische applicaties, zoals applicaties voor transacties met veel waarde of gevoelige medische gegevens .

ASVS is ingedeeld in 19 categorieën.

- V1. Architecture, design and threat modelling .
- V2. Authentication.
- V3. Session management.
- V4. Access control.
- V5. Malicious input handling.
- V7. Cryptography at rest.
- V8. Error handling and logging.
- V9. Data protection.
- V10. Communications.
- V11. HTTP security configuration
- V13. Malicious controls
- V15. Business logic
- V16. File and resources
- V17. Mobile
- V18. Web services
- V19. Configuration

Afhankelijk van het niveau (1,2 of 3) worden in een categorie bepaalde richtlijnen wel of niet meegenomen.

Meer informatie:

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

https://www.owasp.org/images/6/67/OWASPApplicationSecurityVerificationStandard3.0.pdf

7.3.2 NCSC ICT-beveiligingsrichtlijnen voor webapplicaties

In Nederland heeft het Nationaal Cyber Security Centrum (NCSC) ICT-Beveiligingsrichtlijnen voor Webapplicaties ontwikkeld. Anders dan bij OWASP wordt in deze richtlijnen ook aandacht besteed aan IT-beveiligingsrisico's van IT-infrastructuren waarop deze websites zijn gehost.

Er zijn twee documenten: Richtlijnen en Verdieping. De benamingen van deze documenten verklaren grotendeels de inhoud. De Richtlijnen geeft een overzicht op hoofdlijnen en de Verdieping worden de maatregelen verder uitgewerkt. De DigiD-audit (zie paragraaf 7.1.3) bestaat uit een kleine subset van normen uit de richtlijnen.

De richtlijnen zijn opgedeeld in de volgende domeinen:

- Beleidsdomein;
- Uitvoeringsdomein;
    - Toegangsvoorzieningsmiddelen
    - Webapplicaties

  - Platformen en webservers
  - Netwerken

- Beheersingsdomein (control).

In het verdiepingsdocument zijn de richtlijnen gedetailleerd uitgewerkt. Per richtlijn geeft het NCSC aan wat de doelstelling is, welke risico er bestaat en welke classificatie het risico heeft (Laag, Midden, Hoog). Het document geeft vervolgens gedetailleerd maatregelen aan.

De web richtlijnen vormen een goed uitgangspunt en naslagwerk voor het (laten) ontwikkelen van veilige webapplicaties en infrastructuren. Dit geldt ook voor het uitvoeren van IT-beveiligingsonderzoeken. In de praktijk gebeurt dat doorgaans tegen een gedeelte van de richtlijnen, zoals bij de DigiD-audit. Het (laten) testen van webapplicaties en bijbehorende infrastructuren tegen de volledige norm kost veel tijd en vergt een aanzienlijke investering.

Meer informatie:

https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

7.3.3 Grip op SSD

Vanuit het CIP (Centrum Informatiebeveiliging en Privacybescherming) is de methode Grip op Secure Software Development (SSD) ontwikkeld. Deze methode bevat 3 documenten.

- Het Proces.
- De Normen.
- Normen voor Mobiele Apps.

Het Procesdocument vormt de kern van de SSD methode en beschrijft hoe een organisatie het proces zo kan inrichten dat het resultaat veilige software oplevert.

In de Normendocumenten zijn concrete beveiligingseisen opgenomen. Zo zijn er in dit document 31 eisen opgenomen voor (web)applicaties en bevat het document Normen voor Mobiele Apps 19 eisen voor mobiele applicaties. Alle eisen worden in het document uitgebreid beschreven en zijn voorzien van een criterium, doelstelling en er worden concrete voorstellen gedaan voor oplossingen/settings die een applicatie veilig maken. Het is handig dat elke eis ook referenties bevat naar ISO 27002, het SSD Proces document en OWASP ASVS.

Grip op SSD wordt door een aantal organisaties in Nederland gebruikt, waaronder overheidsorganisaties zoals DUO, Logius, SVB en UWV.

