



**ANOVUM**

ONDERZOEK | STANDAARDEN | KENNISCENTRUM



De Winter  
Information  
Solutions

**eset**  
Digital Security  
Progress. Protected.

OWASP

PROTEON

pinkroccade  
TSS LOCAL GOVERNMENT

DIVD Academy

GROEN  
OPLOSSINGEN

proxy

UNICORN  
Security

ZCERT

Mathison

Cynalytics



ZOLDER  
applied security research

DIVD

tex

DSEC  
CONSULTING



Ministerie van Volksgezondheid,  
Welzijn en Sport

OpenNovations



Rijksdienst voor Identiteitsgegevens  
Ministerie van Binnenlandse Zaken en  
Koninkrijksrelaties

naga  
CONSULTANCY

M.R.V.A. DE POUS

Innerheight  
Internetdiensten BV

# Pentesting volgens MIAUW



Brenno de Winter (red.)

# Pentesting volgens de Methodiek voor informatiebeveiligin gsonderzoek met auditwaarde

Brenno de Winter (red.)







# Colofon

## **Pentesting volgens de methodiek voor informatiebeveiligingsonderzoek met auditwaarde**

Samenstelling en redactie: Brenno de Winter

© 2024 Jeroen Diel, Mischa van Geelen, Maaike Hielkema, Ministerie van Volksgezondheid, Welzijn en Sport, Victor de Pous, Brenno de Winter

Omslagontwerp: Mischa van Geelen

Vormgeving binnenwerk: Brenno de Winter

Advies en ondersteuning: Hans van der Looy

Non-fictie: Technologie & Samenleving

Druk: Reclameland.nl

Uitgever: De Winter Information Solutions

18 oktober 2024, eerste druk, NIS2-editie



Auteursrechten: Pentesting volgens Miauw © 2024 by Ministerie van Volksgezondheid, Brenno de Winter, Mischa van Geelen, Maaike Hielkema, Jeroen Diel is licensed under CC BY-ND 4.0 - volledige licentie is aan het einde van dit werk opgenomen Je bent vrij om:

*Delen — het materiaal te kopiëren, te verspreiden en door te geven via elk medium of bestandsformaat voor alle doeleinden, inclusief commerciële doeleinden.*

De licentiegever kan deze toestemming niet intrekken zolang aan de licentievoorwaarden voldaan wordt.

Onder de volgende voorwaarden:

*Naamsvermelding — De gebruiker dient de maker van het werk te vermelden, een link naar de licentie te plaatsen en aan te geven of het werk veranderd is. Je mag dat op redelijke wijze doen, maar niet zodanig dat de indruk gewekt wordt dat de licentiegever instemt met je werk of je gebruikt van het werk.*



Daarnaast geldt:

*Geen Afnieuwende Werken — Je mag het veranderde materiaal niet verspreiden als je het werk hebt geremixt, veranderd of op het werk hebt voortgebouwd.*

Tot slot:

*Geen aanvullende restricties — Je mag geen juridische voorwaarden of technologische voorzieningen toepassen die anderen er juridisch in beperken om iets te doen wat de licentie toestaat.*



## Voorwoord

Of een netwerk, systeem of software veilig is, is voor veel mensen lastig weer te geven. Wat is immers veilig? Er zijn officiële certificeringen die naar procedures kijken, maar het technisch testen blijft een ingewikkeld thema. Hoe moet je kijken naar een rapportage als er geen helder kader is? Welke zekerheden heb je dan? En hoe kan een technisch onderzoek dan goed dienen als input voor een certificering? Na diverse incidenten in de industrie, veel ervaringen bij het doen van (technisch) onderzoek naar producten, maar ook naar incidenten is duidelijk dat we meer houvast nodig hebben.

Bij iets fysieks als een woning zijn de maatregelen makkelijk vanaf lijsten te controleren (heb je buitenverlichting, gecertificeerde sloten, verstevigd deurbeslag, een alarmsysteem, camerasytsem en andere zaken). Bij netwerken en software is het speelveld complexer, maar niet wezenlijk verschillend: er zijn verschillende lijsten met onderzoeken (checklists) die je kunt doorlopen. Het is minder magie dan soms in de industrie wordt beweerd. Maar wat zijn tests die je minimaal wilt hebben doorlopen om een beetje een eerlijk beeld van de staat van beveiliging te hebben?



Daarvoor is deze methodiek ontwikkeld. Het doel is helder: een technisch gericht onderzoek moet daadwerkelijk iets op tafel leggen dat zekerheden biedt. Niet alleen voor de directe ontvanger, maar ook bij bijvoorbeeld een auditor moet erop kunnen vertrouwen dat dit onderzoek de vragen beantwoordt. Daarom is de methodiek opgesteld om iedere stap niet alleen navolgbaar maar ook onweerlegbaar te maken. De navolgbaarheid en onweerlegbaarheid maken dat er sprake is van enige auditwaarde. Het is duidelijk wat er is onderzocht, hoe dat is gedaan en wat het resultaat van dat onderzoek is, waarbij het onderliggende bewijs beschikbaar is om onderzoek te reproduceren of beschikbaar te stellen aan bijvoorbeeld toezichthouders zoals bijvoorbeeld de NIS2 dat vraagt. Alles bij elkaar geeft het een waarom u vertrouwen in een product heeft.

Centraal bij de methodiek staat dat het onderzoek gericht is op feitelijk onderzoek op basis van belangrijke en relevante (internationale) standaarden. Wij brengen dat bij elkaar voor onderzoek, rapportage en het bepalen van de ernst van een bevinding als er onvolkomenheden worden gevonden. Door dat uniform te doen praten we over hetzelfde, wordt veel emotie uit het debat gehaald en kan een discussie op inhoud worden gevoerd.



Het levert niet alleen informatie, te zetten stappen, een handleiding om informatie-beveiligingsonderzoek goed in te schatten op. We krijgen inkoopeisen, processschema's en standaardrapportages. Waar mogelijk worden deze in relevante tools meegenomen. Zo sluiten we niemand buiten en is voldoen aan de methodiek niet ingewikkeld en bannen we alle magie uit om tot navolgbaar onderzoek te komen.

Het langslopen van de noodzakelijke eisen kan alleen goed werken als vraag en antwoord goed op elkaar zijn afgestemd. Van vraagstelling tot toetsing van het eindrapport levert de methodiek de nodige informatie en modellen. Waar gaten vielen, zoals bij veel juridische aspecten, hebben we deze zo goed mogelijk opgevuld. Op die manier geeft deze methodiek houvast voor een eerlijk, objectief beeld bij uitgevoerd onderzoek, waarbij de rapportage inkleuring geeft bij de eisen die de Europese wetgever meer en meer stelt aan informatiebeveiliging.

Het informatiebeveiligingsonderzoek met auditwaarde draait om een aantal zekerheden, die aan het onderzoek zijn te ontleden:

1. Duidelijkheid in deskundigheid. Op basis van de certificering is duidelijk dat het onderzoek is uitgevoerd onder verantwoordelijkheid van iemand die afdoende is geschoold.



2. Duidelijkheid in proces. Er is een duidelijk en helder omschreven proces dat volledig is uitgelopen.
3. Duidelijkheid in compleetheid. Op basis van de standaarden, die volledig worden uitgelopen, is er zekerheid dat de testen die minimaal moeten worden uitgevoerd zijn uitgevoerd. Als deze niet relevant zijn of niet kunnen, dan is dat gedocumenteerd. U weet dat er een compleet onderzoek is uitgevoerd.
4. Duidelijkheid over context. Op basis van de beschikbare informatie is precies duidelijk welke context-informatie wel of niet beschikbaar is.
5. Duidelijkheid in scope. Het is duidelijk wat er precies is onderzocht.
6. Duidelijkheid in onderzoek. Het is duidelijk welke onderzoeken er precies zijn uitgevoerd en dat deze passend bij het product zijn.
7. Duidelijkheid in bewijsvoering. Het onderzoeksbewijs is beschikbaar om reproduceerbaarheid te bieden aan anderen (en daarmee auditwaarde aan het onderzoek toe te voegen) en bewijs te bieden dat het onderzoek is uitgevoerd.



8. Duidelijkheid in bevindingen. Bij bevindingen wordt uniform en zo objectief mogelijk gecommuniceerd over gevonden problemen, de impact en mogelijke oplossingsrichtingen.
9. Duidelijkheid in gevolgde standaarden. Bij het uitvoeren van het informatiebeveiligings-onderzoek is houvast gezocht bij internationale standaarden, waardoor duidelijk is welke onderzoeken minimaal zijn uitgevoerd.

Dit document is het product van het bundelen van veel kennis en lering trekken uit incidenten. Natuurlijk staat informatiebeveiliging niet stil en zal het document regelmatig aan de nieuwe praktijk moeten worden bijgesteld. Ondertussen heeft u eindelijk een stuk houvast in handen. Dank aan alle knappe koppen, die dit mogelijk maken. En voor u: succes!



# Inhoudsopgave

Colofon.....	4
Voorwoord.....	7
Inhoudsopgave.....	12
Hoe het allemaal begon.....	13
Het doel van Miauw: in control zijn.....	17
Het bredere plaatje.....	23
De methodiek.....	27
Het CCV-pentestkeurmerk.....	30
Proces van een pentestonderzoek.....	33
De standaarden uit de methodiek.....	48
De rapportage.....	64
Het proces-verbaal.....	67
Juridische aspecten pentesten voor opdrachtgevers.....	70
Voorbeeldvragen opdrachtgevers.....	143



# Hoe het allemaal begon

*Brenno de Winter*

Een klant van mij wil een dienst afnemen van een leverancier. Er zijn wel wat risico's als de beveiliging niet op orde blijkt te zijn. Met de vraag om de due diligence uit te voeren, komt op een gegeven moment het beveiligingsonderzoek in beeld. In dit geval is dat de penetratietest. In overleg met de leverancier ontstaat er een probleem: zij mogen het onderzoek van hun onderzoekers niet aan mij aanleveren. En daarmee is er niets. De leverancier begrijpt dat er daarmee onoverkomelijke bezwaren gaan zijn en dat de deal van tafel is. Het verbaast me, want het onderzoek dat juist een brevet van vermogen had moeten, is nu gegijzeld door de leverancier van de leverancier.

Uiteindelijk komt er een tussenoplossing. Ik mag de test op kantoor van de leverancier lezen. Maar als ik de pagina's doorlees, valt me iets op. Er ontbreekt nog wel wat. De scope is niet helemaal correct en er blijken toch wel bevindingen te zijn. Lang verhaal kort, ik kan niet opschriften dat het goed zit en zonder de nuance (want geheimhouding) zit het voor mijn klant, de afnemer, niet goed. Opnieuw worden we gegijzeld door de onderzoekers. Mijn voorstel is: alles oplossen en een nieuwe test laten uitvoeren. Misschien door een andere



onderzoekende partij. Het werd een hele dure grap, maar uiteindelijk kwam het goed en kon de dienst worden afgenomen. Maar voor mij was het wel een waarschuwing. Met pentesten is iets aan de hand.

Dat gevoel werd versterkt toen ik een klant kreeg die het slachtoffer was van een ransomwareaanval. Het duurde niet lang, voordat een penetratietest werd aangetroffen. In dat document werd juist infrastructuur onderzocht. Vreemd genoeg zou je op basis van het document nooit concluderen dat er iets aan de hand zou zijn met de technische omgeving. Niet lang daarna werd nog iets pijnlijks duidelijk: op basis van openbare bronnen kun je vaststellingen van de onderzoekers snoeihard weerleggen. Het verhaal op papier was niet in lijn met de praktijk en daarmee is de vraag redelijk: Wat klopt er nog meer niet?

Bij een andere klant was er een penetratietest, waarbij alleen de bevindingen te zien waren. Toen deze klant op een eenvoudige manier werd gehackt, kwam de vraag op: waarom staat dit niet tussen de bevindingen? Dit is zo voor de hand liggend. Nergens in het rapport stond vermeld welke precieze tests zijn uitgevoerd. En toen ik erover nadacht, was dat ook niet het geval in de eerdere tests. In het eerste geval omdat het een bedrijfsgeheim was en in het tweede geval omdat men duidelijk een



skilledbasedprobleem had. Maar duidelijk was dat de rapportage niet bood wat het moest bieden.

Toen kwam het moment dat ik in de coronacrisis de verantwoordelijkheid had om pentesten te laten uitvoeren op CoronaMelder. De resultaten moesten naar de Tweede Kamer en zijn onderdeel van het publieke debat. Het laatste waar je dan op zit te wachten is het niet hebben gedaan van noodzakelijke tests, fouten in de rapportage en reden voor debat over meningen van onderzoeken. Daarom werd al snel gegrepen naar uniforme standaarden. Een testgids die volledig is uitgelopen, uniforme beoordelingen van bevindingen en vooral een rapportage waar je van kan zeggen dat het een zekerheid biedt in plaats van een lijst met fouten.

Die aanpak bleek te werken. We waren meer in control, hadden zicht op wat en hoe was onderzocht, hoe de resultaten waren ontdekt. Daarna volgden meer applicaties en coronatesten die moesten bewijzen dat ze veilig genoeg waren. Het proces van toetsen of volgens open regels was gewerkt, zorgde ook voor een eerlijke meetlat. In alle gevallen werd de penetratietest hetzelfde behandeld. Het gaf wat strubbelingen in het begin, want voor de testende organisatie werd inzichtelijk hoe het werd getest en werd er ook op gecontroleerd. Maar het belangrijkste was dat het werkte.



Na de Covid-periode was duidelijk dat dit een asset was om mee te nemen naar het concern van het Ministerie van Volksgezondheid, Welzijn en Sport. Want de regelgeving vraagt steeds meer om in control te zijn en dat te kunnen bewijzen. De penetratietest is bij veel normenkaders een belangrijk onderdeel. Daarom ontstond de methodiek voor Informatiebeveiligingsonderzoek met Auditwaarde of kortweg: Miauw. Daarbij moest er wel een onderdeel bijkomen: die auditwaarde of toetsbaarheid. Dat doen we in het proces-verbaal, waarin een auditor heeft gekeken naar de inhoud van de test, het doorlopen van het proces, de informatie die wordt verstrekt en vooral de correctheid ervan: heeft de pentester echt de certificeringen, zijn de testen doorlopen, is er onderliggend bewijs, wat de bevindingen zijn en hoe worden die uniform ingeschaald? Miauw was geboren.



# Het doel van Miauw: in control zijn

*Brenno de Winter*

Het belang van goed uitgevoerde penetratietesten (pentests) wordt steeds duidelijker nu wetgeving, zoals de NIS2-richtlijn (Netwerk- en Informatiebeveiligingsrichtlijn) die uitmond in de Cyberbeveiligingswet en de aankomende CRA (Cyber Resilience Act), strengere eisen stelt aan organisaties om te bewijzen dat hun systemen veilig zijn. Zowel de NIS als de CRA verplichten organisaties om te kunnen aantonen dat ze "in control" zijn over hun cyberbeveiliging. Dit houdt niet alleen in dat ze hun risico's onder controle moeten hebben, maar ook dat ze in staat moeten zijn om dit met concreet bewijs te ondersteunen. Artikel 15 van de NIS2-richtlijn benadrukt explicet dat organisaties het onderliggende bewijs bij een audit moeten kunnen leveren.

## **Waarom is een goed uitgevoerde pentest essentieel?**

Een pentest is een methodische test waarbij hackers proberen kwetsbaarheden in een systeem te vinden en te exploiteren. Dit helpt een organisatie met inzicht in waar de zwakke punten zitten en hoe deze kunnen worden versterkt. Niet alle pentesten zijn gelijk. Een slecht uitgevoerde pentest kan leiden tot een vals gevoel van



veiligheid: als belangrijke onderdelen van de infrastructuur over het hoofd worden gezien, de test niet voldoende diepgaand is, kan de ontvanger zich veilig voelen, terwijl er nog steeds aanzienlijke risico's bestaan.

Het uitvoeren van een pentest zonder een duidelijke en gedocumenteerde methodologie kan ertoe leiden dat bepaalde risico's niet worden geïdentificeerd. Een veelvoorkomende fout is bijvoorbeeld het uitvoeren van een pentest zonder aandacht voor geavanceerde aanvalstechnieken of insiderthreats. Hierdoor wordt alleen de oppervlakte getest, maar blijven de complexe kwetsbaarheden verborgen. Dit zou een organisatie kwetsbaar kunnen maken voor bijvoorbeeld ransomwareaanvallen, zoals in het geval van de gemeente Hof van Twente, waar een gebrek aan effectieve beveiliging tot ernstige verstoringen leidde. In control zijn betekent dus niet alleen dat je een test uitvoert, maar dat je ook kunt aantonen wat is getest en waarom.

### **Wetgeving als sturend kader**

De NIS2-richtlijn, die verplicht is voor vitale sectoren zoals energie, transport en gezondheidszorg, vereist dat bedrijven hun systemen regelmatig testen en audits uitvoeren om aan te tonen dat hun beveiliging op orde is. Het tonen van onderliggend bewijs, zoals testresultaten, is verplicht. De aankomende Cyber Resilience Act gaat deze



eisen nog verder aanscherpen. Dit houdt in dat organisaties niet alleen moeten testen op technische kwetsbaarheden, maar ook moeten voldoen aan compliance-eisen die worden gesteld door normenkaders zoals ISO 27001, of sectorale standaarden zoals NEN 7510 voor de gezondheidszorg.

De CRA zal bedrijven dwingen om transparanter te zijn over de beveiliging van hun systemen. Dit betekent dat de penetratietesten niet alleen moeten worden uitgevoerd volgens standaarden die inzichtelijk zijn wat er getest is, maar dat de resultaten ook controleerbaar en reproduceerbaar moeten zijn. Het management moet in staat zijn om te bewijzen dat elke stap in het proces is doorlopen en dat alle bevindingen zijn vastgelegd. Dit helpt niet alleen bij het voldoen aan wetgeving, maar versterkt ook het vertrouwen in de algehele beveiligingshouding van de organisatie.

### **Het belang van transparantie en reproduceerbaarheid**

Het uitvoeren van pentests is slechts een deel van het verhaal. Transparantie en controleerbaarheid zijn net zo belangrijk. Wanneer een pentest wordt uitgevoerd, moet het management er zeker van zijn dat de testmethodologie goed gedocumenteerd is. Dit betekent dat testers niet alleen resultaten moeten opleveren, maar ook moeten kunnen laten zien hoe ze tot die resultaten



zijn gekomen. Een duidelijke methodology, zoals de OWASP Testing Guide, is essentieel om ervoor te zorgen dat alle aspecten van de beveiliging worden gedekt.

De inkoop van de pentest moet dus een bewuste keuze zijn, waarbij vooraf duidelijke afspraken worden gemaakt over de scope van de test en de methodology die wordt gevuld. Dit zorgt ervoor dat het management in de rapportage een helder overzicht krijgt welke risico's zijn getest en welke maatregelen moeten worden genomen. Zo kun je juiste beslissingen nemen en blijven voldoen aan de wettelijke verplichtingen.

In control zijn bij een pentest betekent dat je als organisatie niet alleen begrijpt wat er is getest, maar ook waarom dat is gebeurd. Het betekent dat je transparant kunt zijn over het testproces, dat je bevindingen kunt valideren en dat je kunt aantonen dat je je beveiligingsrisico's onder controle hebt. Dit is niet alleen een wettelijke vereiste, maar is ook een cruciaal element van goede bedrijfsvoering in een wereld waar cyberrisico's voortdurend evolueren.



## **De rol van Miauw**

Met de Methodiek voor Informatiebeveiligingsonderzoek met Auditwaarde (Miauw) geven we een inkleuring aan deze noodzaak. Het biedt een gestructureerde aanpak voor penetratietesten door de toetsbaarheid van het proces en de uitkomsten te waarborgen. Miauw zorgt ervoor dat penetratietesten niet alleen vanuit een technisch perspectief worden uitgevoerd, maar ook op basis van een gestandaardiseerde methodologie die zorgt voor reproduceerbare resultaten. Deze methodiek legt nadruk op transparantie, duidelijkheid in de scope en valideerbare bevindingen, waardoor de risico's van een onvolledig of onjuist uitgevoerd beveiligingsonderzoek geminimaliseerd worden.