Ook Grip op SSD kan voor organisaties een goed uitgangspunt vormen om veilige applicaties te (laten) ontwikkelen en testen. Net als OWASP wordt de IT-infrastructuur vrijwel buiten beschouwing gelaten.

Meer informatie:

http://www.cip-overheid.nl/downloads/grip-op-ssd/

7.3.4 Framework Secure Software

De Secure Software Foundation heeft het Framework Secure Software uitgewerkt. Met dit Framework kunnen organisaties veilige software (laten) ontwikkelen en testen. Het Framework kan volgens de makers zelfs worden gebruikt om tegen te certificeren. Hoewel het Framework sinds mei 2014

bestaat, zijn er eind 2015 echter nog geen certificerende instanties te vinden op de website van de Secure Software Foundation. Het is dan ook de vraag wat het draagvlak van het Framework is.

Het Framework is opgesteld op een hoger abstractieniveau dan de andere technische normenkaders die in dit whitepaper beschreven zijn. Het is daarom minder praktisch toepasbaar.

Meer informatie:

https://www.securesoftwarefoundation.org/FrameworkSecureSoftware.html

7.3.5 Overige richtlijnen

Naast de technische normenkaders die in dit whitepaper worden behandeld, zijn er vele richtlijnen beschikbaar die kunnen bijdragen aan veilige software en IT-infrastructuren. Deze richtlijnen zijn vaak afkomstig van (internationale) overheidsorganisaties of leveranciers van specifieke hard- of software.

Enkele voorbeelden:

http://www.sans.org/

http://www.nist.gov/cyberframework/index.cfm

https://www.microsoft.com/en-us/sdl/default.aspx

https://www.microsoft.com/en-us/download/details.aspx?id=34276

http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

8 Bijlage 2: Standaard vrijwaring

Toestemming en vrijwaring voor

OMSCHRIJVING OPDRACHT

Derde Partij B.V.

(Document1)

VERTROUWELIJK

14 april 2016

Derde Partij B.V.

T.a.v. dhr./mevr. NAAM

STRAAT

POSTCODE PLAATS

Datum: 14 april 2016

Betreft: Toestemming en vrijwaring voor OMSCHRIJVING OPDRACHT
(Document1)

DE ONDERGETEKENDEN:

Derde Partij B.V., gevestigd aan STRAAT te PLAATS, in de persoon van _____, gerechtigd tot het aangaan van deze overeenkomst, hierna aangeduid met “Derde Partij”;

en

Opdrachtnemer B.V., gevestigd aan STRAAT te PLAATS, in de persoon van....., gerechtigd tot het aangaan van deze overeenkomst, hierna aangeduid met “Opdrachtnemer”;

NEMEN IN AANMERKING DAT:

1. Opdrachtnemer in opdracht van **KLANT**, hierna aangeduid met “Opdrachtgever”, activiteiten zal verrichten bestaande uit het uitvoeren van een OMSCHRIJVING OPDRACHT ten behoeve van de ICT-security van Opdrachtgever en de bevindingen daarvan opnemen in een rapport, zoals separaat contractueel overeengekomen tussen Opdrachtgever en Opdrachtnemer.

2. Voor het uitvoeren van de opdracht het noodzakelijk is (security)testen uit te voeren op op systemen en/of applicaties die eigendom zijn van, of gehost en/of beheerd worden door Derde Partij voor Opdrachtgever.

KOMEN OVEREEN DAT:

Toestemming en vrijwaring

3. Het analyseren en/of binnendringen van en/of in het geautomatiseerd werk van Derde Partij, waarbij de beveiliging van het systeem wordt geanalyseerd en/of doorbroken en/of de toegang wordt verworven met behulp van valse signalen of een valse sleutel dan wel een valse hoedanigheid wordt aangenomen, een en ander zoals bedoeld in Artikel 138a Wetboek van Strafrecht, dan wel iedere poging daartoe geschiedt in opdracht van en op uitdrukkelijk verzoek van Derde Partij/Opdrachtgever.