De meerwaarde van een proces-verbaal van een auditor cruciaal. Hij of zij beoordeelt niet alleen de technische uitvoering van de penetratietest, maar valideert ook het proces en het bewijs dat door de testers is geleverd. Dit zorgt ervoor dat de test voldoet aan alle gestelde eisen en normen, en dat de bevindingen kloppen met de werkelijkheid. Dat waarborgt de betrouwbaarheid van het onderzoek, omdat het aantoont dat de pentest is uitgevoerd door gekwalificeerde professionals, dat alle benodigde tests zijn doorlopen, en dat de bevindingen



correct zijn ingeschaald en ondersteund met bewijs.  
Hierdoor kan een organisatie aantonen dat zij "in control"  
is over haar beveiliging, wat niet alleen voldoet aan  
wettelijke verplichtingen, maar ook het vertrouwen  
vergroot in de veiligheid van de systemen.



# Het bredere plaatje

*Brenno de Winter*

Er zijn verschillende typen beveiligingsonderzoeken die organisaties kunnen uitvoeren om hun systemen, netwerken en applicaties te beschermen tegen dreigingen. Elk van deze methoden heeft een specifieke focus en biedt waardevolle inzichten in de zwakke punten en kwetsbaarheden binnen een beveiligingsinfrastructuur. Hier volgen veelvoorkomende beveiligingsonderzoeken:

De eerste *vulnerability scanning* is een geautomatiseerd proces waarbij een systeem of netwerk wordt gescand op bekende beveiligingskwetsbaarheden. Het doel is om potentiële kwetsbaarheden, zoals verouderde software, zwakke configuraties of ongepatchte systemen, te identificeren en in kaart te brengen..

De vulnerability scanner gebruikt databases met bekende kwetsbaarheden (zoals de CVE-lijst) en vergelijkt deze met de geïnstalleerde software en configuraties op een netwerk of systeem. De scanner genereert een rapport met een lijst van ontdekte kwetsbaarheden.

Voordelen: Dit type onderzoek is eenvoudig, snel en kan regelmatig worden uitgevoerd om een continu overzicht van kwetsbaarheden te behouden.



Nadelen: Het biedt echter geen diepgaand inzicht in hoe deze kwetsbaarheden kunnen worden misbruikt en mist context over de impact van een kwetsbaarheid binnen een specifieke organisatie.

De tweede en kern van dit boek *pentesting* of *penetratietesten* is een meer diepgaande en hands-onbenadering waarbij hackers proberen daadwerkelijk in te breken in een systeem. Het doel is om te ontdekken of kwetsbaarheden kunnen worden misbruikt en om te simuleren hoe een echte aanvaller te werk zou gaan.

Een pentest gaat verder dan een vulnerability scan door daadwerkelijk de aanval uit te voeren en te bewijzen dat een kwetsbaarheid kan worden geëxploiteerd. Dit geeft concrete en actiegerichte inzichten in de beveiliging.

Een derde onderzoek, de code review, is een diepgaande analyse van de broncode van een applicatie om beveiligingsfouten en logische kwetsbaarheden te identificeren. Dit proces kan handmatig worden uitgevoerd door ervaren ontwikkelaars of beveiligingsexperts, of door gebruik te maken van geautomatiseerde tools die de code doorzoeken op bekende kwetsbaarheden.

Omdat de code direct wordt gecontroleerd, kunnen kwetsbaarheden in een vroeg stadium worden



opgespoord voordat de applicatie in productie gaat. Het zorgt ervoor dat beveiligingsproblemen worden ontdekt nog voordat ze misbruikt kunnen worden.

Tot slot is *red teaming* het meest uitgebreide en geavanceerde beveiligingsonderzoek, waarbij een team (het red team) de volledige aanvalsketen simuleert. Dit onderzoek gaat verder dan individuele kwetsbaarheden of systemen. Het probeert de beveiliging van de organisatie op de proef te stellen, inclusief fysieke beveiliging, sociale engineering en bedrijfsprocessen.

Red teaming biedt een realistische kijk op hoe goed de volledige beveiliging van een organisatie functioneert. Het onderzoekt niet alleen technische kwetsbaarheden, maar ook zwakheden in mensen en processen.



Elk type beveiligingsonderzoek heeft zijn eigen focus en biedt specifieke inzichten. Vulnerability scanning is ideaal voor het routinematig opsporen van bekende kwetsbaarheden, terwijl pentesting dieper ingaat op daadwerkelijke aanvalsscenario's. Code reviews zijn essentieel voor het vinden van kwetsbaarheden in de broncode van applicaties, en red teaming biedt de meest uitgebreide benadering door de volledige beveiligingsinfrastructuur van een organisatie te testen, inclusief menselijke en fysieke beveiligingslagen. Door deze onderzoeken te combineren, kan een organisatie een robuust beveiligingsprogramma ontwikkelen dat zowel gericht is op preventie als detectie van aanvallen.



# De methodiek

*Brenno de Winter*

Een methodiek klinkt ingewikkeld. Een schema ziet er intimiderend uit. Maar dat valt best mee. Ons doel is juist om het inkopen, uitvoeren en beoordelen van pentesten eenvoudiger en simpeler te maken. Wat we hebben gemaakt, is uiteindelijk een Excel-sheet. Ja, oké, het was veel werk, maar als het eenmaal gemaakt is, dan is het ook af voor iedereen. Het Miauw-schema biedt een overzichtelijke manier om de eisen, uitkomsten en validatie van penetratietesten te tonen. Dit schema is ontworpen om te verduidelijken wat er gevraagd wordt binnen een onderzoek, wat deze eisen opleveren, wat je mist als deze eisen niet worden nageleefd, en hoe een auditor het voldoen kan toetsen. Daarnaast bevat het schema bij elke eis een relevante inkoopeis die organisaties kunnen hanteren om te garanderen dat het onderzoek voldoet aan de gestelde criteria.

## Hoe het Miauw-schema werkt

Eis en beschrijving: Het schema begint met een duidelijke opsomming van de eisen die worden gesteld aan een informatieveiligingsonderzoek. Deze eisen kunnen variëren van het vastleggen van de digitale rapportage tot het vermelden van verplichte certificeringen van de



onderzoekers. Voor elke eis wordt een beschrijving gegeven die de context van de vereiste verduidelijkt. Zo moet bijvoorbeeld de naam van de rapporteur in de rapportage worden vermeld, wat helpt om de verantwoordelijkheid duidelijk te maken.

**Validatie:** Dit deel van het schema beschrijft hoe de eis kan worden gevalideerd door een auditor. Bijvoorbeeld, als er een eis is dat de rapporteur een geldige certificering moet hebben, is het vaststellen: Is die certificering er? Is er bewijs van? Dit geeft houvast voor auditors om vast te stellen dat iedere eisen met bewijs is ingekleurd.

**Wat levert het op:** Voor elke eis wordt beschreven wat voldoen aan de eis oplevert. Dit kan variëren van het bieden van een hoger niveau van zekerheid tot het vaststellen van de verantwoordelijkheid van de betrokken personen. Door deze voordelen duidelijk te maken wordt het belang van het voldoen aan de eisen benadrukt.

**Wat mis je bij afwezigheid:** Dit onderdeel beschrijft wat er verloren gaat als een eis niet wordt nageleefd. Zo kan de afwezigheid van bepaalde informatie leiden tot onzekerheid over de certificering van de onderzoekers of de verantwoordelijkheid binnen het onderzoek. Dit maakt het voor organisaties duidelijk wat de risico's zijn als niet alle eisen worden gevolgd.



Inkoopeisen: Elke eis wordt gekoppeld aan een inkoopeis, wat betekent dat organisaties bij het inkopen van penetratietesten specifiek kunnen eisen dat aan deze eisen wordt voldaan. Dit zorgt ervoor dat de juiste afspraken worden gemaakt en dat er geen misverstanden zijn over wat er verwacht wordt van de penetratietesters en de rapportage.

En meer dan dit is het niet. We hebben niet opnieuw het wiel uitgevonden, maar bij elkaar geraapt wat er al beschikbaar was en het in een logisch kader geplaatst. Veel in de eisen zult u herkennen uit de eerder geschatte problemen, en als u al meer ervaring heeft met pentesten, is het veel bekende materie.

### **Wat we hebben gemaakt**

Met dit schema hebben we een robuust kader gecreëerd dat ervoor zorgt dat penetratietesten niet alleen op een technisch juiste manier worden uitgevoerd, maar ook op een manier die auditwaarde toevoegt. Door deze gestructureerde benadering kunnen organisaties aantonen dat hun beveiliging onder controle is en kunnen auditors eenvoudig toetsen of het onderzoek aan alle eisen voldoet. Dit proces maakt penetratietesten transparanter, reproduceerbaarder en effectiever in het waarborgen van de veiligheid van systemen.



## Het CCV-pentestkeurmerk

*In Nederland is een levendige industrie op het gebied van informatiebeveiliging. Tussen bedrijven is al enkele jaren het CCV-keurmerk voor pentesting. Wij kregen de vraag of deze schema's niet botsen. Dirk Meij schrijft het antwoord, waar wij ons helemaal achter scharen. - Brenno de Winter*

*Dirk Meij*

Vanuit de brancheorganisatie Cyberveilig Nederland is door de werkgroep Kwaliteit en Transparantie het initiatief genomen voor de CCV-Pentest-certificering. Omdat de werkgroep als doel heeft om de keuze tussen cybersecurityleveranciers eenvoudiger te maken, zijn een aantal initiatieven genomen om dit te faciliteren. Een voorbeeld hierbij is het cybersecuritywoordenboek, waarbij geprobeerd wordt om een eenduidig jargon vast te leggen, uit te leggen en te gebruiken zodat iedereen, publiek en privaat, leverancier en afnemer dezelfde taal spreekt. Een ander initiatief is een aantal certificeringen die door het CCV worden bewaakt waar CCV Pentest er een van is.

De reden voor het maken van de CCV-pentest is om leveranciers aan een minimale set van eisen te laten voldoen. Op deze manier kan een potentiële afnemer



meerdere offertes ophalen en deze onderling vergelijken zonder bang te hoeven zijn dat er een onbehoorlijke pentest wordt uitgevoerd. De leveranciers kunnen hiermee hun interne proces verbeteren om te voldoen aan de minimale eisen. Deze eisen omvatten de minimale rapportage-inhoud, wijze hoe een pentest wordt uitgevoerd en minimale opleidingseisen voor een pentester. De leveranciers zijn natuurlijk vrij in het bieden van extra diensten.

De afnemer kan zoals hierboven gezegd een aantal offertes aanvragen bij verschillende pentestleveranciers. De gecertificeerde worden vermeld in het register van de CCV op haar website. De offertes zijn in de basis allemaal voor hetzelfde product en kwaliteit zoals voorgeschreven. Hierdoor kan de potentiële afnemer zijn aandacht meer leggen op andere dingen die voor hem belangrijker zijn, zoals bijvoorbeeld een 'klik' tussen de afnemer en de leverancier, maar bovenal op de prijs. Het vergelijken van de offertes wordt hiermee sterk vereenvoudigd en de garantie op kwaliteit is geborgd.

Het grote voordeel van het CCV-pentestkeurmerk is dat iedereen in de basis hetzelfde werk gaat doen, met een rapportage die gestandaardiseerd is. Het voordeel hiervan is ten eerste dat rapportages onderling te vergelijken zijn, mochten verschillende pentesten in de loop van de tijd



door andere partijen worden uitgevoerd. Een ander voordeel is dat de rapportage van leverancier A door leverancier B op waarde kan worden geschat, mocht een discussie optreden.

Het nadeel van CCV Pentestkeurmerk is dat er door critici geroepen wordt dat het een 'slager is die zijn eigen vlees keurt', een 'certificaat voor en door cybersecuritybedrijven'. Dit is inderdaad het geval, maar het is tot nog toe het enige certificaat met een kwaliteitsdienst dat door een aantal, naar zichzelf kritische bedrijven is opgesteld waar zoveel mogelijk transparantie is toegepast. Het einddoel, leveren van een pentest met hoge kwaliteit, is wel bereikt en dat is het belangrijkste.

Het initiatief van Miauw is een uitbreiding van het CCV-pentestkeurmerk en geen bedreiging. Het kan alleen maar leiden tot een betere kwaliteit van pentesten en leveranciers van pentesten waar de afnemer uiteindelijk van profiteert. De CCV-certificering biedt een minimale set eisen waardoor een afweging gemaakt kan worden tussen leveranciers met de garantie op inhoudelijk een gelijkwaardig product en de Miauw geeft de leveranciers een zichtbaarheid op kwaliteit levering. De combinatie biedt een basis voor verdere uitbreiding en verbetering van het product pentesten en wij dagen iedereen uit om hier een steentje aan bij te dragen.



# Proces van een pentestonderzoek

*Mischa van Geelen*

## *Waarom processen zo belangrijk zijn*

Het proces rondom pentesten speelt een cruciale rol in de effectiviteit van het beveiligingsonderzoek. Door gestructureerde methodieken en processen te volgen, kan de kans op fouten worden geminimaliseerd en wordt verzekerd dat alle belangrijke aspecten van de IT-infrastructuur grondig worden onderzocht. Een systematische aanpak zorgt ervoor dat niets over het hoofd wordt gezien en dat de resultaten betrouwbaar en reproduceerbaar zijn.

Een goed gestructureerd, gepland en uitgevoerd pentestonderzoek helpt bij:

- Identificeren van (kritische) kwetsbaarheden en risico's: Door systematisch te testen, kunnen verborgen zwakke punten in systemen, applicaties en netwerken worden ontdekt, zodat er tijdig maatregelen kunnen worden genomen om deze te mitigeren.
- Verbeteren van de beveiling van de IT-infrastructuur: Inzicht in de huidige



beveiligingsstatus stelt organisaties in staat om gerichte verbeteringen door te voeren en hun verdediging tegen cyberaanvallen te versterken.

### *De rol van Miauw en open standaarden*

De Methodiek voor informatiebeveiligingsonderzoek met auditwaarde biedt een gestructureerd kader voor het plannen, uitvoeren en rapporteren van pentesten.

Door deze methodiek toe te passen, wordt verzekerd dat pentests volledig zijn, efficiënt worden uitgevoerd en waardevolle resultaten opleveren die direct bruikbaar zijn voor het verbeteren van de beveiliging.

In plaats van het wiel opnieuw uit te vinden, maakt Miauw gebruik van bewezen, effectieve en open-source standaarden voor de inhoudelijke uitvoering van pentests. Enkele van deze standaarden zijn:

- Web Application Security Testing Guide (WSTG) – owasp.org
- Mobile Application Security Testing Guide (MASTG) – owasp.org
- IoT Security Testing Guide (ISTG) – owasp.org



- Penetration Testing Execution Standard (PTES) – ptes.org
- Common Vulnerability Scoring System (CVSS) – first.org

Door deze open standaarden te integreren, wordt niet alleen de kwaliteit van het pentestproces verhoogd, maar ook gezorgd voor consistentie en transparantie in de bevindingen en rapportages.

Als ervaren pentester met meer dan 100 uitgevoerde pentesten weet ik dat het volgen van gestructureerde processen essentieel is voor succesvolle resultaten.

Het stelt ons in staat om systematisch te werk te gaan, de communicatie met de klant te verbeteren en uiteindelijk bij te dragen aan een veiligere digitale omgeving. Zonder een solide proces kunnen kritieke kwetsbaarheden over het hoofd worden gezien, wat kan leiden tot ernstige beveiligingsincidenten.

Door het belang van processen te onderkennen en methodieken zoals Miauw te implementeren, kunnen organisaties hun beveiligingshouding aanzienlijk versterken en beter voorbereid zijn op de steeds evoluerende dreigingen.



## Gevolgen van het ontbreken van standaarden

Het negeren van gestructureerde methodieken en standaarden in pentesting kan ernstige consequenties hebben voor organisaties. Als incidentresponder heb ik uit eerste hand ervaren hoe het mis kan gaan wanneer een pentester zijn werk niet volledig uitvoert door het ontbreken van een gestandaardiseerde aanpak. Dit kan leiden tot onvolledige tests, waardoor kritieke kwetsbaarheden over het hoofd worden gezien.

Wanneer pentesters zonder duidelijke methodologie werken, is de kans groot dat zij niet alle potentiële beveiligingslekken ontdekken. Dit kan zeer ongewenste gevolgen hebben voor de organisatie die de pentest laat uitvoeren. In het ergste geval kan het leiden tot enorme schade, zoals bij een succesvolle hack waarbij gevoelige gegevens worden gestolen of systemen worden platgelegd. De financiële impact en reputatieschade kunnen aanzienlijk zijn, en herstel kan veel tijd en middelen vergen.

In bepaalde situaties heb ik kunnen aantonen dat als de pentest volgens een erkende methodiek was uitgevoerd, de door hackers misbruikte toegangswegen en kwetsbaarheden hadden kunnen en moeten worden geïdentificeerd. Het ontbreken van een gestructureerde aanpak heeft in deze gevallen direct bijgedragen aan het



succes van de cyberaanval. Dit onderstreept het cruciale belang van het volgen van gestandaardiseerde processen in pentesting.

Om ervoor te zorgen dat pentests efficiënt en effectief zijn, is het essentieel om processen te volgen zoals beschreven in Miauw. Deze methodiek biedt een solide framework dat helpt bij het systematisch identificeren van kwetsbaarheden. Door het toepassen van Miauw kunnen pentesters een volledige en grondige evaluatie uitvoeren, waarbij alle relevante aspecten van de beveiliging worden onderzocht.

Het volgen van een gestandaardiseerde methodologie zorgt er ook voor dat de resultaten consistent en reproduceerbaar zijn. Dit is belangrijk voor zowel interne als externe audits. Bovendien verhoogt het de geloofwaardigheid van de pentest en het vertrouwen van stakeholders in de bevindingen en aanbevelingen.



## De voordelen van het volgen van processen

Het hanteren van gestructureerde processen in pentesting biedt meerdere voordelen:

- Gestructureerde en gestandaardiseerde aanpak en rapportages: Dit zorgt voor consistentie in de uitvoering en documentatie, waardoor resultaten gemakkelijker te begrijpen en te vergelijken zijn.
- Grotere kans op succesvolle pentests: Een systematische aanpak verhoogt de kans dat alle kritieke kwetsbaarheden worden ontdekt en aangepakt.
- Minimaliseren van fouten en risico's: Door het volgen van bewezen methodieken worden menselijke fouten verminderd en wordt de kans op over het hoofd zien van belangrijke zwakke punten geminimaliseerd.
- Verminderen van financiële schade door security-incidenten: Tijdige identificatie en mitigatie van kwetsbaarheden voorkomen potentiële kostbare beveiligingsincidenten.
- Auditbaarheid voor zowel opdrachtgevers als opdrachtnemers: Gestandaardiseerde processen maken het eenvoudiger om aan te tonen dat de pentest grondig en volgens de juiste procedures is



uitgevoerd, wat belangrijk is voor compliance en certificering.

Door deze processen te omarmen, kunnen zowel pentesters als organisaties bijdragen aan een veiligere digitale omgeving en het vertrouwen van stakeholders versterken.



## Verloop van een pentest

In dit onderdeel bespreken we de verschillende fases die doorlopen worden tijdens een pentest, gebaseerd op beproefde methodieken en standaarden.

De volgende hoofdstukken zullen elk van de zes fasen in detail toelichten:

1. Intake: Het initiale gesprek waarin doelstellingen en scope worden vastgesteld.
2. Pre-engagement: Het opstellen van het Plan van Aanpak en formele overeenkomsten.
3. Overeenstemming: het bereiken van formele akkoord en het plannen van de test.
4. Uitvoering: Het daadwerkelijk uitvoeren van de pentest volgens de afgesproken methodologie.
5. Afronding: Het samenstellen van de rapportage en kwaliteitscontroles.
6. Validatie door derden (optioneel): De optionele externe beoordeling van de uitgevoerde pentest.

Hierna ga ik dieper in op elk van deze fasen en het belang ervan binnen het pentestproces.



## **Intake**

Tijdens de intakefase wordt de basis gelegd voor een succesvolle pentest. In deze fase vindt er een uitgebreid gesprek plaats tussen het pentestteam en de klant. Voorbeeldvragen die een opdrachtgever zou kunnen stellen zijn achter in het boekje te vinden, in het hoofdstuk 'Voorbeeldvragen'.

Voor je met de intake kunt beginnen, is het verstandig om al een geheimhoudingsovereenkomst te hebben gesloten. Er wordt namelijk informatie uitgewisseld die vertrouwelijk kan zijn. Sommige pentesters zullen bij het gesprek al hun eerste vermoedens van bevindingen opdoen.

Het doel is om de behoeften en verwachtingen van de klant helder te krijgen. Hierbij worden de doelstellingen van de pentest besproken: wat wil de klant bereiken, welke specifieke zorgen zijn er, en welke resultaten worden er verwacht?

Daarnaast wordt in deze fase de scope van de pentest globaal ingeschat. Dit betekent dat er een voorlopige lijst wordt opgesteld van de systemen, applicaties en netwerken die getest moeten worden. Eventuele beperkingen, zoals tijd, budget of technische restricties, worden ook besproken. Het is essentieel om alle



betrokken partijen op één lijn te krijgen om misverstanden in latere fases te voorkomen.

Tot slot wordt er aandacht besteed aan logistieke en organisatorische aspecten. Denk hierbij aan communicatiekanalen, contactpersonen en eventuele benodigde toegangsmiddelen. Door deze zaken vroegtijdig te adresseren, wordt de weg geëffend voor een soepele voortgang van het project.

### **Pre-engagement**

In de pre-engagementfase wordt de informatie uit de intake omgezet in concrete plannen en afspraken. Er wordt een gedetailleerd Plan van Aanpak (PvA) opgesteld dat de methodologie, scope, tijdslijnen en benodigde resources beschrijft. Dit plan dient als blauwdruk voor de pentest en zorgt voor transparantie richting de klant.

Daarnaast wordt er een offerte opgesteld die de financiële aspecten van het project dekt. Hierin worden kosten gespecificeerd voor de verschillende onderdelen van de pentest. De scope wordt formeel bevestigd om ervoor te zorgen dat beide partijen exact weten wat er getest zal worden en onder welke voorwaarden.



Belangrijke juridische documenten zoals vrijwaringsverklaringen worden in deze fase voorbereid en aangeboden. Deze documenten beschermen zowel de klant als het pentest-team en zorgen voor een vertrouwelijke omgang met gevoelige informatie. Alle processen en methodologieën die gehanteerd worden, zijn gebaseerd op open standaarden zoals OWASP MSTG, ISTG, WSTG en PTES, wat bijdraagt aan een kwalitatieve en consistente aanpak.

## **Overeenstemming**

Nadat de klant de offerte en het Plan van Aanpak heeft beoordeeld, wordt er formele overeenstemming bereikt. Dit houdt in dat alle documentatie, inclusief juridische overeenkomsten, wordt ondertekend en geretourneerd. Deze formele goedkeuring is essentieel om verder te kunnen met de planning en uitvoering van de pentest. Om een pentest tot een succes te laten worden, is het ook voor de opdrachtgever belangrijk om in deze fase te valideren of de scope-objecten correct en volledig zijn.

Met de getekende documenten op hun plaats kan het pentestteam beginnen met het opstellen van een gedetailleerde planning. Dit omvat het vastleggen van specifieke data en tijden voor de testactiviteiten, het



toewijzen van teamleden en het regelen van eventuele noodzakelijke toegang tot systemen en locaties.

Bovendien worden in deze fase alle betrokken stakeholders geïnformeerd over de aankomende activiteiten. Dit zorgt voor transparantie en stelt iedereen in staat om zich voor te bereiden op hun rol in het proces. Het bevestigen van de overeenstemming legt de basis voor een gestructureerde en efficiënte uitvoering van de pentest.

## **Uitvoering**

De uitvoering is de kernfase van het pentest-proces waarin het daadwerkelijke testen plaatsvindt. Het pentest-team voert de tests uit zoals beschreven in het Plan van Aanpak en de offerte, met strikte naleving van de afgesproken scope en methodologieën. Hierbij worden zowel geautomatiseerde tools als handmatige technieken gebruikt om kwetsbaarheden en beveiligingslekken te identificeren.

Tijdens de tests wordt er nauwkeurig gedocumenteerd welke stappen er worden genomen, welke systemen worden getest en welke bevindingen er zijn. Dit is cruciaal voor de transparantie en voor het kunnen reproduceren van resultaten. Eventuele scope-objecten die onbereikbaar



zijn of niet getest kunnen worden, worden gedetailleerd gedocumenteerd en aan de klant gerapporteerd, zodat hierop actie kan worden ondernomen.

Na afronding van de testactiviteiten wordt er een uitgebreide rapportage opgesteld. Deze rapportage is gebaseerd op open standaarden en bevat een overzicht van alle bevindingen, inclusief risico-inschattingen en aanbevelingen voor mitigatie. Het doel is om de klant een duidelijk en bruikbaar inzicht te geven in de beveiligingsstatus van hun systemen.

## Afronding

In de afrondingsfase wordt de rapportage verder verfijnd en klaargemaakt voor presentatie aan de klant. De rapportage ondergaat een grondige peerreview binnen het pentest-team om de nauwkeurigheid, volledigheid en kwaliteit te waarborgen. Feedback uit deze review wordt verwerkt om het eindresultaat te optimaliseren.

Alle verzamelde bewijsmaterialen, zoals logbestanden, screenshots en proof of concepts, worden georganiseerd en veilig opgeslagen. Deze materialen ondersteunen de bevindingen in de rapportage en kunnen belangrijk zijn voor eventuele vervolgacties of audits.



Daarnaast worden alle gebruikte checklists en documentatie gecontroleerd en afgevinkt. Dit dient als interne kwaliteitscontrole om te verzekeren dat alle geplande testactiviteiten zijn uitgevoerd en dat er niets over het hoofd is gezien. Het pentest-team bereidt zich hiermee voor op de afsluitende presentatie en eventuele vragen van de klant.

### **Validatie door derden (optioneel)**

In sommige gevallen kan de klant of een externe partij behoeft hebben aan extra zekerheid over de kwaliteit en de resultaten van de pentest. In deze optionele fase wordt er een onafhankelijke validatie uitgevoerd door een derde partij, zoals een auditor.

De derde partij beoordeelt de aangeleverde bewijsstukken, methodologieën en rapportages. Op basis hiervan wordt er een proces-verbaal afgegeven dat bevestigt dat de pentest volgens de juiste procedures en standaarden is uitgevoerd. Dit kan van bijzonder belang zijn voor organisaties die moeten voldoen aan specifieke wettelijke of industrietstandaarden.



Deze extra stap biedt niet alleen meer vertrouwen in de resultaten, maar kan ook bijdragen aan de reputatie van de organisatie op het gebied van informatieveiligheid. Het toont aan dat men bereid is om transparant en grondig te werk te gaan in het beveiligen van systemen en data.



# De standaarden uit de methodiek

*Brenno de Winter*

Er zijn verschillende standaarden, die een rol spelen bij het uitvoeren van pentesten. Voor het uitvoeren van testen zijn er openbaar beschikbare testingguides, testschema's beschikbaar van het Open Web Application Security Project. Zo weet je exact wat in ieder geval aan testen in aanmerking komt. Hierdoor vergeet je geen basale controles uit te voeren.

OWASP biedt verschillende testguides die gericht zijn op het testen van de beveiliging van specifieke soorten applicaties en technologieën. Hieronder volgen enkele belangrijke OWASP-testingguides.

## **OWASP Web Security Testing Guide (WSTG)**

De OWASP Web Security Testing Guide is een uitgebreide handleiding voor het testen van webapplicaties. Het biedt een systematische aanpak om de veiligheid van webapplicaties te beoordelen en omvat verschillende testcategorieën, zoals informatieverzameling, configuratie-management, authenticatie, autorisatie, sessiebeheer, inputvalidatie en meer. De WSTG is geschikt voor pentesters, ontwikkelaars en beveiligingsprofessionals die de beveiliging van webapplicaties willen beoordelen. Het



biedt gedetailleerde technieken en testgevallen om verschillende soorten kwetsbaarheden op te sporen.

### **OWASP Mobile Security Testing Guide (MSTG)**

Deze gids is specifiek gericht op het testen van mobiele applicaties. De MSTG biedt richtlijnen voor het identificeren en analyseren van beveiligingsproblemen in mobiele apps, met specifieke aandacht voor zowel iOS- als Android-platforms. Het omvat tests voor app-beveiliging, gegevensopslag, netwerkcommunicatie, en platformspecifieke bedreigingen. De MSTG is geschikt voor beveiligingsprofessionals en ontwikkelaars, die zich richten op mobiele applicatiebeveiliging. Het biedt methodologieën voor het testen van kwetsbaarheden zoals onveilige gegevensopslag, zwakke encryptie, en onveilige netwerkverbindingen.

### **OWASP API Security Testing Guide**

Deze guide richt zich specifiek op het testen van Application Programming Interfaces (API's). Het biedt een gedetailleerde benadering voor het identificeren van beveiligingsproblemen die specifiek zijn voor API's, zoals authenticatie- en autorisatieproblemen, onveilige



configuraties, en kwetsbaarheden in gegevensverwerking. Deze gids is handig voor pentesters en ontwikkelaars die de veiligheid van API's willen waarborgen. De gids helpt bij het opsporen van kwetsbaarheden zoals onveilige endpoints, onvoldoende toegangscontrole en misconfiguraties.

## **OWASP IoT Security Testing Guide**

Deze gids biedt richtlijnen voor het testen van de beveiliging van Internet of Things (IoT)-apparaten en hun ecosystemen. Het bevat methodologieën voor het testen van verschillende aspecten van IoT, zoals apparaat-firmware, netwerkcommunicatie, hardware-interfaces, en cloud-backend-beveiliging. Geschikt voor beveiligingsprofessionals die zich richten op IoT-beveiliging. Het helpt bij het identificeren van kwetsbaarheden zoals zwakke wachtwoorden, onveilige firmware-updates, en onversleutelde communicatie.

Alle gidsen geven een gestructureerde aanpak voor het beoordelen van verschillende typen applicaties en technologieën. Ze helpen om specifieke kwetsbaarheden te identificeren en aan te pakken, en dragen bij aan een betere beveiligingshouding van software en systemen.



Vaak zie je bij pentesting nog weleens worden verwezen naar de OWASP TOP-10 voor pentesting. Alleen deze lijst bevat geen test en soms zelfs zaken waar je niet technisch op kunt testen, maar op zou moeten auditen.

De OWASP Top-10 is primair bedoeld voor educatieve doeleinden en richt zich op het verhogen van bewustzijn over de meest voorkomende beveiligingsrisico's in webapplicaties. Het biedt een overzicht van veelvoorkomende kwetsbaarheden, zoals SQL-injectie of onvoldoende logging, en is nuttig om ontwikkelaars en securityprofessionals te helpen hun kennis over beveiliging te verbeteren. De OWASP Top-10 is echter geen allesomvattende standaard of testkader voor een penetratietest. Het bevat alleen een set richtlijnen en voorbeelden van kwetsbaarheden die breed worden aangetroffen, maar het is niet geschikt als diepgaand audit- of validatie-instrument.

Een penetratietest vereist veel meer dan alleen het controleren van de OWASP Top-10. Het is een diepgaand proces dat zich richt op zowel technische als contextspecifieke risico's, afhankelijk van de infrastructuur, het bedrijf en de applicatie. Een goed voorbeeld van iets dat niet eenvoudig te testen is aan de hand van de OWASP Top-10, is bijvoorbeeld business logic flaws. Dit zijn kwetsbaarheden in de manier waarop de



applicatie bedrijfsregels implementeert en hoe die regels kunnen worden misbruikt door aanvallers. Businesslogica kwetsbaarheden vereisen een grondige kennis van de applicatiecontext en kunnen niet worden opgespoord door de generieke controle op de OWASP Top-10.

Een ander concreet voorbeeld van wat niet eenvoudig door de OWASP Top-10 gedekt wordt, is het testen van een complex multifactorauthenticatiesysteem dat specifiek is voor de bedrijfsumgeving van een klant. Een kwetsbaarheid waarbij het mechanisme voor authenticatie kan worden omzeild door een combinatie van sessie-overname en timingaanvallen vereist gespecialiseerde penetratietestscenario's die verder gaan dan de bekende OWASP-kwetsbaarheden, omdat het specifieke technische configuraties en bedrijfsumstandigheden vereist om te begrijpen waar het probleem ligt.

Soms wordt nog weleens naar de OWASP Application Security Verification Standard (ASVS) verwezen. Deze nuttige standaard is echter niet geschikt voor het uitvoeren van pentests, omdat het primair is ontworpen als een raamwerk voor het beoordelen van de beveiligingsvereisten van webapplicaties en niet als een hands-on testmethodologie. ASVS richt zich op het definiëren van beveiligingscontroles die in de software-ontwikkelingscyclus geïmplementeerd moeten worden, en



biedt een gedetailleerde lijst van verificatie-eisen voor ontwikkelaars om te volgen. Het specificert geen technieken of procedures voor het daadwerkelijk testen van kwetsbaarheden in een applicatie, zoals pentests dat doen. Belangrijk is wel te beseffen dat voor een *code review* ASVS wel heel nuttig is!

Pentesten zijn gericht op het identificeren van reële beveiligingsproblemen in een applicatie door middel van actieve aanvallen en exploitatie van kwetsbaarheden. ASVS biedt daarentegen een checklistbenadering die eerder geschikt is voor audits en het beoordelen van de volledigheid van beveiligingsmaatregelen, zonder de diepgaande hands-on aanvallen die typisch zijn voor een penetratietest.



## *Standaard voor ernst van bevindingen: CVSS*

Het inschalen van kwetsbaarheden is een essentieel onderdeel van elk beveiligingsproces, en het Common Vulnerability Scoring System (CVSS) biedt hiervoor een gestandaardiseerde aanpak. CVSS helpt beveiligingsprofessionals om kwetsbaarheden een score toe te kennen, variërend van 0.0 (informatief) tot 10.0 (kritiek), waarmee het belang en de prioriteit van de kwetsbaarheden worden bepaald. Deze scores geven een numerieke weergave van de ernst van een kwetsbaarheid en zijn gebaseerd op een combinatie van drie hoofddelen: de Basis Score, de Tijdelijke Score en de Omgevingsscore. Elk van deze delen biedt waardevolle inzichten die helpen bij het beheren van beveiligingsrisico's.

### **Startpunt: De basisscore**

De eerste stap in het inschalen van een kwetsbaarheid is het berekenen van de basisscore. Dit deel van CVSS richt zich op de intrinsieke eigenschappen van de kwetsbaarheid die onveranderlijk blijven, ongeacht de tijd of de specifieke omstandigheden. De basisscore beoordeelt de kwetsbaarheid op twee gebieden: exploitability (hoeveel misbruik kun je ermee maken) en impact (wat zijn de gevolgen).



Bij exploitability wordt gekeken naar factoren zoals hoe de kwetsbaarheid kan worden benaderd (via netwerktoegang of lokaal), de complexiteit van de aanval en of er interactie van de gebruiker nodig is. Dit geeft een idee van hoe gemakkelijk het is voor een aanvaller om de kwetsbaarheid uit te buiten.

De impact wordt vervolgens beoordeeld op drie kernaspecten van informatieveiliging: vertrouwelijkheid, integriteit en beschikbaarheid. Worden gevoelige gegevens blootgesteld? Kan een aanvaller gegevens wijzigen of wissen? Heeft de kwetsbaarheid invloed op de beschikbaarheid van de dienst of het systeem? Elk van deze vragen speelt een rol bij het bepalen van de basisscore, die varieert van 0.0 tot 10.0, waarbij hogere scores wijzen op ernstigere kwetsbaarheden.

### **Tijdelijke score: variabele omstandigheden**

Nadat de basisscore is vastgesteld, komt de tijdelijke score in zicht. Deze houdt rekening met de dynamische factoren die de exploitatie van de kwetsbaarheid beïnvloeden. Denk hierbij aan de beschikbaarheid van exploitcode die misbruik van de kwetsbaarheid vergemakkelijkt, of aan de



beschikbaarheid van een patch of workaround die de gevolgen kan verminderen.

De tijdelijke score voegt een laag aan flexibiliteit toe aan het model, waardoor het mogelijk is om kwetsbaarheden in te schalen op basis van actuele informatie. Als bijvoorbeeld een patch beschikbaar is, kan de tijdelijke score worden verlaagd om rekening te houden met de verminderde dreiging. Dit helpt beveiligingsprofessionals om te reageren op veranderende omstandigheden en kwetsbaarheden beter te prioriteren naarmate er meer informatie beschikbaar komt.

### **Omgevingsscore: de context**

De omgevingsscore voegt een derde dimensie toe aan het model door rekening te houden met de specifieke context van de organisatie. In plaats van kwetsbaarheden alleen op basis van hun technische eigenschappen in te schalen, houdt de omgevingsscore rekening met factoren zoals de waarde van het getroffen systeem, de gevoeligheid van gegevens en de mate waarin een kwetsbaarheid daadwerkelijk kan worden misbruikt in de gegeven situatie.

Met versie 4.0 heeft CVSS meer aandacht besteed aan het toevoegen van contextuele gegevens. Dit betekent dat



tijdens de intake van een pentest gedetailleerde informatie wordt verzameld over hoe en waar de kwetsbaarheden binnen de organisatie impact zouden kunnen hebben. Hoe belangrijk is het getroffen systeem voor de bedrijfsvoering? Wat zijn de gegevens die beschermd moeten worden? Zijn er extra beveiligingsmaatregelen in plaats die de impact kunnen beperken? Deze vragen helpen om de bevindingen niet alleen vanuit technisch oogpunt, maar ook vanuit bedrijfsrisico's te evalueren.

## **Inschaling**

Het inschalen van kwetsbaarheden met CVSS verloopt via een aantal stappen. Het begint met de Basis Score, waarbij de inherente eigenschappen van de kwetsbaarheid worden beoordeeld. Daarna wordt de Tijdelijke Score aangepast op basis van factoren, zoals is er exploitcode beschikbaar en wat kun je doen om de gevolgen te beperken of is er al een oplossing beschikbaar? Ten slotte wordt de omgevingsscore toegepast om de score te verfijnen op basis van specifieke organisatorische context. Het eindresultaat is een score die aangeeft hoe ernstig een kwetsbaarheid is, onderverdeeld in de volgende categorieën:



1. 0.0 – Informatief: Kwetsbaarheden met een score van 0.0 vormen geen direct beveiligingsrisico, maar kunnen nuttige informatie geven voor verbeteringen. Denk bijvoorbeeld aan configuratiewaarschuwingen of informatie die geen directe bedreiging vormt, maar wel aandacht verdient.
2. 0.1 tot 3.9 – Laag: Deze kwetsbaarheden hebben een beperkte impact en zijn moeilijk uit te buiten. Ze vormen geen onmiddellijke bedreiging voor de beveiliging, maar kunnen op termijn wel aandacht nodig hebben om potentiële risico's te minimaliseren.
3. 4.0 tot 6.9 – Middel: Bevindingen in dit bereik zijn reëel en hebben een aanzienlijke impact. Ze zijn niet altijd eenvoudig te exploiteren, maar kunnen bij specifieke omstandigheden toch grote gevolgen hebben voor de beveiliging. Het aanpakken van deze kwetsbaarheden is belangrijk om escalatie van risico's te voorkomen.
4. 7.0 tot 8.9 – Hoog: Deze kwetsbaarheden vormen een significant risico en kunnen gemakkelijk worden uitgebuit. Ze hebben een aanzienlijke invloed op de vertrouwelijkheid, integriteit of



beschikbaarheid van systemen. Actie is vereist om deze problemen snel op te lossen.

5. 9.0 tot 10.0 – Kritiek: Kwetsbaarheden met een score in dit bereik vormen een ernstige bedreiging. Ze zijn vaak eenvoudig uit te buiten en kunnen leiden tot een volledige compromittering van systemen of gegevens. Directe actie is noodzakelijk om schade te voorkomen.

### **De intake is belangrijk voor de score**

Met een goed doordachte aanpak voor de intake van een pentest – waarin de context van de bedrijfsomgeving duidelijk wordt begrepen – kunnen CVSS-scores effectief worden ingezet om actieplannen op te stellen en beveiligingsmiddelen optimaal te gebruiken. Door niet alleen naar de technische details te kijken, maar ook naar de bedrijfsimpact, wordt het risicomanagement afgestemd op de werkelijke behoeften van de organisatie.

Door deze gestructureerde aanpak biedt CVSS niet alleen een numerieke waarde voor kwetsbaarheden, maar ook een holistisch inzicht in de bedreigingen die de organisatie daadwerkelijk kan raken. Dit maakt het een onmisbaar hulpmiddel voor het beheer van



cybersecurityrisico's en de prioritering van herstelmaatregelen.

### *De eeuwige uitzondering: CIS-controls*

Een van de lijsten met checks om uit te voeren zijn de CIS-controls, een set richtlijnen voor informatiebeveiliging, ontwikkeld door het Center for Internet Security. Ze zijn bedoeld om organisaties te helpen hun beveiliging te verbeteren door praktische maatregelen aan te bieden die de kans op beveiligingsincidenten verkleinen. Deze controls richten zich op best practices zoals het inventariseren van hardware, het beheren van software-updates en het instellen van toegangsrechten. Hoewel ze een nuttig kader bieden, betekent het niet voldoen aan een specifieke controle niet automatisch dat een systeem kwetsbaar is; het kan wel wijzen op een verhoogd risico.