4. Opdrachtnemer is niet aansprakelijk voor enige schade, gevolgschade daaronder begrepen, en is in geen geval gehouden tot vergoeding van bedrijfsschade, winstderving, schade voortvloeiende uit aanspraken van derden jegens Derde Partij of welke andere schade dan ook, veroorzaakt door het analyseren en/of binnendringen dan wel iedere poging tot het analyseren en/of binnendringen

van het geautomatiseerde werk van Derde Partij. Deze handelingen voltrekken zich onder de uitdrukkelijke voorwaarde dat Opdrachtnemer uitsluitend de beveiliging tracht te analyseren, te doorbreken en/of toegang tracht te verwerven tot door Derde Partij/Opdrachtgever aangegeven onderdelen van het geautomatiseerd werk.

Overige bepalingen

5. De toestemming en vrijwaring heeft betrekking op de volgende systemen en/of applicaties:

   - NETWERK A
   - NETWERK B
   - APPLICATIE A
   - APPLICATIE B

   [IP-ranges en/of URLs zullen separaat tussen partijen worden overeengekomen en gecommuniceerd.]

   Wijzigingen na ondertekening van deze overeenkomst zullen per e-mail overeengekomen worden.

6. De toestemming en vrijwaring geldt vanaf het, in het contract of separaat, overeengekomen begin van de opdracht tot de oplevering van het definitieve rapport aan Opdrachtgever. Als Opdrachtgever naar aanleiding van het rapport tot een of meerdere aansluitende heronderzoeken door Opdrachtnemer besluit, geldt deze toestemming en vrijwaring ook gedurende de uitvoering van deze heronderzoeken.

7. Alle mogelijkheden die Opdrachtnemer bekend zijn om systemen en applicaties binnen te dringen, dan wel gegevens aan deze systemen en applicaties te onttrekken, zullen door Derde Partij worden toegestaan, met uitzondering van aanvallen waarvan vooraf algemeen bekend is dat die de systemen en applicaties onbereikbaar maken (zogenoemde Denial of Service aanvallen).

8. Eventuele externe tests door Opdrachtnemer zullen worden uitgevoerd vanaf systemen uit het domein madison-gurkha.com waarbij deze systemen zich in een van de volgende netwerkranges bevinden:

   - 88.159.10.0/26
   - 194.151.35.240/28
   - 87.251.52.176/28
   - 2a01:670:310::/48 (IPv6)
   - 2001:7b8:609::/48 (IPv6)

   Als vanaf een ander netwerk wordt getest door Opdrachtnemer, zal dit van tevoren bekend worden gemaakt aan Derde Partij.

Vertrouwelijkheid

9. Alle informatie en gegevens die tussen Opdrachtnemer en Derde Partij worden uitgewisseld of waarvan kennis genomen wordt, waaronder in elk geval programmatuur, voorbereidend materiaal, documentatie, knowhow en bedrijfsgeheimen van Opdrachtnemer en Derde Partij, worden als vertrouwelijk behandeld door beide partijen. De partij die vertrouwelijke informatie ontvangt, zal van deze informatie slechts gebruik maken voor het doel waarvoor deze verstrekt is en deze informatie niet aan derden verstrekken of kenbaar maken, tenzij schriftelijk anders

overeengekomen tussen partijen dan wel er een wettelijke verplichting tot openbaarmaking van deze informatie is.

Slotbepaling

10. Op deze overeenkomst is Nederlands recht van toepassing.

In tweevoud opgemaakt, geparafeerd en ondertekend.

Derde Partij B.V.	**Opdrachtnemer B.V.**
Datum:	Datum:
Naam/functie:	Naam/functie:
Handtekening:	Handtekening:

9 Bijlage 3: Standaard contract

Overeenkomst ten behoeve van

OMSCHRIJVING OPDRACHT

Klantnaam B.V.

(Document1)

VERTROUWELIJK

14 april 2016

Klantnaam B.V.