Een van de grootste oorzaken van beveiligingsincidenten zijn configuratiefouten. Deze fouten ontstaan wanneer systemen, netwerken of applicaties niet correct zijn ingesteld, waardoor er beveiligingslekken ontstaan. Voorbeelden hiervan zijn slecht geconfigureerde firewalls, databases met onbeperkte toegang of het gebruik van standaardwachtwoorden. Onderzoek toont aan dat 80% van de beveiligingsincidenten verband houdt met onjuiste



configuraties. Dit onderstreept hoe belangrijk het is om configuraties goed te beheren en regelmatig te controleren op fouten.

Configuraties spelen een cruciale rol in beveiliging, omdat ze de toegang en functionaliteit van systemen bepalen. Een goed ingestelde configuratie kan potentiële bedreigingen beperken, terwijl een foutieve configuratie juist kansen voor aanvallers creëert. Configuratiefouten kunnen voorkomen in vrijwel elke omgeving, en vaak zijn ze het gevolg van menselijke fouten, gebrek aan kennis of onvoldoende toezicht.

De CIS-controls helpen bij het identificeren en voorkomen van configuratiefouten door duidelijke richtlijnen te geven over hoe systemen moeten worden ingesteld en beheerd. Ze beschrijven bijvoorbeeld hoe firewall-instellingen kunnen worden geoptimaliseerd, welke toegangsrechten minimaal noodzakelijk zijn en hoe logging en monitoring effectief kunnen worden toegepast. Dit maakt het mogelijk om configuratiefouten vroegtijdig te detecteren en te corrigeren.

Het niet voldoen aan een CIS-control betekent niet direct dat een organisatie kwetsbaar is voor aanvallen. De controls zijn bedoeld als richtlijnen om risico's te verminderen en de algehele beveiligingshouding te verbeteren. Wanneer een controle niet wordt nageleefd,



kan dit wijzen op een potentiële zwakte, maar het betekent niet per se dat een systeem onmiddellijk kan worden uitgebuit. Daarnaast zijn er controls, die simpelweg zo algemeen zijn, waardoor ze niet van toepassing zijn. Neem bijvoorbeeld een mailserver. Op basis van de CIS-controls zal de mailserver een bevinding zijn. Maar voor het doel (mailserver) is dat een logische bevinding dat deze wordt aangetroffen. Ook het niet volgen van een hardeningscontrol kan noodzakelijk zijn om een dienst überhaupt te laten draaien.

De context waarin een configuratiefout zich voordoet speelt een belangrijke rol. Een verkeerde configuratie op een openbare server kan bijvoorbeeld veel gevaarlijker zijn dan dezelfde fout op een intern systeem zonder externe toegang. Dit maakt duidelijk waarom configuratiefouten niet automatisch kunnen worden voorzien van een CVSS-score (Common Vulnerability Scoring System). CVSS is ontworpen om kwetsbaarheden in softwarecode te beoordelen op basis van hun exploitability en impact, terwijl configuratiefouten eerder afhankelijk zijn van omgevingsfactoren en het specifieke gebruik van een systeem. In de rapportage wordt het daarom alleen aangegeven als wel of niet aangetroffen zonder waardeoordeel. De uitleg van de partij die onderzocht wordt, is de input voor de ontvanger van het onderzoek. Die moet namelijk in control zijn.



Configuraties zijn essentieel voor de beveiliging van systemen en spelen een grote rol in het voorkomen van beveiligingsincidenten. De CIS-controls bieden een nuttig kader om configuratiefouten te voorkomen en te corrigeren, maar het niet naleven van een specifieke control wijst niet automatisch op een directe kwetsbaarheid. Door te begrijpen dat configuratiefouten 80% van de incidenten veroorzaken, wordt het belang van goed beheer en controle van configuraties extra benadrukt. Het naleven van de CIS-controls helpt bij het creëren van een robuuste beveiliging, waarbij risico's worden geminimaliseerd en de weerbaarheid tegen aanvallen wordt vergroot. Maar niet voldoen is niet automatisch fout. Een CIS-bevinding is niet meer dan een vaststelling dat een regel niet gevuld is zonder daar direct een waardeoordeel aan te kunnen verbinden. Deze krijgen in de rapportage niet meer dan een vaststelling zonder CVSS-score.



# De rapportage

*Brenno de Winter*

Met het schema van Miauw komt er een sjabloon voor een pentestrappartage mee. Het is gemaakt door Jeroen Diel, Mischa van Geelen, Maaike Hielkema en mijzelf. Dit voorbeeld is ontwikkeld om pentesters een duidelijke en professionele structuur te bieden bij het vastleggen van hun onderzoek en bevindingen. Alle punten uit de methodiek zijn in de rapportage verwerkt. Daarmee is de rapportage in zichzelf ook een hulpmiddel dat niets wordt vergeten.

Deze opzet helpt bij het waarborgen van consistentie in rapportages en zorgt ervoor dat alle belangrijke elementen systematisch worden gedocumenteerd. Het rapport begint met een sectie voor documentbeheer, waarin de basisgegevens van het project worden vermeld, zoals de klantnaam, projectreferentie en de vertrouwelijkheidsclassificatie volgens het Traffic Light Protocol (TLP). Hiermee wordt vanaf het begin duidelijk wie toegang heeft tot het rapport en hoe de inhoud beschermd moet worden. Daarnaast biedt de sjabloon een gedetailleerd overzicht van het versiemanagement, zodat betrokken partijen altijd kunnen terugvinden welke wijzigingen zijn doorgevoerd en door wie.



De sectie over de accreditaties van de auteur speelt een belangrijke rol in het vergroten van de geloofwaardigheid van het rapport. Door relevante certificeringen en kwalificaties van de pentester te vermelden, zoals OSCP of OSEP, samen met bewijsstukken, wordt aangetoond dat de bevindingen zijn opgesteld door een gekwalificeerde professional. Door vervolgens een handtekening te zetten verklaart de professional naar eer en geweten het onderzoek te hebben uitgevoerd. In combinatie met de uitgebreide versiegeschiedenis biedt dit transparantie en geeft het inzicht in de evolutie van het rapport en de genomen stappen.

De Miauw-conceptsjabloon is in de eerste plaats bedoeld om pentesters op weg te helpen, door hen een duidelijke richtlijn te geven voor het opstellen van een professioneel pentest-rapport. Deze laagdrempelige aanpak maakt het voor iedereen, van beginners tot ervaren professionals, mogelijk om een kwalitatief hoogstaand rapport te schrijven dat voldoet aan de professionele normen van het vakgebied. Op deze manier wordt de toegankelijkheid van pentesten vergroot, zodat meer mensen een bijdrage kunnen leveren aan het verbeteren van beveiliging.

Daarnaast is het sjabloon waardevol voor auditors. Zij geven onder de methodiek immers een proces-verbaal af. De opzet van het rapport maakt het namelijk mogelijk om



de bevindingen direct te gebruiken als basis voor verdere juridische documentatie. Een auditor kan op basis van de zorgvuldig gedocumenteerde bevindingen en analyses een proces-verbaal afgeven dat voldoet aan de eisen voor formele rapportages. Hierdoor is de conceptrapportage niet alleen een hulpmiddel voor pentesters, maar ook een essentieel onderdeel in het traject van audit en juridische opvolging, waarmee de kwaliteit en betrouwbaarheid van de hele beveiligingsketen worden verhoogd.



# Het proces-verbaal

*Brenno de Winter*

Na het uitvoeren van een informatiebeveiligingsonderzoek met auditwaarde kan een auditor op basis van het Miauw-schema een procesverbaal opstellen. In dit proces voert de auditor het onderzoek niet opnieuw uit, maar controleert wel per eis of er voldoende bewijs is verzameld. Hierdoor ontstaat een helder overzicht van wat er wel of niet tijdens de penetratietest is gedocumenteerd. Voor de ontvanger is dan duidelijk welke onderdelen van het object zijn onderzocht in de penetratietest, welke bevindingen zijn geregistreerd en of er op basis van deze informatie sprake is van 'in control' zijn.

Het proces-verbaal voegt daarbij een belangrijke meerwaarde toe door de onafhankelijkheid van het onderzoek te vergroten. De betrokken auditor is een externe partij die het werk van de pentester objectief beoordeelt. Dit zorgt ervoor dat er een extra laag van controle wordt toegevoegd, waardoor de organisatie meer zekerheid krijgt dat het onderzoek grondig en volgens de juiste procedures is uitgevoerd. Deze objectieve vaststelling versterkt het vertrouwen in de



bevindingen en zorgt ervoor dat er geen sprake is van eenzijdige interpretaties of gemiste aandachtspunten.

Daarnaast biedt het proces-verbaal waardevolle inzichten voor het management, dat vaak minder technische kennis heeft. Door de bevindingen op een duidelijke en gestructureerde manier te presenteren kunnen zij beter begrijpen wat de resultaten betekenen. Dit helpt bij het nemen van onderbouwde beslissingen over welke risico's prioriteit moeten krijgen en welke maatregelen genomen moeten worden. Het proces-verbaal maakt het voor het management mogelijk om inzicht te krijgen in de mate van compliance en beveiliging zonder diep in de technische details te hoeven duiken.

'In control' zijn betekent dat een organisatie voldoende maatregelen heeft genomen om risico's te beheersen en te voldoen aan relevante wet- en regelgeving. Dit is van groot belang voor wetgeving zoals de Algemene Verordening Gegevensbescherming (AVG), die vereist dat organisaties passende technische en organisatorische maatregelen nemen om persoonsgegevens te beschermen. Daarnaast is het van toepassing op de Wet op het financieel toezicht (Wft) voor financiële instellingen die hun informatiebeveiliging op orde moeten hebben en de NIS2-richtlijn (Netwerk- en Informatiebeveiligingsrichtlijn), die voorziet in hogere



eisen voor cyberveiligheid in sectoren met kritieke infrastructuur. In Nederland wordt dat omgezet in de Cyberbeveiligingswet. Ook kan het proces-verbaal relevant zijn voor de ISO 27001- of NEN7510-certificering, waar strikte eisen worden gesteld aan het naleven van informatiebeveiligingsnormen. In al die gevallen is het onderzoek reproduceerbaar en daadwerkelijk getoetst.

Het proces-verbaal helpt organisaties om aan te tonen dat zij aan deze wet- en regelgeving voldoen, doordat het inzichtelijk maakt welke beveiligingsmaatregelen effectief zijn en waar nog verbeteringen nodig zijn. Dit vergroot niet alleen de naleving van de wet, maar versterkt ook de weerbaarheid tegen beveiligingsincidenten en datalekken, wat bijdraagt aan het beheersen van juridische en financiële risico's.

Kortom, het proces-verbaal vormt een essentieel onderdeel van het auditproces, dat niet alleen de objectiviteit en grondigheid van een onderzoek waarborgt, maar ook helpt om te voldoen aan belangrijke wet- en regelgeving, en zo bijdraagt aan de algehele controle en weerbaarheid van de organisatie.



# Juridische aspecten pentesten voor opdrachtgevers

*Victor de Pous*

## Kernboodschap

Een penetratietest (pentest) is een essentiële vorm van digitaal beveiligingsonderzoek, omdat hiermee proactief kwetsbaarheden in netwerk- en informatiesystemen kunnen worden geïdentificeerd, voordat (on)opzettelijke veroorzaakte incidenten plaatsvinden. Reactief bewijst de pentest onder meer zijn waarde bij de identificatie van de oorzaak, de beoordeling van de schade-omvang en de implementatie van corrigerende maatregelen om herhaling te voorkomen. Kennis van de verschillende juridische aspecten van pentesten is voor iedere van opdrachtgever een basisvoorwaarde voor de rechtmatige en effectieve uitvoering.

## Uitgangspunten

1. Informatiebeveiliging is voor elke organisatie in Nederland een wettelijke verplichting (zorgplicht). Rijkoverheidsorganisaties moeten daarnaast beleidsregels omtrent informatiebeveiliging uitvoeren, zoals onder meer vastgelegd in het Besluit Voorschrift



Informatiebeveiliging Rijksdienst 2007, het Besluit Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie en de Baseline Informatiebeveiliging Overheid (BIO).

2. Onderdeel van deze juridische zorgplicht is het verifiëren of de getroffen risicobeheersmaatregelen zijn geïmplementeerd, worden nageleefd en blijvend adequaat zijn. Ook het verantwoording afleggen hierover is steeds belangrijker geworden vanwege transparantie- en rapportageverplichtingen. Deze en andere processen, zoals incidentrespons, vereisen de uitvoering van digitaal beveiligingsonderzoek.

3. De penetratietest (pentest) is een belangrijke vorm van beveiligingsonderzoek, die een vast onderdeel vormt van een coherent informatiebeveiligingsbeleid en algemeen wordt beschouwd als onmisbaar voor het versterken van de digitale weerbaarheid. VWS Concern gebruikt de volgende werkdefinitie:

*'Een door eigen personeel of derden uit te voeren offensief beveiligingsonderzoek, waarbij gecontroleerd wordt gezocht naar kwetsbaarheden in een of meer beveilige netwerk- en informatiesystemen of onderdelen daarvan, die kunnen worden gebruikt voor het inbreken in deze*



*systemen en/of die zonder opzet of  
autonomoem de gegevensverwerking van de  
onderzochte organisatie kunnen verstoren  
of anderszins nadelige gevolgen kunnen  
hebben'.*

4. Het uitvoeren van een pentest vereist zorgvuldigheid. Feitelijk (technisch en operationeel) richt een pentest zich op het identificeren van zoveel mogelijk kwetsbaarheden zonder schade aan te richten aan de netwerk- en informatiesystemen. Juridische zorgvuldigheid is essentieel bij de opzet, planning en uitvoering van de offensieve handelingen, wat betekent dat er strikte naleving moet zijn van de toepasselijke wettelijke en beleidskaders en de nauwkeurige opvolging van de opdracht (contractueel vastgelegd bij uitbesteding).

5. Bovendien is het belangrijk dat de bevindingen van een pentest herleidbaar, controleerbaar en bewijsrechtelijk van voldoende gewicht (audit-waarde) zijn. De resultaten moeten reproduceerbaar, verifieerbaar, duidelijk, nauwkeurig en voorzien van context en aanbevelingen voor mitigatie zijn. Het volgen van industrienormen en standaarden draagt bij aan de consistentie en betrouwbaarheid.



## Inleiding juridische aspecten

Informatiebeveiliging ('information security') verwijst naar het beveiligen van computersystemen, netwerken en gegevens op basis van de beperking en beheersing van risico's. Het gaat om het geheel van technische, organisatorische en operationele maatregelen dat zich richt op de voortdurende borging van de beschikbaarheid (waarbij gebruikers toegang hebben tot systemen), integriteit (waarbij de verwerkte gegevens volledig en juist zijn) en vertrouwelijkheid (waarbij uitsluitend geautoriseerde gebruikers toegang hebben tot de systemen en gegevens)<sup>1</sup>.

Het brede maatschappelijke belang van informatiebeveiliging vloeit voort uit de bescherming van fundamentele rechten, nationale veiligheid, de continuïteit van diensten, economische stabiliteit en het vertrouwen in de digitale samenleving. Informatiebeveiliging is dan ook een multidisciplinair vakgebied waarin technische, organisatorische en juridische expertise worden geïntegreerd en naadloos samenwerken.

Digitale systemen kunnen echter fouten en andere onvolkomenheden bevatten, waardoor de veiligheid en goede werking van het systeem, netwerk of onderdelen

---

<sup>1</sup> Internationaal wordt er gesproken van 'CIA': confidentiality, integrity, availability (ISO/IEC 27000:2022).



daarvan, zoals computerprogramma's of protocollen, autonoom en zonder opzet wordt verzwakt. Hiervan wordt in toenemende mate misbruik gemaakt door criminale en statelijke actoren.

Feitelijk en juridisch wordt in dit kader vooral gesproken van kwetsbaarheden. In navolging van de EU Cybersecurity Act (CSA) verstaat de herziene Europese EU-richtlijn beveiliging netwerk- en informatiesystemen (NIS2), die op 18 oktober 2024 mede van toepassing wordt op rijksoverheidsorganisaties, onder een '*kwetsbaarheid*': 'een zwakheid, vatbaarheid of gebrek van ICT-producten of ICT-diensten die door een cyberdreiging kan worden uitgebuit' (art. 6, punt 15 NIS2).

Een '*cyberbedreiging*' is volgens het Europese recht: 'elke potentiële omstandigheid, gebeurtenis of actie die netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen kan schaden, verstören of op andere wijze negatief kan beïnvloeden' (art. 2, punt 8 CSA).

Het identificeren van kwetsbaarheden in ICT-systeem vereist zorgvuldig onderzoek. Een essentiële vorm van digitaal beveiligingsonderzoek is de penetratietest (pentest), waarbij de onderzoeker de rol van een kwaadwillige (aanvaller) aanneemt en gecontroleerd probeert binnen te dringen in een netwerk-,



informatiesysteem of een specifiek onderdeel daarvan, zoals een applicatie.

De uitkomst van de pentest moet leiden tot de identificatie van een of meer herleidbare, controleerbare en reproduceerbare bevindingen, die in beginsel vertrouwelijk zijn. Vervolgens rapporteert de pentester deze bevindingen aan de interne of externe opdrachtgever, met een gedetailleerde analyse, omschrijving en classificatie van de kwetsbaarheden, aangevuld met oplossingsgerichte adviezen ter versterking van de digitale weerbaarheid van de onderzochte organisatie.

In deze notitie komen beknopt een aantal juridische aspecten van pentesten aan bod. Dat is noodzakelijk, omdat het recht een belangrijke en duale rol vervult bij het uitvoeren van deze offensieve digitale beveiligingsonderzoeken. Kennis van de juridische aspecten van pentesten:

- Ondersteunt bij het treffen van risicobeheersmaatregelen (zorgplicht) en bij het naleven van andere wettelijke, beleidsmatige en contractuele beveiligingsvoorschriften, waaronder meldplicht en verantwoordingsplicht (*juridische compliance*);



- Biedt attentiepunten voor het effectiever uitvoeren van beveiligingsonderzoeken binnen de dwingendrechte kaders (*waardecreatie*).

Het tweede facet is mogelijk onderbelicht. Door een goed begrip van de juridische kaders kunnen zowel opdrachtgevers als pentesters niet alleen rechtmäßig handelen, maar ook de aanpak optimaliseren. Voor pentesters betekent dit dat zij hun methodologie kunnen aanpassen en verfijnen om binnen de juridische grenzen maximaal resultaat te behalen, wat leidt tot effectievere en efficiëntere beveiligingsonderzoeken.

Beide facetten dragen bij aan de versterking van de digitale weerbaarheid, inclusief het herstelvermogen na een incident, en aan de beperking van het risico op juridische aansprakelijkheid van organisaties.

## Informatiebeveiligingsrecht

Uit oogpunt van goed (openbaar) bestuur is het raadzaam om ten minste basale kennis van het rechtskader van ICT, inclusief informatiebeveiliging, te hebben en toegang tot specialistische kennis ter ondersteuning. Dit uitgangspunt volgt ook de NIS2-richtlijn, die expliciet bepaalt dat zowel informatiebeveiliging als het naleven van deze wet een



bestuursverantwoordelijkheid is. Voor individuele bestuurders geldt onder andere een educatieplicht.

Iedere organisatie is tegenwoordig verplicht ICT te beveiligen, want de juridische vrijblijvendheid van het treffen van beschermingsmaatregelen ligt achter ons. Zo gold deze verplichting voor de houder van een persoonsregistratie sinds de gefaseerde inwerkingtreding van de eerste Nederlandse privacywet, de Wet persoonsregistraties, die op 1 juli 1989 in werking trad.

Informatiebeveiliging wordt momenteel in toenemende mate in wet- en regelgeving voorgeschreven, vooral door de Europese Unie. Dat proces begon met de richtlijn privacybescherming uit 1995, die Nederland door middel van de Wet bescherming persoonsgegevens (Wbp) implementeerde en die op 1 september 2001 in werking trad. Daarnaast is iedere organisatie als contractspartij gebonden aan overeenkomsten met een digitale beveiligingscomponent.

Speciaal voor rijksoverheidsorganisaties is er tevens beleid. Zo gold sinds 1 januari 1995 het Besluit Voorschrift Informatiebeveiliging Rijksdienst (VIR 1994), terwijl nu de versie uit 2007 (VIR 2007) van toepassing is. Overigens waren er al aan het begin van de jaren tachtig



beveiligingsvoorschriften in relatie tot computersystemen en gegevensverwerking voor de Rijksoverheid van kracht<sup>2</sup>.