T.a.v. dhr./mevr. NAAM

STRAAT

POSTCODE PLAATS

Datum: 14 april 2016

Betreft: Overeenkomst ten behoeve van OMSCHRIJVING OPDRACHT
(Document1)

DE ONDERGETEKENDEN:

Klantnaam B.V., gevestigd aan STRAAT te PLAATS, in de persoon van _____, gerechtigd tot het aangaan van deze overeenkomst, hierna aangeduid met “Opdrachtgever”;

en

Opdrachtnemer B.V., gevestigd aan STRAAT te Plaat, in de persoon ....., gerechtigd tot het aangaan van deze overeenkomst, hierna aangeduid met “Opdrachtnemer”;

NEMEN IN AANMERKING DAT:

1. Opdrachtgever ondersteuning wenst te krijgen bij het identificeren, verminderen en voorkomen van ICT-securityrisico’s.

2. Om dit te realiseren zal Opdrachtnemer voor Opdrachtgever activiteiten verrichten bestaande uit het uitvoeren van een OMSCHRIJVING OPDRACHT ten behoeve van de ICT-security van Opdrachtgever en de bevindingen daarvan opnemen in een rapport, zoals beschreven in de offerte met kenmerk OFF-2011MMDD.01.

3. Door ondertekening van deze overeenkomst verklaart Opdrachtgever zich akkoord met deze activiteiten van Opdrachtnemer voor Opdrachtgever.

4. Door ondertekening van deze overeenkomst verklaart Opdrachtgever zich ervan bewust te zijn dat resultaten van beveiligingsonderzoeken geen garantie bieden voor de toekomst en dat volledige beveiliging van systemen en organisaties nooit gegarandeerd kan worden. Opdrachtgever is zich er tevens van bewust dat standaard- en maatwerksoftware doorgaans (ICT-security)fouten bevatten die nog niet bekend zijn en die niet binnen de overeengekomen tijd (allemaal) door Opdrachtnemer kunnen worden opgespoord. Opdrachtnemer kan daarvoor dan ook niet aansprakelijk gehouden worden.

KOMEN OVEREEN DAT:

Toestemming en vrijwaring

5. Het analyseren en/of binnendringen van en/of in het geautomatiseerd werk van Opdrachtgever, waarbij de beveiliging van het systeem wordt geanalyseerd en/of doorbroken en/of de toegang wordt verworven met behulp van valse signalen of een valse sleutel dan wel een valse hoedanigheid wordt aangenomen, een en ander zoals bedoeld in Artikel 138a Wetboek van Strafrecht, dan wel iedere poging daartoe geschiedt in opdracht van en op uitdrukkelijk verzoek van Opdrachtgever.
6. Opdrachtnemer is niet aansprakelijk voor enige schade, gevolgschade daaronder begrepen, en is in geen geval gehouden tot vergoeding van bedrijfsschade, winstderving, schade voortvloeiende uit aanspraken van derden jegens Opdrachtgever of welke andere schade dan ook, veroorzaakt door het analyseren en/of binnendringen dan wel iedere poging tot het analyseren en/of binnendringen van het geautomatiseerde werk van Opdrachtgever. Deze handelingen voltrekken zich onder de uitdrukkelijke voorwaarde dat Opdrachtnemer uitsluitend de beveiliging tracht te analyseren, te doorbreken en/of toegang tracht te verwerven tot door Opdrachtgever aangegeven onderdelen van het geautomatiseerd werk.

Uitvoering van de overeenkomst

7. De opdracht heeft betrekking op de volgende systemen en/of applicaties:

   - NETWERK A
   - NETWERK B
   - APPLICATIE A
   - APPLICATIE B

   [IP-ranges en/of URLs zullen separaat tussen partijen worden overeengekomen en gecommuniceerd.]

Wijzigingen na ondertekening van deze overeenkomst zullen per e-mail overeengekomen worden.

8. De opdracht zal in onderling overleg worden ingepland. Als een overeengekomen planning door Opdrachtgever binnen 14 dagen voor aanvang geannuleerd wordt, is Opdrachtnemer gerechtigd de verloren mandagen tegen het geldende tarief inclusief eventuele kortingen in rekening te brengen evenals eventuele annuleringskosten voor hotels. Dit voor zover de verloren mandagen en kosten redelijkerwijs niet door Opdrachtnemer kunnen worden vermeden, respectievelijk verkleind. Deze bepaling geldt ook als de opdracht door omstandigheden bij Opdrachtgever of bij door Opdrachtgever ingeschakelde derden geen doorgang kan vinden.

9. Voor het uitvoeren van beveiligingsonderzoeken is het noodzakelijk om de systemen van Opdrachtgever (steekproefsgewijs) aan (penetratie)testen te onderwerpen. Opdrachtgever bevestigt volledig bevoegd te zijn tot het aanvragen en toestaan van ICT-beveiligingsonderzoeken en (penetratie)testen op de systemen en applicaties. Als programmatuur en/of apparatuur eigendom zijn van Derde Partij(en), dan zal Opdrachtgever zorgdragen voor het inlichten van de Derde Partij(en) van de door Opdrachtnemer te verrichten tests. Opdrachtgever moet deze Derde Partij(en) verzoeken om Opdrachtnemer schriftelijke toestemming en vrijwaring voor de tests te geven, conform het gestelde in artikel 5 en 6 van deze overeenkomst. Voordat met de uitvoering van de werkzaamheden kan worden gestart, moet Opdrachtnemer in het bezit zijn van deze toestemming en vrijwaring van Derde Partij(en).

10. Afhankelijk van de soort opdracht moet Opdrachtnemer

- computerapparatuur aansluiten op het netwerk van Opdrachtgever of de bovengenoemde Derde Partij(en), en/of
- door personeel van Opdrachtgever of bovengenoemde Derde Partijen programmatuur laten draaien op de systemen van Opdrachtgever of bovengenoemde Derde Partij(en), en/of
- informatie verzamelen bij Opdrachtgever of bovengenoemde Derde Partij(en) en deze in elektronische vorm meenemen voor verdere analyse, en/of
- data behorende bij de door Opdrachtgever ter beschikking gestelde (test)accounts wijzigen

om de opdracht efficiënt en effectief te verrichten. Opdrachtgever verleent hiervoor toestemming en zal zorgdragen voor toestemming van de Derde Partij(en). Als Opdrachtnemer door Opdrachtgever of Derde Partij(en) wordt beperkt in de uitvoering van haar onderzoek, kan dit leiden tot extra kosten en/of minder diepgang van het onderzoek en/of minder betrouwbare resultaten.

11. Alle mogelijkheden die Opdrachtnemer bekend zijn om systemen en applicaties binnen te dringen, dan wel gegevens aan deze systemen en applicaties te onttrekken, zullen door Opdrachtgever worden toegestaan, met uitzondering van aanvallen waarvan vooraf algemeen bekend is dat die de systemen en applicaties onbereikbaar maken (zogenoemde Denial of Service aanvallen).

12. Eventuele externe tests door Opdrachtnemer zullen worden uitgevoerd vanaf systemen uit het domein madison-gurkha.com waarbij deze systemen zich in een van de volgende netwerkranges bevinden:

    - 88.159.10.0/26
    - 194.151.35.240/28
    - 87.251.52.176/28
    - 2a01:670:310::/48 (IPv6)
    - 2001:7b8:609::/48 (IPv6)

    Als vanaf een ander netwerk wordt getest door Opdrachtnemer, zal dit van tevoren bekend worden gemaakt aan Opdrachtgever.

13. Als personeel van Opdrachtnemer op locatie van de Opdrachtgever haar werkzaamheden moet verrichten, dan zorgt Opdrachtgever voor werkplekken die voldoen aan de geldende Arbo-richtlijnen.

Tarieven en facturering

14. Opdrachtnemer zal de opdracht fixed-price verrichten voor een totaalbedrag van € BEDRAG, inclusief reis- en verblijfkosten binnen Nederland, exclusief BTW. Eventuele additionele werkzaamheden zullen, na schriftelijke toestemming van de Opdrachtgever, afzonderlijk gespecificeerd en gefactureerd worden.