Het is goed om te beseffen dat de juridische aspecten van informatiebeveiliging breder zijn dan de typische ‘single-issue’ wetgeving of beleid, zoals de Richtlijnen NIS en NIS2 en de Baseline Informatiebeveiliging Overheid (BIO).

Terwijl informatiebeveiliging zich richt op het beperken en beheersen van risico’s die de beschikbaarheid, integriteit en/of vertrouwelijkheid van informatie kunnen bedreigen, is het aandachtsgebied van de juridische aspecten van informatiebeveiliging namelijk aanzienlijk uitgebreider.

Het rechtsgebied omvat naast wettelijke verplichtingen ook definities, rechten en andere juridische normen, zoals regels voor aansprakelijkheid, verboden en toezicht en handhaving. Het informatiebeveiligingsrecht is dan ook een integratievek dat de klassieke, verticale indeling in staatsrecht, privaatrecht, strafrecht en bestuursrecht horizontaal doorkruist.

Deze kwalificatie doet echter niets af aan het feit dat de wettelijke en beleidsmatige zorgplicht tot beveiligen een centraal onderdeel vormt. Hierbij gaat het telkens om het aanpakken van het algemene probleem van een gebrek

---

2 <https://autoriteitpersoonsgegevens.nl/nl/nieuws/nieuwe-eu-brede-regels-avg-boetes-bedrijven-op-komst>



aan beschikbaarheid, integriteit en vertrouwelijkheid van de gegevensverwerking.

## Wettelijke verplichtingen

Diverse wetgeving en beleid verplichten organisaties om risicobeheersmaatregelen te treffen om computersystemen, netwerken, hun gebruikers en anderen te beschermen tegen dreigingen, incidenten en de gevolgen daarvan. Deze juridische zorgplicht geldt in beginsel voor elke organisatie.

Het doel van de maatregelen is om de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens (in feite de verwerking ervan) proactief en preventief te waarborgen. Onder vertrouwelijkheid worden mede begrepen: authenticatie, identificatie en autorisatie, omdat deze begrippen direct gerelateerd zijn aan het beschermen van de toegang tot gegevens.

De focus op alle drie de kernbegrippen is cruciaal voor een evenwichtige benadering van informatiebeveiliging. Dat laat onverlet dat de bescherming van ieder kernbegrip afzonderlijk belangrijk is en dat een schending van één van deze elementen ook een beveiligingsprobleem vormt.

Daarnaast worden reactieve en correctieve maatregelen voorgeschreven om snel en effectief te kunnen reageren



op beveiligingsincidenten, de schade te beperken en herstelmaatregelen te nemen. Behalve de wettelijke zorgplicht – veelal, maar niet uitsluitend, op basis van open, risicogebaseerde en techniekonafhankelijke normen en rekening houdend met de stand der techniek, internationale normen en bijvoorbeeld uitvoeringskosten – gelden er andere dwingendrechtelijke voorschriften.

Een voorbeeld hiervan zijn meldplichten, waaronder informatieplichten bij incidenten en een registratieplicht voor essentiële en belangrijke entiteiten op grond van de NIS2-richtlijn. De registratie helpt autoriteiten om een overzicht te hebben van de relevante entiteiten en zorgt voor een beter gecoördineerde aanpak van informatiebeveiliging op nationaal en EU-niveau.

Daarnaast worden transparantie en ‘accountability’, dat wil in dit perspectief zeggen verantwoording afleggen over informatiebeveiliging, maatschappelijk en juridisch steeds belangrijker. Een cruciaal onderdeel van deze verantwoordingsplicht vormt de documentatieplicht. Organisaties moeten documentatie bijhouden die aantoont welke maatregelen zijn genomen om informatie te beveiligen en de handhaving van die maatregelen.

Verder moeten bestuursleden van een essentiële en belangrijke entiteit in de zin van de NIS2-richtlijn een opleiding volgen (educatieplicht). Bovendien kan er voor



hen persoonlijke aansprakelijkheid ontstaan indien de organisatie de regels niet naleeft. Hieruit volgt nadrukkelijk dat zowel informatiebeveiliging als de rechtskaders hiervan Chefsache zijn geworden. Het gaat om een formele, actieve en inhoudelijke betrokkenheid.

Zo moeten bestuurders over de juiste kennis beschikken om de te treffen risicobeheersmaatregelen te kunnen beoordelen, goed te keuren en toezicht te houden op de uitvoering ervan. Dit is een continu proces, wat mede geldt voor de voorgeschreven opleiding en training, inclusief de rechtsaspecten van informatiebeveiliging.

## Toezicht en sancties

Kenmerkend voor het informatiebeveiligingsrecht is het overheidstoezicht, dat verschillende doelen dient. Dit omvat het waarborgen van naleving van wet- en regelgeving, wat belangrijk is om te verzekeren dat organisaties de vereiste maatregelen implementeren en controleren. Het toezicht draagt bij aan de bescherming van de maatschappij door te zorgen voor de beveiliging van kritieke infrastructuren en diensten die van vitaal belang zijn voor het dagelijkse leven en de economie.



Daarnaast helpt overheidstoezicht bij de preventie van digitale dreigingen door kwetsbaarheden en potentiële risico's te identificeren, aan te pakken en hierover te informeren. Actief toezicht en handhaving door overheidsinstanties zorgen ervoor dat organisaties snel en adequaat kunnen reageren op opkomende dreigingen.

Op overtreding van wettelijke beveiligingsverplichtingen voor netwerk- en informatiesystemen staan doorgaans zware sancties in de vorm van bestuurlijke geldboetes van een toezichthouder. De dreiging van hoge bestuursrechtelijke geldboetes die 'doeltreffend, evenredig en afschrikkend' van aard moeten zijn (onder andere ex art. 83, lid 1 AVG, art. 34, lid 1 NIS2), versterkt doorgaans het belang van de juridische normering en de noodzaak hieraan te voldoen door op naleving te controleren.

De hoogte van bestuurlijke boetes die een Europese toezichthouder voor overtreding van de privacywetgeving oplegt, zijn inmiddels geharmoniseerd<sup>3</sup>. Daarbij geldt de grote van de organisatie het startpunt, gevolgd door de kwalificatie van de ernst van de overtreding: laag, midden en hoog. Hoe dit systeem er op grond van de NIS2-richtlijn uitziet, is nog niet bekend.

---

3 Minister Yesilgöz (Justitie en Veiligheid) in antwoord op vragen.  
Kamerbrief van 31 januari 2021, 3806822.



Een geldboete van een toezichthouder laat onverlet dat degene die schade door een veiligheidsincident heeft naar de burgerlijke rechter kan stappen om vergoeding van toerekenbare schade te vorderen. Bovendien kan men in de Nederlandse rechtspraktijk een stijgende lijn waarnemen bij groepsgeringen op grond van de Wet afwikkeling Massaschade in collectieve actie (WAMCA).

## Onderzoek als juridische zorgplicht

Elke organisatie moet beveiligingsmaatregelen voor netwerk- en informatiesystemen treffen. Bij deze zorgplicht geldt een helder uitgangspunt ten aanzien van verantwoordelijkheden. 'Zoals aangegeven in de Nederlandse Cybersecurity Agenda en de Roadmap Digitaal Veilige Hard- en Software zijn organisaties in de eerste plaats zelf verantwoordelijk voor cybersecurity. Voor softwarefabrikanten geldt dat zij primair verantwoordelijk zijn voor de digitale veiligheid van de door hen aangeboden producten en diensten,' aldus de minister van Justitie en Veiligheid in 2022<sup>4</sup>.

Uit de zorgplicht vloeit de verplichting voort om beveiligingsonderzoeken uit te voeren. Enerzijds gaat het om het controleren of de geïmplementeerde maatregelen effectief zijn en blijven passen bij de actuele dreigingen.

---

<sup>4</sup> Hof van Justitie van de Europese Unie, 6 oktober 2021,  
ECLI:EU:C:2021:811.



Anderzijds is onderzoek vereist als onderdeel van incidentrespons, waarbij ook de oorzaken en gevolgen van beveiligingsincidenten worden geanalyseerd.

Daarnaast zijn beveiligingsonderzoeken noodzakelijk in verschillende andere situaties. Bijvoorbeeld, ze zijn cruciaal na belangrijke systeemwijzigingen, zoals software-updates of systeemmigraties, om te waarborgen dat geen nieuwe kwetsbaarheden zijn geïntroduceerd. Bij het voldoen aan compliancevereisten vormen pentesten een verplicht onderdeel van het beveiligingsbeleid.

Verder moeten ze worden uitgevoerd voorafgaand aan de implementatie van nieuwe applicaties om de beveiliging te garanderen, en als onderdeel van een continu informatie-beveiligingsprogramma om zwakke punten proactief te identificeren en te verhelpen. Tenslotte spelen digitale beveiligingsonderzoeken een rol bij due diligence (onderzoeks- en beoordelingsproces) bij fusies, overnames, of samenwerkingen, om digitale risico's te evalueren.

Algemeen geldt de rechtsregel dat iedereen zich conform de maatschappelijke zorgvuldigheid dient te gedragen. Schending van dit belangrijke rechtsbeginsel door een daad kan onder voorwaarden onrechtmatig zijn (art. 6:162 BW). Het is niet ondenkbaar dat het verzuim van het uitvoeren van een digitaal beveiligingsonderzoek,



waardoor schade is ontstaan, als onrechtmatig wordt beschouwd, indien naast schade ook aan de overige vereisten is voldaan: onrechtmatigheid, toerekenbaarheid, causaliteit en relativiteit.

Bovendien gelden er specifieke wettelijke voorschriften (direct of indirect) met betrekking tot het uitvoeren van beveiligingsonderzoek of staan op de rol:

- Een aanbieder van een essentiële dienst en een digitaledienstverlener zijn verplicht tot het treffen van ‘passende en evenredige technische en organisatorische maatregelen om de risico’s voor de beveiliging van hun netwerk- en informatiesystemen te beheersen’. Hiertoe behoort in ieder geval mede ‘toezicht, controle en testen’ (art. 7, lid 1 onder d Wbni);
- Een gegevensverantwoordelijke en een verwerker moeten beschikken over ‘een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking (art. 32, lid 1 onder d AVG);
- ‘Het is noodzakelijk dat essentiële en belangrijke entiteiten regelmatige beveiligingstests uitvoeren,



zoals penetratietests en kwetsbaarheidsbeoordelingen, om de effectiviteit van hun maatregelen voor netwerk- en informatiebeveiliging te waarborgen' (considerans 52 NIS2).

- Een essentiële entiteit en een belangrijke entiteit moeten een maatregel treffen ten gericht op de 'beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden' (art. 21, lid 1, onder e NIS2).
- 'De in lid 1 bedoelde maatregelen zijn gebaseerd op een benadering die alle gevaren omvat en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen, en omvatten ten minste het volgende;) beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen (art. 21, lid 2, onder f NIS).

Naast de controle op de implementatie en werking van de risicobeheersmaatregelen vereist controle op incidenten aandacht en uitvoering. Ook hiervoor gelden rechtstreekse wettelijke voorschriften (art. 7, lid 1 onder b Wbni, art. 32, lid 1 onder AVG en bijvoorbeeld art. 21, lid 1



onder b NIS2). Een dergelijk incident kan voor de getroffen organisatie mede de algemene juridische verplichting met zich meebrengen tot het voorkomen of beperken van schade (volgens het leerstuk onrechtmatige daad en/of een schadebeperkingsplicht ex overeenkomstenrecht).

Zover bekend definieert de EU-verordening DORA vooralsnog als enige wettelijke regeling expliciet een ('dreigingsgestuurde') penetratietest (art. 3, lid 17 DORA) en verplicht bepaalde financiële entiteiten eenmaal in de drie jaar een dergelijke test uit te voeren (art. 26, lid 1 DORA). De BIO daarentegen verplicht dat overheidsorganisaties hun informatiesystemen jaarlijks controleren 'op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid.

Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of pentesten (art. 8.8.2). De VNG heeft hiervoor een handreiking opgesteld. Zie in dit kader ook de whitepaper Securitytesten van het NCSC. Ook bij het gebruik van DigiD is een jaarlijkse audit verplicht gesteld in de aansluitvoorwaarden voor afnemers en de auditverklaring aan de minister van BZK te sturen.

De verantwoordingsplicht uit de Europese privacywetgeving, zoals vastgelegd in de AVG, heeft invloed op het uitvoeren van digitale beveiligings-



onderzoeken. Volgens artikel 5, lid 2 van de AVG is de verwerkingsverantwoordelijke niet alleen verantwoordelijk voor de naleving van de zes privacybeginselen (waaronder beveiliging), maar moet hij de naleving ook kunnen aantonen ('accountability' in de vorm van een verantwoordingsplicht).

Door regelmatig te onderzoeken, kunnen organisaties aantonen dat zij proactief maatregelen nemen om informatiebeveiliging te waarborgen en te voldoen aan hun verplichtingen. Behalve de privacywet (art. 32, lid 1, onder d AVG) komt deze lijn terug in andere normen, zoals ISO 27001 (algemeen) en bijvoorbeeld NEN 7510 (bijzonder: voor de Nederlandse zorgsector). Het uitvoeren van een pentest is een manier om naleving van de beveiligingsvoorschriften aan te tonen en te bewijzen, die bijvoorbeeld is uitgewerkt in de 'controls' van NEN7510 bij uitbestede softwareontwikkeling (artikelen A.14.2.7, A.14.2.8 en A.14.2.9).

De ontwerpverordening Cyber Resilience Act (CRA), waarvan het Europees Parlement op 12 maart 2024 het Europees Parlement de voorlopige tekst heeft aangenomen, introduceert nieuwe cyberbeveiligingsverplichtingen voor hardware- en softwareproducten die op de EU-markt worden gebracht.



De CRA introduceert onder andere een stelsel van zorgplichten, dat wil zeggen essentiële risicogebaseerde digitale veiligheidsvooraanstaande voor alle producten met digitale elementen (horizontaal) waaraan fabrikanten, leveranciers en importeurs (supply chain) van dergelijke producten moeten voldoen voorafgaand aan het voor het eerst op de interne markt aanbieden en tijdens de levenscyclus van het product, gcomplementeerd met markttoezicht door de overheid.

Belangrijke elementen van de CRA zijn de verplichting voor fabrikanten om security-by-designprincipes toe te passen, het uitvoeren van conformiteitsbeoordelingen en het tijdig melden van kwetsbaarheden en beveiligings-incidenten. De wetgeving legt ook verantwoordelijkheden op aan importeurs en distributeurs om te zorgen dat producten voldoen aan de digitale beveiligingseisen voor ze op de markt worden gebracht.

## Beveiligingsonderzoeken

Er bestaan diverse digitale beveiligingsonderzoeken. Organisaties kunnen op grond van de Europese privacywetgeving (art. 35 AVG) verplicht zijn een '*gegevensbeschermingseffectbeoordeling*' (Data Protection Impact Assessment of DPIA) uit te voeren. Dit is een onderzoek om de privacyrisico's van een



gegevensverwerking in kaart te brengen en vervolgens maatregelen te nemen om de risico's te verkleinen.

Terwijl een DPIA wettelijk bezien betrekking heeft op een voorafgaand onderzoek naar de verwerking van persoonsgegevens, gericht op het identificeren van hoogrisico's voor de rechten en vrijheden van natuurlijke personen, betreft een pentest een offensief onderzoek (dat vooraf, achteraf of doorlopend kan worden uitgevoerd) om kwetsbaarheden in systemen te identificeren, ongeacht de verwerkte gegevens.

Hoewel pentesten slechts beperkt expliciet wettelijk of beleidsmatig worden voorgeschreven, vloeit de verplichting voort uit de zorgplicht, waar het uitvoeren van digitaal bevolkingsonderzoek deel van uitmaakt, in samenhang met het feit dat pentesten gelden als best practice in het kader van informatiebeveiliging.

De Baseline Informatiebeveiliging Overheid (BIO), die sinds 1 januari 2019 voor iedere overheidsorganisatie verplicht is (verplichtende zelfregulering) bepaalt het volgende:

*'Informatiesystemen worden jaarlijks  
gecontroleerd op technische naleving van  
beveiligingsnormen en risico's ten aanzien  
van de feitelijke veiligheid. Dit kan*



*bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of pentesten.  
(artikel 18.2.3.1, 2 BIO).*

Behalve een DPIA en pentest is er de audit, die wordt uitgevoerd door een onafhankelijke en gekwalificeerde onderzoeker (auditor). Zo schrijft de Wet politiegegevens een jaarlijkse privacy-audit voor als periodiek instrument voor het interne toezicht binnen een organisatie (art. 33, lid 1 Wpg). Dit onderzoek richt zich algemeen op de vraag of een organisatie daadwerkelijk doet wat het verplicht is om te doen en bevat in dit geval een stevige beveiligingscomponent vanwege het belang daarvan voor een zorgvuldige omgang met persoonsgegevens.

De audit speelt ook een rol bij de certificering van organisaties volgens de algemene normen voor informatiebeveiliging ISO 27001 en ISO 27002. Deze internationale standaarden zijn tot op heden volgens het Nederlandse recht niet explicet wettelijk voorgeschreven. Dat ligt anders voor de nationale NEN 7510, de sinds 1 januari 2018 verplichte informatiebeveiligingsnorm bij gegevensuitwisseling in de zorgsector (art. 3 Besluit Elektronische Gegevensverwerking Zorgaanbieders).

Een ander type digitaal beveiligingsonderzoek is de '*vulnerability scan*', waarbij een technisch hulpmiddel wordt gebruikt om geautomatiseerd te zoeken naar bekende



kwetsbaarheden in systemen of netwerken. Deze scans vergelijken het systeem met gepubliceerde kwetsbaarheden, zoals die in de CVE-database, om ervoor te zorgen dat bekende beveiligingslekken worden geïdentificeerd en verholpen.

Bij een '*code review*' daarentegen beoordelen een of meerdere programmeurs, die niet betrokken zijn bij de ontwikkeling van de betreffende software, de broncode op kwaliteit in brede zin (leesbaarheid, onderhoudbaarheid, naleving van coding standards en by-design voorvoorschriften), inclusief aspecten van informatiebeveiliging die toezien op de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevensverwerking.

De onderzoeksactiviteit '*red-teaming*' in relatie tot netwerk- en informatiesystemen heeft betrekking op het testen van de digitale veiligheid van systemen, processen en mensen op een manier die verder gaat dan een pentest. Het doel is niet alleen om kwetsbaarheden te identificeren, maar ook om te beoordelen hoe effectief de respons van de organisatie is op een bredere aanvalssimulatie. Red-teaming omvat bijvoorbeeld mede fysieke toegangsverschaffing en social engineering (het verkrijgen van toegang door manipulatie van menselijke interacties).



De Rijksoverheid werkt sinds 2022 aan een normenkader voor securitytesten. De focus ligt op het creëren van een gestandaardiseerde aanpak voor het uitvoeren van securitytesten, zodat deze consistent en effectief zijn. Tegelijkertijd wordt red-teaming opgenomen in de begroting en planning, wat betekent dat deze vorm van beveiligingsonderzoek formeel wordt erkend en gefinancierd.

Zowel de inhoudelijke als procedurele maatregelen zijn nieuw voor de overheid. ‘*Purple-teaming*’ verwijst naar de samenwerking tussen rode en blauwe teams binnen het veiligheidsdomein, waarbij ‘*blue teams*’ opereren vanuit de organisatie zelf om verdedigingstactieken te verbeteren.

## Penetratietesten

Een penetratietest wordt algemeen beschouwd als een essentiële methode om aan de juridische zorgplicht voor informatiebeveiliging te voldoen, zowel proactief als reactief. Ze helpen bij het identificeren van kwetsbaarheden in systemen en processen, en dragen op deze wijze bij aan het versterken van de digitale weerbaarheid; ook na incidenten.

Bij een penetratietest gaat het om het op verzoek en gecontroleerd binnendringen in netwerk- en informatiesystemen, of ten minste een poging daartoe.



Binnendringen zonder toestemming vindt eveneens plaats, maar dan door criminelen, statelijke actoren en hackers. De laatste categorie handelt uit maatschappelijke betrokkenheid en zonder wederrechtelijk oogmerk.

Of de pentest intern of extern wordt uitgevoerd, handmatig of geautomatiseerd, statisch of dynamisch, eenmalig, periodiek of continu (monitoring), of op basis van een combinatie hiervan, het structureel testen van de eigen organisatie geldt als een best practice en cruciaal onderdeel om de proactieve aanpak van informatiebeveiliging te verbeteren en te versnellen. Dit geldt des te meer voor producenten en leveranciers van digitale producten en diensten.