15. Opdrachtgever moet binnen 9 maanden na ondertekening van deze overeenkomst Opdrachtnemer verzoeken de opdracht in te plannen. Na het verstrijken van deze termijn wordt het contractueel afgesproken maximum/fixed-price bedrag in rekening gebracht. Opdrachtgever heeft na dit factureringsmoment nog 3 maanden de tijd om de opdracht alsnog in te laten plannen. Na deze termijn van 3 maanden vervallen de rechten op uitvoering van de opdracht.

16. Betaling van facturen moet binnen 30 dagen na factuurdatum geschieden.

Vertrouwelijkheid

17. Alle informatie en gegevens die tussen Opdrachtnemer en Opdrachtgever worden uitgewisseld of waarvan kennis genomen wordt, waaronder in elk geval programmatuur, voorbereidend materiaal, documentatie, knowhow en bedrijfsgeheimen van Opdrachtnemer en Opdrachtgever, worden als vertrouwelijk behandeld door beide partijen. De partij die vertrouwelijke informatie ontvangt, zal van deze informatie slechts gebruik maken voor het doel waarvoor deze verstrekt is en deze informatie niet aan derden verstrekken of kenbaar maken, tenzij schriftelijk anders overeengekomen tussen partijen dan wel er een wettelijke verplichting tot openbaarmaking van deze informatie is.

18. Als Opdrachtnemer persoonsgegevens, kopieën van paspoorten of andere vertrouwelijke informatie van haar personeel ter beschikking moet stellen aan Opdrachtgever, dan zal Opdrachtgever zorgdragen voor veilige bewaring van deze gegevens conform de Wet Bescherming Persoonsgegevens (WBP) en deze gegevens binnen vier weken na afloop van de opdracht correct vernietigen, behoudens wettelijke richtlijnen die een langere bewaartermijn voorschrijven. Bij overtreding geldt een direct opeisbare boete van € 10.000 onverminderd het recht op volledige schadevergoeding.

Algemene voorwaarden

De algemene voorwaarden van Opdrachtnemer, zoals gedeponeerd bij Kamer van Koophandel XXX te PLAATS op DATUM onder nummer YYYY, zijn aan Opdrachtgever toegezonden. Door ondertekening van deze overeenkomst verklaart Opdrachtgever deze algemene voorwaarden te hebben ontvangen en daarvan kennis te hebben genomen. Deze algemene voorwaarden zijn dan ook van toepassing op deze overeenkomst.

In tweevoud opgemaakt, geparafeerd en ondertekend.

Klantnaam B.V.	**Opdrachtnemer B.V.**
Datum:	Datum:
Naam/functie:	Naam/functie:
Handtekening:	Handtekening:

10 Bijlage 4: Intake formulier webapplicaties

Dit formulier is bedoeld om een zo goed mogelijk beeld te krijgen van de te onderzoeken applicatie om zo een passende offerte uit te brengen. Ook krijgen wij graag in een vroeg stadium een beeld van de aspecten die van belang zijn bij de uitvoering van een test. De vragen daarover in de rubriek randvoorwaarden kunnen eventueel ook direct na gunning worden ingevuld.

1	**Contactgegevens**	
1a	Bedrijfsnaam	
1b	Contactpersoon en functie	
1c	Email	
1d	Telefoon (mobiel)	

2	**Algemeen**	
2a	Wat is de naam van de applicatie?	
2b	Geef een kort beschrijving van de applicatie	
2c	Welke methodiek moet bij het onderzoek worden gebruikt?	Black/Grey/Crystal box/Penetratietst
2d	Welke gegevens moeten worden beschermd en welke risico's ziet de organisatie zelf?	
2e	Gewenste startdatum van het onderzoek	

3	**Indicatie van de omvang/complexiteit**	
3a	Hoeveel schermen telt de applicatie (indicatief)?	
3b	Hoeveel formulieren (indicatief)?	
3c	Hoeveel velden (indicatief)?	
3d	Welke rollen kent de applicatie en welke moeten worden getest?	