Na een beveiligingsincident kan een pentest reactief helpen om de oorzaak te achterhalen, de schade te beoordelen en kwetsbaarheden te identificeren die zijn misbruikt. Dit ondersteunt het verbeteren van de beveiligingsmaatregelen en het voorkomen van toekomstige incidenten (incidentresponse en -analyse).

Zoals hierboven al beschreven hanteert VWS Concern als werkdefinitie de volgende omschrijving van een penetratietest als verzamelbegrip:

*'Een door eigen personeel of een derde uit te voeren offensief beveiligingsonderzoek,*



*waarbij gecontroleerd wordt gezocht naar kwetsbaarheden in een of meer beveiligde netwerk- en informatiesystemen of onderdelen daarvan, die kunnen worden gebruikt voor het inbreken in deze systemen en/of die zonder opzet of autonoom de gegevensverwerking van de onderzochte organisatie kunnen verstören of anderszins nadelige gevolgen kunnen hebben.'*

De gecontroleerde modus operandi betekent dat het onderzoeksproces zorgvuldig wordt opgezet, gepland en uitgevoerd binnen afgesproken kaders om ervoor te zorgen dat het systeem of netwerk geen vermeidbare schade opleert en dat de test rechtmatig verloopt.

Pentesten kunnen een brede focus hebben en zich richten op algemene onderzoeken naar kwetsbaarheden, maar er bestaat ook een specifiek type pentest dat gebruikmaakt van gedetailleerde informatie over specifieke dreigingen en aanvallerscenario's. Dankzij Verordening DORA is er nu een wettelijke definitie beschikbaar voor dit type test. Een 'dreigingsgestuurde penetratietest' ('threat-led penetration testing' of TLPT) wordt gedefinieerd als:

*'Een kader waarin de tactiek, technieken en procedures van levenschrale, als een*



*reële cyberdreiging ervaren  
dreigingsactoren worden nagebootst en  
waarin een gecontroleerde, op maat  
gesneden, door inlichtingen gestuurde  
(red team) test van de kritieke reëel  
bestaande productiesystemen van de  
financiële entiteit wordt uitgevoerd' (art. 3,  
lid 17 DORA).*

Hieruit volgt dat de diversiteit van pentesten onder andere blijkt uit de informatiepositie van degene die het onderzoek uitvoert. Naarmate de pentester over meer voorkennis en toegangsrechten tot het te testen systeem of netwerk beschikt, valt er meer te onderzoeken en proefondervindelijk uit te proberen. Daarmee verandert ook het scenario. Het is belangrijk te beseffen dat, naarmate de informatiepositie sterker is, als regel ook het aantal bevindingen toeneemt.

In de meest basale vorm is er sprake van een 'black box'-test. Hierbij is alleen de strikt noodzakelijke informatie beschikbaar, zoals een IP-adres of een URL. Bij een 'grey box'-test is meer informatie beschikbaar, zoals details over achterliggende netwerken, systemen en een gebruikersaccount. Een 'white box'-test houdt in dat de onderzoeker volledige toegang krijgt tot het systeem of netwerk, inclusief de broncodes van



computerprogramma's. Hiermee kan een volledig veiligheidsbeeld ontstaan.

Een zorgvuldige bepaling en omschrijving van de scope van een pentest in een Statement of Work (SoW), met onder andere doelbinding, testperiode en vervaldatum, is van groot belang voor zowel de onderzoeker als de te onderzoeken organisatie. Daarbij wegen breedte (omvang: netwerk-, server- en applicatieniveau) en diepte (gelaagdheid van het systeem en toegangsrechten) mee. Voor de pentester geldt dat hij moet weten wat en hoe diep er gepenetreerd moet worden, terwijl de organisatie baat heeft bij een goede, inhoudelijke en zo optimaal mogelijke test om de beveiliging te controleren en te verbeteren.

Het is echter belangrijk op te merken dat deze vaststelling in de praktijk vaak onvolledig of ontoereikend is. Voor de opdrachtgever schort het vaak aan duidelijkheid over het onderzoek, terwijl voor de pentester onvoldoende bepaald is wat het aan te vallen vlak is, totdat verschillende stappen van informatievergaring zijn doorlopen. Dit betekent dat het bereiken van een zo optimaal mogelijke veiligheidscontrole kan vragen om een dynamische opdrachtbeschrijving.



## Geheimhouding

Geheimhouding speelt een belangrijke rol bij het uitvoeren van digitaal veiligheidsonderzoek. Dat geldt wanneer eigen medewerkers de organisatie onderzoeken als bij uitbesteding. Allereerst is er vertrouwelijke detailinformatie over de netwerk- en informatiesystemen en onderdelen daarvan die onderzocht worden, terwijl vervolgens de bevindingen bestaan uit zeer gevoelige informatie over kwetsbaarheden in een systeem. Indien deze informatie en vooral de bevindingen in verkeerde handen valt, kunnen kwaadwillenden de zwakke plekken misbruiken om aanvallen uit te voeren.

Geheimhouding zorgt ervoor dat de resultaten van de pentest alleen beschikbaar zijn voor geautoriseerde personen, wat op zichzelf een risicobeheersmaatregel is, omdat de verplichting helpt om de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevensverwerking via de onderzochte systemen te waarborgen en het risico op digitale aanvallen te minimaliseren. Bovendien beschermt geheimhouding de reputatie van de organisatie en voorkomt het mogelijke juridische en financiële consequenties die uit ongeautoriseerde openbaarmaking voortvloeien.

Wanneer een pentest intern wordt uitgevoerd, heeft de onderzochte organisatie meer controle over wie toegang



heeft tot de gevoelige informatie die tijdens de test wordt verzameld. Dit minimaliseert het risico op informatielekken. Interne medewerkers zijn doorgaans al gebonden aan de bestaande geheimhoudingsprotocollen en arbeidsovereenkomsten, waardoor het eenvoudiger is om ervoor te zorgen dat geheimhouding wordt nageleefd, heeft de organisatie direct zicht op de onderzoeksprocessen, wat helpt bij het snel identificeren en beperken van risico's met betrekking tot informatiebeveiliging.



Bij uitbesteding daarentegen heeft een externe partij toegang tot zeer gevoelige bedrijfsinformatie, wat het risico op het lekken vergroot. Omdat de informatie buiten de directe controle van de organisatie valt, is het essentieel om een geheimhoudingsovereenkomst (Non-Disclosure Agreement) te sluiten met de externe pentester. Dit zorgt ervoor dat alle ontdekte kwetsbaarheden en andere vertrouwelijke informatie beschermd blijven en niet worden gedeeld met derden.

De organisatie moet echter vertrouwen op de externe partij om de geheimhouding te waarborgen, wat het belang van contractuele afspraken over geheimhouding en bijvoorbeeld sancties bij overtreding nog belangrijker maakt. Daarnaast moet de pentestdienstverlener zich houden aan alle relevante wet- en regelgeving en beleid, en kan elke geheimhoudingsinbreuk de uitbesteder schaden.

Een ander laat onverlet dat de openbare resultaten van digitaal beveiligingsonderzoek waarde kunnen hebben in het kader van transparantie, vertrouwen en verantwoordingsplicht. Door bepaalde resultaten van digitaal beveiligingsonderzoek openbaar te maken, kunnen organisaties aantonen dat zij proactief bezig zijn met het identificeren en mitigeren van kwetsbaarheden.



Dit versterkt het vertrouwen van klanten, stakeholders en de samenleving in de veiligheid en betrouwbaarheid van hun systemen, producten en diensten. Bovendien kan het dienen om naleving van wettelijke normen en conformiteitsbeoordelingen aan te tonen, zoals vereist door de AI Act en bijvoorbeeld de aankomende CRA.

## Standaarden

Pentestdienstverleners gebruiken mogelijk eigen methodieken en technieken, terwijl er diverse erkende standaarden beschikbaar zijn. Het toepassen van erkende standaarden kent aantrekkelijke voordelen. Hierdoor wordt een minimaal beveiligingsniveau geborgd en de uniformiteit die door het volgen van deze standaarden ontstaat, voorkomt discussies en conflicten of helpt deze ten minste te beslechten. Ook het werk van een auditor kan niet plaatsvinden zonder standaardisatie.

Het nut van standaardisatie is breder: Standaarden zorgen voor de zorgvuldige vaststelling van het voorwerp van de test, gedetailleerde vastlegging van bevindingen en gestructureerde classificatie van de ernst van bevindingen kunnen dienen als inkoopeisen. Het gaat dan om een programma van eisen (PvE) of een onderdeel daarvan.



Het verdient aanbeveling de beschikbare, open beveiligingsteststandaarden deel van de formele opdrachtverlening voor een penetratietest uit te laten maken. Zo heeft het Open Web Application Security Project (OWASP) een collectie standaarden vastgesteld die gedetailleerd antwoord geven op de vraag wat er getest moet worden.

Nuttig zijn onder andere de top 10 van veel voorkomende beveiligingstekortkomingen, die eveneens beschikbaar is voor applicatieprogrammeerinterfaces (API), voor awareness. Op basis van deze lijsten kan een penetratietest niet langer volstaan met uitsluitend een scan, omdat er ook fouten worden benoemd die het noodzakelijk maken de klant te bevragen. Andere OWASP-standaarden zien toe op het testen van webapplicaties (WSTG) en mobiele applicaties (MSTG). Het simpelweg uitvragen van standaarden waarborgt een minimaal niveau en veronderstelt een white box- of grey box-test.

Ook zijn er standaarden beschikbaar voor de verslaglegging van de bevindingen van een onderzoek. De Penetration Testing Execution Standard vermeldt nauwgezet op welke wijze een test kan worden opgetekend. In combinatie met de eis dat het onderzoek dusdanig moet worden uitgevoerd dat het reproduceerbaar is, is het nu mogelijk om bij twijfel een



zinvolle contra-expertise uit te laten voeren op (delen van) het onderzoek. Deze reproduceerbaarheid is van groot belang voor juridische en compliance-doeleinden. De betrouwbaarheid en herhaalbaarheid van de test zijn dan cruciaal.

Vervolgens biedt het Common Vulnerability Scoring System (CVSS) een gestandaardiseerde methode voor het classificeren en rapporteren van kwetsbaarheden, waarbij de ernst van een kwetsbaarheid wordt beoordeeld op een schaal van 0 (informatief) tot 10 (zeer ernstig).

Deze scoringmethode houdt rekening met diverse factoren, zoals potentiële impact van de kwetsbaarheid, exploitatiecomplexiteit en beschikbaarheid van een 'exploit' (een stukje software, code of een reeks commando's die gebruikmaakt van een kwetsbaarheid of fout in een systeem, software of netwerk om ongewenste of ongeautoriseerde acties uit te voeren).

Daarnaast kan de CVSS-score worden aangepast aan de specifieke context van een organisatie, waardoor de score een context-specifieke weergave van risico's biedt. Dit stelt organisaties in staat om kwetsbaarheden niet alleen op technisch niveau, maar ook in het kader van bedrijfscontinuïteit en operationele impact te evalueren.



Veel organisaties hanteren een CVSS-score van 4 of hoger als drempelwaarde, waarbij een dergelijke score wordt gezien als een blokkade voor de livegang van nieuwe of gewijzigde informatiesystemen. In deze context fungeert de CVSS-score als een objectieve risicomaatstaf die organisaties ondersteunt bij het vaststellen van hun risicobereidheid en -tolerantie. Aangezien elke organisatie unieke risicoprofielen en beveiligingsvereisten heeft, kunnen zij aanvullende drempelwaarden definiëren, afhankelijk van hun eigen risicomagementstrategieën en beveiligingsbeleid. Dit leidt tot een meer gepersonaliseerde en afgestemde aanpak van kwetsbaarheidsbeheer.

Terwijl geheimhouding van de bevindingen van een pentest uit oogpunt van digitale weerbaarheid niet ter discussie staat, kan het voor opdrachtgevers een strategische keuze zijn om na een succesvolle (her)test de bevindingen met belanghebbenden te delen.

Dit draagt bij aan verhoogde transparantie en versterkt het vertrouwen in de geïmplementeerde beveiligingsmaatregelen van de organisatie. Daarnaast kan openbaarmaking bijdragen aan het voldoen aan externe compliance- en certificeringseisen, zoals ISO 27001, wat de beveiligingspositie van de organisatie verder versterkt en de naleving van industrietstandaarden aantoon.



## Pentest als contractuele voorwaarde

Indien een toeleverancier contractueel verplicht is om de gegevensverwerking van zijn opdrachtgever te beveiligen, moet deze zorgplicht die voortvloeit uit de AVG en NIS2-richtlijn contractueel worden geborgd. Dit houdt in dat de toeleverancier niet alleen passende maatregelen moet implementeren, maar ook actief moet controleren of deze maatregelen effectief zijn en blijven, door middel van digitale beveiligingsonderzoek. Deze verplichtingen moeten duidelijk in de contracten worden vastgelegd om naleving te waarborgen en de aansprakelijkheid in geval van niet-naleving te regelen.

In toenemende mate wordt echter de verplichting tot het uitvoeren van digitale beveiligingsonderzoek, inclusief risico-inschattingen zoals een DPIA, opgenomen in overeenkomsten indien wetgeving dit niet voorschrijft. Deze ontwikkeling weerspiegelt een groeiende trend om proactief de hogere beveiligingsstandaarden na te leven en risico's te beperken.

Bij de toenemende aandacht voor de versterking van de digitale weerbaarheid en de zoektocht naar meer kwaliteitswaarborgen en zekerheden kan de gebruikersorganisatie dezelfde lijn volgen ten aanzien van pentesten. In dit gevolg wordt een pentest als voorwaarde



opgenomen als onderdeel van een contract voor de levering van een product of dienst.

De uitkomst van een pentest geeft inzicht in de status van de informatiebeveiliging op een specifiek moment en in een specifiek geval, waardoor discussies en conflicten kunnen worden voorkomen. Door de bevindingen vast te leggen in een duidelijk en gedetailleerd rapport met auditwaarde, beschikken alle partijen over een gemeenschappelijke basis, wat de samenwerking en communicatie aanzienlijk verbetert.

Bovendien kunnen een codereview, DPIA en penetratietest elkaar aanvullen. Een DPIA helpt bij het identificeren en evalueren van privacyrisico's, een code review richt zich op het opsporen van fouten en beveiligingsproblemen in de broncode van software, terwijl een pentest aanvallen simuleert om kwetsbaarheden in netwerk- en informatiesystemen te ontdekken. Samen vormen deze onderzoeken een holistische benadering van informatiebeveiliging, waarbij verschillende aspecten worden gedekt.

Een dergelijke pentestclausule leidt vervolgens in een afzonderlijke overeenkomst voor de penetratietest tussen de opdrachtgever en de externe pentestdienstverlener. De overeenkomst specificeert de scope, doelstellingen, methodologie en rapportagevereisten van het



beveiligingsonderzoek, wat zorgt voor heldere verwachtingen en verantwoordelijkheden.

Door deze afspraken worden niet alleen de informatiebeveiliging verbeterd, maar ook de transparantie en het vertrouwen tussen partijen bevorderd. Daarnaast draagt een duidelijke contractuele basis bij aan juridische zekerheid en naleving van relevante wet- en regelgeving en beleid.

## Pentestovereenkomst

De hoofdregel is onmiskenbaar: voer geen penetratietest uit zonder uitdrukkelijke toestemming van een bevoegde vertegenwoordiger van de eigenaar of bestuurder van de organisatie die de te onderzoeken ICT-systeem in gebruik heeft. Zonder deze toestemming kan zelfs de handeling van louter het scannen van netwerk- en informatiesystemen onder het delict computervredebreuk (art. 138ab Sr) vallen.

De toestemming is nauw verbonden met de omvang en diepgang (reikwijdte of 'scope') van het beveiligingsonderzoek, zoals vastgelegd in een Statement of Work (SoW). Naast toestemming verleent de opdrachtgever doorgaans diverse vrijwaringen aan de pentester.



Bij uitbesteding kwalificeren de afspraken met een externe veiligheidsdienstverlener als een overeenkomst tot opdracht (art. 7:400 BW). Op basis van een in het contract opgenomen vrijwaringsbeding wordt een partij gevrijwaard.

In deze context verkrijgt de pentester bescherming tegen vorderingen, zoals een claim tot betaling van schade die door de test is ontstaan en door een derde (of de opdrachtgever) bij hem wordt neergelegd. In geval van claims van derden neemt de opdrachtgever deze over, waardoor de pentester buiten schot blijft.

Indien een contractspartij haar eigen aansprakelijkheid beperkt of uitsluit, wordt dit juridisch exoneratie genoemd. Het gebruik van een vrijwaringsbeding en exoneratiebeding in algemene voorwaarden is onderworpen aan de kaders van het Burgerlijk Wetboek.

Dit laat onverlet dat iedere (offensieve) digitale beveiligingstest in opdracht altijd zorgvuldig moet worden uitgevoerd. ‘De opdrachtnemer zal bij de uitvoering van zijn werkzaamheden de zorg van een goed opdrachtnemer in acht moeten nemen,’ aldus art. 401 BW.

Daarbij gaat het om handelen conform objectieve kwaliteitseisen die aan een redelijk bekwaam en redelijk handelend pentester in het concrete geval mogen worden



gesteld. Dit betreft een open minimumnorm. Er wordt getoetst aan het niveau van een gemiddelde vakgenoot, tenzij anders blijkt.

Het is bijvoorbeeld vereist dat de pentester zijn opdrachtgever niet onnodig blootstelt aan voorzienbare en vermijdbare risico's. Bovendien bestaat de mogelijkheid dat een pentester zijn opdrachtgever vrijwaart tegen claims van derden, indien hij bijvoorbeeld buiten de afgesproken scope handelde of anderszins grove schuld heeft bij een incident. In dat geval handelt de pentester de claims van derden af.

Zowel het element van expliciete toestemming als vrijwaring kan mede afhankelijk zijn van de gebruikte technische hulpmiddelen (tooling, zoals scanning software) bij het uitvoeren van een pentest. Uit theorie en praktijk blijkt dat de scope van een digitaal beveiligingsonderzoek vaak pas wordt ontdekt of vastgesteld bij de uitvoering van scans.

Dit betekent vervolgens dat toestemming geven en vrijwaren voor de uitvoering soms eerder een iteratief proces is dan een eenmalige, voorafgaande handeling op basis van vaststaande gegevens. Het gaat dan om een proces van herhaalde beslissingen dat om continu aandacht vraagt van een beslissingsbevoegde medewerker of manager van de geteste organisatie



(opdrachtgever); iemand die deze verantwoordelijkheid formeel heeft en bevoegd is om toestemming te geven om een object op een bepaald niveau te scannen.

## Verwerkersovereenkomst

Bij uitbesteding van een digitaal beveiligingsonderzoek is het vaak onvermijdelijk om naast de overeenkomst van opdracht ook een verwerkersovereenkomst in de zin van de AVG te sluiten met de externe pentester. Dit heeft te maken met de mogelijkheid dat de onderzoeker bij de uitvoering van de test onverhooppt toegang kan krijgen tot persoonsgegevens die de opdrachtgever verwerkt.

De wet vereist dat indien een verwerkingsverantwoordelijke (opdrachtgever) een verwerker (externe pentester) inschakelt om gegevens namens hen te verwerken, er een schriftelijke overeenkomst moet zijn die de verantwoordelijkheden en verplichtingen van beide partijen vastlegt (art. 28 AVG). De overeenkomst moet specifieke bepalingen bevatten over onder andere de aard en het doel van de verwerking, de duur van de verwerking en de soorten persoonsgegevens die worden verwerkt.

Daarnaast is het ook in dit kader belangrijk om te beseffen dat de wet gegevensverwerking breed definieert, wat



betekent dat bijna elke handeling die betrekking heeft op persoonsgegevens onder de term 'verwerking' valt:

*'een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens' (art. 4, lid 2 AVG).*

Dit omvat bijvoorbeeld het lezen, kopiëren of analyseren van gegevens tijdens een penetratietest. Bij uitbesteding blijft de opdrachtgever (van bijvoorbeeld een penetratietest) te allen tijde zelfverantwoordelijk voor de persoonsgegevens die hij verwerkt.

De AVG verplicht bij uitbesteding van de verwerking van persoonsgegevens het sluiten van een verwerkersovereenkomst. Daarbij geldt in dit kader de opdrachtgever als gegevensverantwoordelijke en de



onderzoeker als verwerker (art. 28 AVG); een zienswijze die door een privacytoezichthouder in een EU-lidstaat is bevestigd.