3e	Is het een webapplicatie? Of kent het een andere interface, bijv. Soap, fat client, silverlight, flash, etc.	
3e1	Hoe wordt met het systeem verbonden? Is dit HTTP(S) (website), SOAP (API) of iets anders?	
3e2	Is er buiten de standaard web browser nog iets anders benodigd? Zoals Flash, Silverlight, Java, of een fat client.	
3f	Moet ook de server waarop de applicatie draait, worden onderzocht?	
3g	Maakt de onderliggende infrastructuur deel uit van het onderzoek?	

4	**Als ook de broncode onderzocht moet worden (optioneel)**	
4a	In welke taal is de applicatie geschreven en van welke frameworks wordt gebruik gemaakt?	
4b	Uit hoeveel regels code bestaat de applicatie (excl. Html, commentaar en eventuele frameworks)	

5	**Randvoorwaarden**	
5a	Wordt de applicatie intern of extern gehost? Indien extern, bij welke provider? Betreft het dan shared of dedicated hosting?	
5b	Welke organisatie is juridisch eigenaar van het systeem waarop de applicatie draait?	
5c	Wat is de URL/ip adres waarop de test moet plaatsvinden?	
5d	Kan deze URL rechtstreeks worden benaderd of alleen via vpn of met openstelling van de FW, of moet de test onsite? Indien onsite, waar?	
5e	Vindt de test plaats in productie of in een acceptatie/test omgeving?	
5f	Vindt login via username en wachtwoord plaats, of is er sprak van extra bescherming zoals bijv. Tokens of certificaten?	

5g	Wordt de applicatie beschermd door een application level firewall e/o IDS/IPS?	

6	**Aanvullende opmerkingen / aandachtspunten**	
6a	Geef hier uw aanvullende opmerkingen/aandachtpunten	

11 Bijlage 5: Intakeformulier IT-infrastructuur

Dit formulier is bedoeld om een zo goed mogelijk beeld te krijgen van de te onderzoeken IT-infrastructuur om zo een passende offerte uit te brengen. Ook krijgen wij graag in een vroeg stadium een beeld van de aspecten die van belang zijn bij de uitvoering van een test. De vragen daarover in de rubriek randvoorwaarden kunnen eventueel ook direct na gunning worden ingevuld.

Contactgegevens	
Bedrijfsnaam	
Contactpersoon en functie	
Email	
Telefoon (mobiel)	

	Algemeen	
1	**Betreft het een onderzoek vanaf het internet of op locatie op een intern netwerk/dmz?**	☐ Intern netwerk ☐ DMZ ☐ Internet
1a	Welke methodiek moet bij het onderzoek worden gebruikt?	Black/Grey/Crystal box/Penetratietest
1b	Moet een eventueel heronderzoek meegenomen worden in het voorstel	☐ Ja ☐ Nee
1c	Welke gegevens moeten worden beschermd en welke risico's ziet de organisatie zelf?	

1d

	Indicatie van de omvang/complexiteit (Black, Grey Box Penetratietest)	
2	**Welke IP adressen / ranges moeten worden onderzocht? Indien niet bekend, of niet gewenst nu te verstrekken, graag een indicatie van het aantal te onderzoeken IP adressen?**	
2a	Hoeveel systemen zijn vanaf het internet benaderbaar?	

2b

	Indicatie van de omvang/complexiteit (Crystal Box)	
2c	Hoeveel systemen moeten er worden onderzocht?	
	Geef van elk te onderzoeken systeem het operating systeem en de primaire functie (indien gewenst kan ook een infrastructuur ontwerp worden bijgevoegd	

3

3a	Randvoorwaarden	
3b	Welke organisatie is juridisch eigenaar van de te onderzoeken systemen?	
	Wordt de IT-infrastructuur beschermd door een IDS/IPS?	
4	**Als de opdracht op locatie moet worden uitgevoerd, wat is dan het adres van de locatie?**	

4a

4b	Aanvullende opmerkingen / aandachtspunten	
	Geef hier uw aanvullende opmerkingen/aandachtpunten	

5

5a		
5b		
5c		

6		
6a		