Zonder verwerksovereenkomst ontbreekt een verwerkingsgrond voor de pentester en kan hij in voorkomende gevallen de wet schenden. Op grond van de verwerksovereenkomst verkrijgt de pentester voorafgaand toestemming om eventueel persoonsgegevens te downloaden, aangevuld met de verplichting om de gegevens vervolgens naar keuze van de opdrachtgever onomkeerbaar te vernietigen of desgewenst terug te geven.

## Auteursrechtelijke aspecten

Op digitale technologie, zoals computerprogramma's, rusten doorgaans intellectuele eigendomsrechten. Daarbij spelen computerprogramma's in verschillende vormen en het daarop geldende auteursrecht een overheersende rol, zowel voor leveranciers als gebruikersorganisaties. De meeste software die een organisatie gebruikt, is in licentie gegeven door de auteursrechthebbende en/of bevoegde leverancier. De rechtsverhouding tussen partijen wordt geregeld door het wettelijke auteursrecht (artt. 45h-45n Auteurswet), de gebruiksovereenkomst en andere afspraken zoals vastgelegd in een onderhoudsovereenkomst.



Het uitvoeren van een penetratietest op software (computercode) waarop een ander de eigendomsrechten heeft, roept de vraag op of hiervoor toestemming van de auteursrechthebbende vereist is. Deze intellectuele eigendomswetgeving verleent de maker sterke beschermingsrechten. De rechthebbende kan exclusief over zijn eigen werk beschikken.

Het auteursrecht betreft het exclusieve recht van de maker of diens rechtverkrijgenden om de computercode openbaar te maken en te verveelvoudigen, behoudens de beperkingen die bij wet zijn gesteld (art. 1 Auteurswet). Dit geldt ook voor software: besturingssystemen, toepassingsssoftware en interfaces, zoals gebruikersinterfaces (UI) en applicatieprogrammeerinterfaces (API).

De wet benoemt en regelt het testen van een computerprogramma. De rechtmatige gebruiker (licentienemer) mag de software van de producent testen, maar deze handelingen moeten zich beperken tot het achterhalen van de aan de software ten grondslag liggende ideeën en beginselen (art. 45I Aw). Een onderzoek naar veiligheidsbreuken valt hier in beginsel niet onder.

Het Nederlands recht kent geen expliciete uitzondering voor beveiligingsonderzoek, maar het uitvoeren van een



penetratietest zonder het maken van kopieën of het verspreiden van de onderzochte software valt in beginsel binnen de kaders van de Auteurswet. Dit komt doordat er op deze wijze geen inbreuk wordt gemaakt op de exclusieve rechten van de auteursrechthebbende.

Het is echter belangrijk dat technische beschermingsmaatregelen, zoals Digital Rights Management (DRM), niet mogen worden omzeild, aangezien dit in strijd is met de auteursrechtelijke bescherming en als een ontoelaatbare handeling wordt beschouwd onder de Auteurswet.

Volgens de Auteurswet (art 45j, lid 1 Aw) mag degene die bevoegd is een computerprogramma te gebruiken (licentienemer), 'zonder toestemming van de auteursrechthebbende, alle handelingen verrichten die noodzakelijk zijn voor het in overeenstemming met zijn bestemming gebruiken van het computerprogramma, met inbegrip van het verbeteren van fouten.'

Dit brengt in beginsel met zich mee dat bepaalde vormen van testen, zoals het identificeren van beveiligingsfouten<sup>5</sup>,

---

5 De CVE-lijst (Common Vulnerabilities and Exposures) is een internationale database die bekende beveiligingskwetsbaarheden in software en hardware identificeert en categoriseert. Elke kwetsbaarheid krijgt een uniek CVE-ID, wat zorgt voor consistente en gestandaardiseerde rapportage over beveiligingslekken. De lijst helpt beveiligingsprofessionals, ontwikkelaars en organisaties bij het snel



onder noodzakelijk gebruik kunnen vallen en dus geen aparte toestemming van de auteursrechthebbende vereisen.

In het geval de uitvoering van een penetratietest wel als verveelvoudiging kan worden beschouwd, vooral indien er tijdelijke kopieën van de software worden gemaakt. In dat geval is voorafgaande toestemming van de auteursrechthebbende op de computercode juridisch noodzakelijk.

## Recht op fouterherstel door licentienemer

Beveiligingsonderzoek kan leiden tot de identificatie van kwetsbaarheden, welke bevindingen vervolgens om actie vragen om de veiligheid van digitale technologie en processen te verbeteren, onder andere door het verhelpen van fouten in software. Volgens het contractenrecht is de softwareproducent in beginsel verplicht om gebreken in een computerprogramma te verhelpen indien de computercode niet voldoet aan de vastgelegde specificaties, waaronder ook veiligheidsgebreken vallen. Deze verplichting is gebaseerd op wettelijke bepalingen zoals de conformiteitseis, de

---

identificeren van kwetsbaarheden, zodat ze patches of beveiligingsmaatregelen kunnen implementeren om de risico's te verkleinen. De CVE-lijst wordt beheerd door het MITRE-organisatie in samenwerking met beveiligingsgemeenschappen wereldwijd.



regels rondom gebrek aan nakoming en de principes van redelijkheid en billijkheid.

Door middel van de gebruiksvoorwaarden (licentieovereenkomst) en algemene voorwaarden proberen softwarefabrikanten echter hun verplichting af te zwakken. Dit gebeurt bijvoorbeeld door clausules op te nemen waarin wordt gesteld dat het geleverde computerprogramma niet foutloos is en niet zonder onderbreking kan werken.

Ook wordt een computerprogramma soms geleverd 'zoals deze is' ('as is'), zonder enige garanties of waarborgen, expliciet of impliciet, over de kwaliteit, functionaliteit of geschiktheid van het product. Bovendien is de volgende clausule gangbaar: 'De producent is niet aansprakelijk voor enige schade die voortvloeit uit het gebruik van de software, inclusief maar niet beperkt tot onderbrekingen of fouten in de software.' De afdwingbaarheid van dergelijke clausules kan echter variëren. In sommige gevallen, zoals bij consumentencontracten of bij grote nalatigheid, kunnen dergelijke clausules worden beperkt of ongeldig verklaard.

Hoe het ook zij, de Leidraad Coordinated Vulnerability Disclosure uit 2018 gaat uit van een termijn van 60 dagen voor het verhelpen van de kwetsbaarheid door de producent.



*'Met een CVD-beleid wordt geprobeerd een balans te vinden tussen het belang om kwetsbaarheden zo snel mogelijk bekend te maken, zodat men maatregelen kan treffen, en het belang van ontwikkelaars en leveranciers om voldoende tijd te hebben de kwetsbaarheid te verhelpen. Het NCSC hanteert voor dit proces een standaardtermijn van 60 dagen tussen melding en publieke bekendmaking. Er kunnen echter omstandigheden zijn waardoor besloten wordt deze termijn te verlengen of in te korten.*

Gebruikers hebben ook rechten waarvan niet bij contract kan worden afgeweken. In het kader van de verbetering van informatiebeveiligingsaspecten van software is het doorgaans onderbelichte Europese recht op fouterstel door de licentienemer vermeld.

Iedere rechtmatige gebruiker beschikt onder andere over het onvervreemdbare, wettelijk verankerde recht een computerprogramma te verveelvoudigen in het kader van het laden, het in beeld brengen of het verbeteren van fouten (art. 45j AW). Dit recht is essentieel voor het waarborgen van de functionaliteit en veiligheid van software.



Hierbij past een kanttekening. Licentienemers beschikken doorgaans niet over de broncode van het computerprogramma, tenzij het open source software betreft of indien er afspraken zijn gemaakt over een broncodedeopot (software-escrow).

Zonder de software in broncodetaal wordt fouterstel erg moeilijk. Wie desalniettemin over de broncode wil beschikken, moet de machinetaal (objectcode, die bestaat uit nullen en enen) decompileren. De voor de computer leesbare vorm wordt hiermee omgezet naar een voor de mens leesbare en te wijzigen vorm. Dit proces heet 'reverse engineering'.

Deze handeling is volgens de wet voor een rechtmatige gebruiker (licentienemer) uitsluitend toegestaan voor het maken van interoperabele programmatuur (art. 45m AW). Anders gezegd, het wettelijke recht op 'decompilatie' van de objectcode geldt dus niet voor testdoeleinden of het herstellen van een veiligheidsfout, tenzij dit expliciet wordt verleend in de licentieovereenkomst.

Recentelijk heeft de Europese rechter echter een andere opvatting geuit over dit verbod, specifiek met betrekking tot het herstellen van veiligheidsfouten. Het gaat om een mede in het licht van penetratietesten belangrijk arrest. De onderzochte software kan naar aanleiding van



bevindingen worden aangepast om beveiligings- en functionele problemen op te lossen.

Iedere licentienemer van een computerprogramma heeft volgens de Europese rechter op grond van de wet ook het recht de objectcode te 'decompileren teneinde fouten te verbeteren die de werking ervan beïnvloeden, ook wanneer de verbetering erin bestaat een functie te deactiveren die de goede werking verstoort van de toepassing waarvan het programma deel uitmaakt'.

De enige beperking die de rechter aan deze regel stelt, is dat de licentienemer een dergelijke decompilatie slechts mag 'verrichten voor zover dit noodzakelijk is voor die verbetering en, in voorkomend geval, met inachtneming van de voorwaarden die bij overeenkomst met de auteursrechthebbende van dit programma zijn vastgelegd.'

## Geautomatiseerd werk (strafrecht)

Onder bepaalde omstandigheden kan het uitvoeren van een pentest of een ander offensief beveiligingsonderzoek, zowel met als zonder toestemming het domein van het strafrecht betreden. In het bijzonder gaat het om de strafbaarstelling van handelingen onder de noemer computercriminaliteit. Bij computerdelicten speelt het bestanddeel 'geautomatiseerd werk' vaak een rol. De



rechtsontwikkeling van de definitie van een geautomatiseerd werk volgens art. 80sexies Wetboek van Strafrecht is als volgt:

*'Onder geautomatiseerd werk wordt verstaan een inrichting die bestemd is om langs elektronische weg gegevens op te slaan en te verwerken'*

1 maart 1993, Wet computercriminaliteit

*'Onder geautomatiseerd werk wordt verstaan een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen'*

1 september 2006, Wet computercriminaliteit II

*'Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken'*

1 maart 2019, Wet computercriminaliteit III



Daaraan is in vergelijking met de vorige versie uit 2006 het element 'netwerk' aan toegevoegd, maar het uitgangspunt dat het fysieke apparatuur betreft, blijft ongewijzigd.

Belangrijk in dit kader is het arrest van de Hoge Raad van 19 maart 2024 (website huisartsenpost), waarin het hoogste rechtscollege in navolging van het Gerechtshof Den Haag nadrukkelijk de website scheidt van de fysieke apparatuur die nodig is voor het functioneren van een website.

De Hoge Raad stelt dat een website feitelijk bestaat uit een samenstel van gegevens, geen fysieke vorm heeft en derhalve het karakter van een inrichting ontbreekt. De zienswijze heeft onder andere gevolgen voor het delict computervredebreuk (art. 138ab Sr), waarvan een 'geautomatiseerd werk' (of onderdeel daarvan) nadrukkelijk deel uitmaakt.

*'Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in*



*ieder geval sprake indien de toegang tot  
het werk wordt verworven:*

- a. door het doorbreken van een  
beveiliging,*
- b. door een technische ingreep,*
- c. met behulp van valse signalen of een  
valse sleutel, of*
- d. door het aannemen van een valse  
hoedanigheid.'*

Volgens de wetsgeschiedenis moeten onder een 'geautomatiseerd werk' uitsluitend fysieke apparaten worden begrepen, terwijl het bij delict computervredebreuk telkens gaat om de bescherming van een (beveiligd) apparaat en niet de gegevens zelfs die daarin verwerkt worden.

Volgens het Haagse hof (na verwijzing naar jurisprudentie van de Hoge Raad): 'Uit het voorgaande kan worden afgeleid dat onder een geautomatiseerd werk steeds een (onderdeel van) een fysiek apparaat is begrepen. Dus een computer, server, router, ereader, chip of wat dies meer zij, maar in elk geval zogenaamde hardware. Het gaat in alle gevallen niet om software, zoals



computerprogramma's, of voor onderhavige casus relevant websites (...)'.

In de woorden van de Hoge Raad: 'Nu een website feitelijk slechts bestaat uit een samenstel van gegevens, geen fysieke vorm heeft en derhalve het karakter van inrichting ontbeert, bestaat op grond van het voorgaande voldoende aanleiding om een website niet aan te merken als geautomatiseerd werk.' In deze casus volgde vrijsprak.

Het arrest impliceert dat websites op een andere manier ontworpen moeten worden om in aanmerking te komen voor strafrechtelijke bescherming. Dit kan bijvoorbeeld worden bereikt door de integratie van geautomatiseerde componenten, zoals de toevoeging van servers en routers die specifiek voor de website zijn en deze ondersteunen.

Bovendien kan de architectuur worden aangepast door een afhankelijkheid van fysieke apparaten voor gegevensverwerking te creëren. Verder kan functionaliteit worden toegevoegd die opzettelijk gebruikmaakt van geautomatiseerde systemen, zoals real-time data-analyse en automatische updates.



## Computervredebreuk

Een offensieve beveiligingstest die wordt uitgevoerd zonder toestemming van de organisatie die het voorwerp van onderzoek is, kan leiden tot een digitale inbraak (hack) of poging daartoe, gepleegd door de pentester. De eerste vraag die opkomt, betreft de rechtmatigheid van het bezit van technische hulpmiddelen (tools) die kunnen worden gebruikt om ongeautoriseerde toegang tot beveiligde netwerk- en informatiesystemen te verkrijgen.

Het Wetboek van Strafrecht stelt strafbaar het vervaardigen, verkopen, verwerven, invoeren, verspreiden of anderszins ter beschikking stellen of vorhanden hebben van een 'technisch hulpmiddel dat hoofdzakelijk geschikt is gemaakt of ontworpen is tot het plegen van computervredebreuk' (art. 139d lid 2 Sr). Een tool die de pentester gebruikt bij zijn onderzoek kan in beginsel onder een dergelijk 'technisch hulpmiddel' vallen, maar dan moet er aan twee criteria zijn voldaan. De tool moet:

- 'hoofdzakelijk' zijn gemaakt of ontworpen om te hacken: en
- gemaakt zijn, in bezit zijn en meer, met het oogmerk om te hacken.

De criteria bieden zowel de organisatie die intern penetratietests uitvoert als een professionele



dienstverlener die in opdracht test, in de regel voldoende ruimte om tools, zoals scanning software, bij offensieve beveiligingstesten rechtmatig in te zetten, op voorwaarde dat het onderzoek plaatsvindt met expliciete toestemming en zonder wederrechtelijk oogmerk.

Zoals vermeld beschouwt de Hoge Raad inmiddels een (bepaalde) website niet als een 'geautomatiseerd werk' in de context van het strafrecht. Dit betekent dat het scannen van een website zonder toestemming van de onderzochte organisatie in beginsel ook niet juridisch kan worden geclassificeerd als (een poging tot) computervredebreuk.

Dit kan echter anders liggen bij het hacken van een computer, server, router, e-reader, chip of andere apparatuur, maar ook bij bijvoorbeeld een website zoals Outlook Web Access (OWA). De rechtkant Rotterdam beschouwt OWA als meer dan alleen een website/gebruikersinterface en stelt dat er meerdere technische componenten nodig zijn om gebruik te kunnen maken van de webversie van Outlook, zoals netwerkapparatuur, een besturingssysteem, de applicatielaag en de databaseservers.

Daarnaast is het van belang te onderstrepen dat het arrest van de Hoge Raad niet per definitie inhoudt dat alle vormen van ongeoorloofd scannen of andere interacties



met websites juridisch toelaatbaar zijn volgens het strafrecht, privacyrecht, auteursrecht of contractenrecht. Zo kan ongeoorloofd scannen van een website resulteren in onrechtmatige verwerking van persoonsgegevens of een inbreuk op het auteursrecht op software.

Voor de volledigheid, sinds de inwerkingtreding van de Wet Computercriminaliteit III op 1 maart 2019 heeft de politie de bevoegdheid om heimelijk een geautomatiseerd werk van een verdachte binnen te dringen (art. 126nba Sv), zoals een laptop of een smartphone. Ook bij deze wettelijke hackbevoegdheid gaat het om een offensief middel, dat bovendien aan strikte voorwaarden is verbonden en alleen mag worden ingezet bij verdenking van een ernstig strafbaar feit.

## Coordinated Vulnerability Disclosure

Een ethisch hacker die zonder expliciete toestemming en wederrechtelijk oogmerk onderzoek verricht naar kwetsbaarheden in ICT-systemen van derden, kan juridisch in de problemen komen. Vanuit het oogpunt van algemeen belang vraagt deze situatie om bescherming van personen die te goeder trouw handelen. Daarom hebben enkele landen regelingen ingesteld voor het melden van digitaal veiligheidsproblemen die op deze



wijze zijn ontdekt. In Nederland is de leidraad Coordinated Vulnerability Disclosure (2018) van het Nationaal Cyber Security Centrum (NCSC) van kracht.

Het Openbaar Ministerie (OM) vindt het naar eigen zeggen belangrijk dat hackers kwetsbaarheden kunnen blijven zoeken en melden zodat ICT-systeem veiliger kunnen worden gemaakt. Daarom stimuleert het OM organisaties beleid over vast te stellen voor het melden van kwetsbaarheden in hun ICT-systeem.

Nota bene, een dergelijke CVD-regeling bindt zowel de organisaties als de melder. Onderzoekers krijgen van het OM het advies om hun stappen in een logbestand bij te houden om te kunnen aantonen dat ze zich aan de regels houden.

Dit beleid probeert een balans te vinden tussen het belang van het snel bekendmaken van kwetsbaarheden, zodat passende maatregelen getroffen kunnen worden, en het belang van ontwikkelaars en leveranciers om voldoende tijd te hebben om de kwetsbaarheid te verhelpen.

Nederland hanteert een dual beleid. Wie een technische kwetsbaarheid vindt in een systeem van de Rijksoverheid, kan dit melden bij het NCSC. Als het gaat om een kwetsbaarheid in digitale technologie van een andere organisatie, dient de ontdekker eerst de eigenaar van het



systeem of de productleverancier te benaderen. Pas als deze organisatie niet of niet adequaat reageert, kan de ontdekker de kwetsbaarheid bij het NCSC melden, dat vervolgens als intermediair fungeert en de kwetsbaarheid bij de betreffende organisatie meldt.

Daarbij passen kanttekeningen. Het CVD-beleid van OM en NCSC staat of valt met een toepasselijke CVD-regeling per organisatie. Voor rijksoverheidsorganisaties is deze regeling uniform beschikbaar. Dit geldt bijvoorbeeld waarschijnlijk niet voor iedere zorginstelling.

Organisaties die nog geen CVD-regeling hebben opgesteld en gepubliceerd, doen er goed aan om deze als onderdeel van hun informatiebeveiligingsbeleid alsnog op te nemen. Bij gebrek aan een dergelijke regeling vallen de betrokkenen (pentester, onderzochte organisatie en OM) terug op de algemene beleids- en rechtsregels, omdat er niet voldaan is aan de vereisten van ethisch hacken.

Een andere kanttekening betreft een aanverwante geheimhoudingskwestie, namelijk een verplichting die vaak in arbeidsovereenkomsten is opgenomen. Indien werknemers op verzoek van het management hun eigen organisatie onderzoeken en de bevindingen die tot actie nopen niet leiden tot verbeteringen van de informatiebeveiliging, kan een werknemer door openbaarmaking van de testresultaten uiteindelijk als



klokkenluider worden beschouwd. Het Nederlandse recht kent sinds 1 juli 2016 Wet Huis voor klokkenluiders, welke regeling momenteel wordt herzien op grond van het Europese recht.

Belangrijk is ook dat het CVD-beleid van een organisatie een ethisch hacker in beginsel wel vrijwaart van strafrechtelijke aansprakelijkheid, maar niet van civielrechtelijke of bestuursrechtelijke aansprakelijkheid. Voorbeelden van privaatrechtelijke aansprakelijkheid zijn schadeclaims van de gehackte organisatie, terwijl bestuursrechtelijke aansprakelijkheid een geldboete van een toezichthouder kan behelen vanwege een inbreuk op het privacyrecht of AI-recht.

Tot op heden is het CVD-beleid in Nederland een vorm van zelfregulering, aangezien wetgeving dit niet voorschrijft. Dat laat onverlet dat de BIO het hebben van een Coordinated Vulnerability Disclosure-procedure wel verplicht voor iedere overheidsinstantie (16.1.3.1 BIO).

Deze situatie verandert door de NIS2-richtlijn. Volgens de richtlijn duidt de gecoördineerde bekendmaking van kwetsbaarheden 'een gestructureerd proces aan waarbij kwetsbaarheden aan de fabrikant of aanbieder van de potentieel kwetsbare ICT-producten of ICT-diensten worden gemeld op een manier die deze in staat stelt de kwetsbaarheid te diagnosticeren en te verhelpen voordat



gedetailleerde informatie over de kwetsbaarheid aan derden of aan het publiek wordt bekendgemaakt' (considerans 58 NIS2).

Allereerst moeten lidstaten voor 18 oktober 2024, als onderdeel van hun nationale cybersecuritystrategie, beleid formuleren, aannemen en uitvoeren voor het beheer van kwetsbaarheden, waarbij de bevordering en facilitering van gecoördineerde kwetsbaarheidsmelding onder artikel 12, lid 1 wordt omvat.

Een belangrijk element van dit beleid is de rol die op nationaal niveau wordt toegekend aan ten minste één Computer Security Incident Response Team (CSIRT) om op te treden als coördinator voor de doeleinden van CVD en het ontvangen van meldingen van kwetsbaarheden (art. 12, lid 1 en 11, lid 3 onder g NIS2).

Behalve de nieuwe wettelijke verplichtingen op landenniveau, moeten essentiële en belangrijke entiteiten, waaronder rijksoverheidsorganisaties, technische, operationele en organisatorische risicobeheersingsmaatregelen op het gebied van cybersecurity toepassen (art. 21 NIS2). Deze juridische zorgplicht omvat explicet kwetsbaarheidsbeheer ('vulnerability handling') en incidentenmeldingsprocedures ('incident reporting').



## Forensisch bewijs

Forensisch onderzoek helpt bij het opsporen van daders of de oorzaken van (mogelijke) strafbare feiten of delicten op basis van wetenschappelijk bewijs, doorgaans met behulp van technologie. Dit type onderzoek naar waarheidsvinding kan zowel worden uitgevoerd door de politie en speciale onderzoeksinstituten van de overheid, zoals het Nederlands Forensisch Instituut of NFI, als particuliere onderzoekers. De resultaten van het onderzoek kunnen dienen als bewijs in strafprocedures.

Een van de vele gebieden binnen de forensische wetenschap betreft digitaal sporenonderzoek, dat wil zeggen onderzoek naar digitale sporen en gegevens die in beginsel op andere wijze niet of moeilijk zijn te achterhalen. Ook een digitaal bewijsmiddel heeft als doel zekerheid te verschaffen over gestelde feiten.

Onderzoekers stellen de sporen veilig en analyseren deze. Dit domein, ook wel forensische informatica ('digital forensics') genoemd, neemt al jaren in omvang en belang toe.

Hoewel forensisch of gerechtelijk onderzoek doorgaans primair verbonden is aan de strafrechtspleging, kan forensische informatica breder worden ingezet, namelijk



voor het vinden van juridisch bewijs in en op basis van computers, software, netwerken, websites en bijvoorbeeld opslagmedia ten behoeve van het gehele juridische en beleidsmatige spectrum.

Dit omvat naast het strafrecht ook privaatrechtelijke, bestuursrechtelijke of staatsrechtelijke kwesties. Met andere woorden, forensische informatica richt zich tegenwoordig niet langer uitsluitend op digitaal bewijs ten behoeve van de opsporing van strafbare feiten en het vervolgen van verdachten.

De achterliggende ratio is belangrijk. Het ontsluiten, veiligstellen en analyseren van digitale sporen voor wetenschappelijke bewijsvoering kan immers op vrijwel alles betrekking hebben. Dit kan variëren van het vaststellen van schendingen van intellectuele eigendomsrechten tot wanprestatie van een wederpartij, of het controleren van beveiligingsmaatregelen, ook digitaal. Dit geldt in elke rechtsverhouding: tussen burgers en bedrijven onderling, tussen burger en bedrijf, en tussen overheidsorganisaties onderling.

Tijdens een penetratietest worden digitale technologie en/of processen onderzocht op kwetsbaarheden door middel van offensieve scanning. De bevindingen bestaan in wezen uit elektronische gegevens en kunnen als



digitale sporen worden gebruikt in een forensisch onderzoek.

Enerzijds gaat het om de productie van digitaal bewijs: de wijze waarop bewijs ontstaat, wordt verzameld en hoe de kracht van dat bewijs tot stand komt. Anderzijds moet bewijs worden veiliggesteld: de borging dat het geproduceerde bewijs ook daadwerkelijk als zodanig kan worden ingezet, bijvoorbeeld in een juridische procedure.

Mede afhankelijk van de gebruikte hulpmiddelen, gevolgde methodieken, gestandaardiseerde rapportages en de beoordeling daarvan door een IT-auditor, kunnen de bevindingen van een penetratietest leiden tot sluitende, erkende wetenschappelijke bewijsvoering.

## Rechtsontwikkelingen

Uit de praktijk blijkt dat de ene kwetsbaarheid niet dezelfde is als de andere. Zo wordt er onder andere onderscheid gemaakt tussen gewone en kritieke varianten, gerelateerd aan de potentiële impact en ernst van de kwetsbaarheid. Daarnaast worden kwetsbaarheden geklassificeerd als 'bekende' en 'zero-day' kwetsbaarheden.

Een zero-daykwetsbaarheid wordt doorgaans omschreven als een beveiligingsfout die onbekend is bij de software- of



hardware-ontwikkelaars op het moment dat deze wordt ontdekt of misbruikt. Omdat de kwetsbaarheid niet bekend is bij de verantwoordelijke partijen, hebben ze geen tijd gehad ('zero time') om een patch of oplossing te ontwikkelen, wat de naam verklaart.

Een kanttekening hierbij is dat kwetsbaarheden doorgaans worden geassocieerd met de vertrouwelijkheid van gegevensverwerking, terwijl informatiebeveiliging ook betrekking heeft op de kernbegrippen beschikbaarheid en integriteit.

Veel standaardisatieorganisaties koppelen een kwetsbaarheid aan de omstandigheid dat er misbruik van kan worden gemaakt. Met andere woorden, als een zwakheid of gebrek niet kan worden aangevallen (bijvoorbeeld met speciaal hiervoor geschreven computercode of een 'exploit') of anderszins kan worden misbruikt, wordt dit kennelijk niet als een kwetsbaarheid beschouwd.

Het is echter belangrijk te erkennen dat niet alle kwetsbaarheden directe exploitatie door een aanvaller vereisen om een bedreiging te vormen. Autonome systeemfouten, softwarebugs en operationele risico's (het resultaat van zowel opzettelijk handelen als nalaten) kunnen net zo schadelijk zijn en moeten daarom serieus



worden genomen in het kader van informatiebeveiliging, net als opzettelijke handelingen van kwaadwillenden.

Het NIST (in SP 800-30) en het Europese agentschap ENISA hanteren een bredere definitie van een kwetsbaarheid en beschouwen een kwetsbaarheid als een technische zwakheid die in de praktijk tot een veiligheidsprobleem kan leiden, zowel per ongeluk als door opzettelijk misbruik. Deze benadering verdient steun, omdat elke vorm van een gebrek met een digitaal veiligheidsrisico in beginsel actie vereist, ongeacht de intentie. Op deze lijn zit inmiddels ook de Europese wetgever. Zoals gezegd, de NIS2 definieert 'kwetsbaarheid' als volgt:

*'een zwakheid, vatbaarheid of gebrek van ICT-producten of ICT-diensten die door een cyberdreiging kan worden uitgebuit'*  
(art. 6 onder 15 NIS2).

Onder een 'cyberbedreiging' moet vervolgens de CSA (Cybersecurity Act) worden verstaan:

*'elke potentiële omstandigheid, gebeurtenis of actie die netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen kan schaden, verstören of op andere wijze*



*'negatief kan beïnvloeden' (art. 2, lid 8 CSA).*

Beiden zijn ruime definities. Belangrijk is verder het ontwerp EU Cybersecurity Resilience Act (CRA). In deze verordening gaat het om veiligheidsmaatregelen voor een '*product with digital elements*', dat wil zeggen '*any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately*' (art. 3, lid 1 ontwerp-CRA).

De producten met digitale elementen moeten volgens veiligheidseisen worden ontworpen, ontwikkeld en geproduceerd zodat ze een geschikt informatiebeveiligingsniveau waarborgen op basis van de risico's en moeten worden geleverd zonder bekende kwetsbaarheden waarvan misbruik kan worden gemaakt. Daarbij is uitvoerig testen onvermijdelijk. Het ontwerp onderscheidt in drie productcategorieën met digitale elementen, gerelateerd aan de kritieke status van de toepassing: gewoon, kritiek en hoog-kritiek.

Het is opmerkelijk dat de Nederlandse Leidraad Coordinated Vulnerability Disclosure (CVD) geen definitie van een kwetsbaarheid hanteert en niet verwijst naar de Europeesrechtelijke definitie. Het NCSC hanteert voor het verhelpen van de kwetsbaarheid een standaardtermijn



van 60 dagen tussen de CVD-melding en de publieke bekendmaking.

Een andere juridische ontwikkeling komt uit het consumentenrecht. Om het goede en veilige gebruik te garanderen, zijn aanbieders van een digitaal product of dienst op grond van de Richtlijn levering digitale inhoud (art. 7:50a t/m 7:50f BW) en de Richtlijn verkoop goederen (art. 7:18 t/m 7:23 BW) verplicht om software-updates te leveren, waaronder nadrukkelijk begrepen veiligheidsupdates.

In 2017 wilde minister van J&V digitaal onveilige bedrijven die verzuimden een ‘security patch’ voortvarend te installeren aanpakken, maar dit plan leidde niet tot nieuwe regulering. In 2029 later overwoog deze minister opnieuw in de markt in te grijpen, nu omdat vitale aanbieders beveiligingsadviezen kennelijk onvoldoende opvolgen:

*Waar nodig zal gebruik worden gemaakt van de interventiemogelijkheden onder de Wbni als dat nodig is in het kader van nationale veiligheid. Het NCSC zal bijvoorbeeld vaker toezichthouders informeren over situaties waarin een vitale aanbieder beveiligingsadviezen onvoldoende opvolgt, waardoor risico's*



*voor de nationale veiligheid blijven bestaan. De VPN-Pulse kwetsbaarheid laat zien dat waarschuwingen en adviezen van het NCSC niet altijd direct worden opgevolgd.*

De aansprakelijkheidswestie in relatie tot een kwetsbaarheid begint met de vraag wie waarvoor verantwoordelijk is. Hierover bestaat in zoverre overeenstemming dat volgens de minister van Justitie en Veiligheid organisaties in de eerste plaats zelf verantwoordelijk voor hun eigen cybersecurity zijn, terwijl voor softwarefabrikanten geldt dat zij primair verantwoordelijk zijn voor de digitale veiligheid van de door hen aangeboden producten en diensten.<sup>4</sup> Dat is in lijn met opvattingen van anderen, zoals de Onderzoeksraad voor Veiligheid (OVV) waarop de Kamervragen betrekking hebben.

Fouten in software, inclusief veiligheidsgebreken, kunnen tot aansprakelijkheid voor schade leiden die hieruit ontstaat, zowel op grond van het leerstuk van de onrechtmatige daad als toerekenbare tekortkoming (wanprestatie) bij de uitvoering van een overeenkomst. In beide gevallen dient de kwetsbaarheid aan iemand te worden toegerekend. Rechtspraak over kwetsbaarheden naar Nederlands recht ontbreekt vrijwel.



Om softwarereproducenten te stimuleren meer aan informatiebeveiliging te doen, wilde het kabinet Rutte III een bijzondere juridische aansprakelijkheid voor onveilige software in het Nederlandse recht introduceren. Dit beleidsvoornemen, vastgelegd in het regeerakkoord van 10 oktober 2017, werd niet uitgevoerd.

In plaats daarvan benadrukte de minister het belang van het maken van kwaliteits- en aansprakelijkheidsafspraken op internationaal en Europees niveau over digitale veiligheid, vanwege het grensoverschrijdende karakter van de markt voor ICT-producten en -diensten. Dit is in overeenstemming met de aanbevelingen van de Onderzoeksraad voor Veiligheid (OVV).

Al genoemd is de Cyber Resilience Act (CRA), de aankomende verordening gericht op het instellen van gemeenschappelijke informatiebeveiligingsnormen voor producten met digitale elementen (productveiligheid). Verder werkt de EU aan de herziening van de Richtlijn productaansprakelijkheid, die bedoeld is om de regels hiervoor aan te passen aan de digitale en circulaire economie, evenals aan moderne technologische ontwikkelingen zoals kunstmatige intelligentie (AI).

Tot slot en niet onbelangrijk, wordt sinds 1999 wereldwijd de Common Vulnerabilities and Exposures (CVE)-lijst gebruikt. Deze lijst, opgericht door het MITRE Corp. in



samenwerking met de internationale informatiebeveiligingsgemeenschap, kent aan kwetsbaarheden een uniek identificatienummer toe.

Dit nummer maakt het eenvoudiger om kwetsbaarheden te volgen, informatie uit te wisselen en de computercode te beoordelen. Het CVE-systeem wordt door beveiligingsexperts, overheden en bedrijven wereldwijd erkend en bevordert de internationale samenwerking en standaardisering op het gebied van informatiebeveiliging.

Daarnaast draagt het CVE-systeem bij aan een gestandaardiseerde en gestructureerde aanpak voor het identificeren en beheren van kwetsbaarheden, wat resulteert in een verbeterde informatiebeveiliging. De CVE-lijst stelt softwareproducenten in staat om voortdurend bekende kwetsbaarheden te identificeren en te verhelpen. De CVE-lijst wordt vaak gebruikt in combinatie met andere beveiligingsdatabases, zoals de National Vulnerability Database (NVD), die extra details en context over kwetsbaarheden biedt.

## Conclusies

Digitale kwaliteitstekortkomingen, zoals kwetsbaarheden (wettelijk gedefinieerd als ‘zwakke plekken, vatbaarheden of gebreken in ICT-producten of -diensten die kunnen



worden misbruikt door cyberdreigingen'), maken individuele gebruikers, organisaties en de samenleving kwetsbaar. Enerzijds vergemakkelijkt een tekortkoming in relatie tot ICT de uitvoering van computercriminaliteit, anderzijds vergroten kwetsbaarheden autonoom en zonder opzet het risico op verstoring en uitval van bedrijfsprocessen.

Elke organisatie, ongeacht sector en omvang, heeft vanwege het maatschappelijk belang van digitale weerbaarheid een wettelijke zorgplicht voor informatiebeveiliging. Deze richt zich op het treffen van organisatorische, technische en operationele risicobeheersmaatregelen om de beschikbaarheid, continuïteit en vertrouwelijkheid van de gegevensverwerking te waarborgen, waarvoor de organisatie verantwoordelijk is.

Voor rijksoverheidsorganisaties vallen bovendien de verplichting om beleidsregels uit te voeren, zoals onder meer vastgelegd in het Besluit Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR 2007), het Besluit Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI 2013) en de Baseline Informatiebeveiliging Overheid (BIO).

Deze juridische zorgplicht omvat ook controleren en verantwoording afleggen over de implementatie, naleving



en voortdurende adequaatheid van de getroffen risicobeheersmaatregelen. De NIS2-richtlijn benoemt dit expliciet.

Organisaties die onder haar reikwijdte en die van de Nederlandse implementatiewet Cyberbeveiligingswet (Cbw) vallen, moeten beleid en procedures hebben '*om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen*' (art. 21, lid 2, onder f NIS2). Daarnaast moeten beveiligingsincidenten worden gecontroleerd en aangepakt (art. 21, lid 2 onder b NIS2). Hetzelfde geldt onder andere op grond van de privacywetgeving.

Digitale beveiligingsonderzoeken, zoals penetratietesten, zijn cruciaal voor een proactieve benadering van informatiebeveiliging. Dit type testen helpt organisaties om kwetsbaarheden in hun systemen te identificeren en aan te pakken voordat kwaadwillenden deze kunnen uitbuiten of voordat de wakheden anderszins tot problemen leiden.

Reactieve penetratietesten moeten vervolgens plaatsvinden na een incident om de oorzaak te identificeren, de omvang van de schade te beoordelen en passende maatregelen te implementeren om herhaling te voorkomen. Daarbij speelt het recht telkens een belangrijke rol.



Het juridisch zorgvuldig uitvoeren van penetratietesten faciliteert zowel de naleving van zorgplichten en andere wettelijke, beleidsmatige en contractuele voorschriften (juridische compliance) als een effectieve uitvoering binnen de juridische kaders (waardecreatie). Beide aspecten dragen bij aan het versterken van de digitale weerbaarheid en het beperken van het risico op juridische en politieke aansprakelijkheid.

## Voorbeeldvragen opdrachtgevers

### Algemene vereisten

- Kunt u bevestigen dat het rapport in digitale vorm wordt geleverd?
- Zal de naam van de rapporteur, certificeringen (bijv. OSCP, OSCE) en contactgegevens worden opgenomen in het rapport?
- Hoe zorgt u ervoor dat het rapport accuraat en waarheidsgetrouw is?
- Welk versiebeheersysteem of methode wordt gebruikt om wijzigingen in het rapport bij te houden tijdens de voorbereiding?
- Wordt er een digitale handtekening van de rapporteur bij het rapport geleverd?



## **Pentest Execution Standard (PTES)**

- Kunt u bevestigen dat uw onderzoek is uitgevoerd volgens de zeven fasen van PTES: Pre-engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post Exploitation en Reporting?
- Zal het rapport dit formaat in detail weergeven voor elke fase?
- Hoe zorgt u ervoor dat alle noodzakelijke informatie wordt verzameld tijdens elke fase ter ondersteuning van bevindingen en aanbevelingen?
- Kunt u bevestigen dat uw onderzoek is uitgevoerd volgens de beste praktijken in de industrie (bijv. NIST Cybersecurity Framework)?
- Zijn er specifieke PTES-fasen of activiteiten waarbij extra begeleiding of middelen zijn gezocht van externe experts?

## **Vertrouwelijkheid**

- Hoe zorgt u ervoor dat geheimhoudingsovereenkomsten die voorafgaand aan het onderzoek zijn gemaakt correct worden gedocumenteerd in het rapport?



- Zullen alle betrokken partijen (bijv. cliënten, stakeholders) op de hoogte worden gebracht van hun verplichtingen onder deze overeenkomsten?
- Zijn er specifieke procedures voor het omgaan met vertrouwelijke informatie of gevoelige gegevens die tijdens uw onderzoek zijn verzameld?
- Kunt u bevestigen dat een duidelijke en beknopte samenvatting van geheimhoudingsovereenkomst zal worden opgenomen in de managementsamenvatting van het rapport?
- Hoe zorgt u voor naleving van relevante wetten, voorschriften en industrienormen (bijv. AVG) bij het verzamelen en opslaan van persoonlijke gegevens?

### **Intakegesprek en Plan van Aanpak**

- Zal de offerte een verslag van het intakegesprekgesprek bevatten, inclusief namen, datum, deelnemers en belangrijke punten of actiepunten die tijdens de discussie zijn overeengekomen?
- Zal het rapport een verslag van het intakegesprekgesprek bevatten, inclusief namen, datum, deelnemers en belangrijke punten of



actiepunten die tijdens de discussie zijn overeengekomen?

- Kunt u bevestigen dat eventuele wijzigingen in scope of vereisten die na het oorspronkelijke intakegesprek zijn gemaakt, correct schriftelijk zijn gedocumenteerd (bijv. via e-mail of formele memo)?
- Zal een duidelijke en beknopte samenvatting van de verwachtingen, behoeften en prioriteiten worden opgenomen in de managementsamenvatting van het rapport?

### **Scopedefinitie en onderzoeksmethodologie**

- Kunt u bevestigen dat de scope van het onderzoek duidelijk schriftelijk is gedefinieerd voordat u met uw onderzoek begon?
- Indien infra/webapplicatie: Hoe zorgt u ervoor dat alle objecten die binnen de scope zijn geïdentificeerd, worden getest met een combinatie van handmatige testen (bijv. OWASP Web Application Security Testing Guide, WSTG) en geautomatiseerde tools (bijv. Nessus)?
- Indien mobiel: Zal het rapport een beschrijving bevatten van hoe mobiele applicatietesten zijn uitgevoerd voor elk scope-object?



- Hoe zorgt u voor naleving van relevante standaarden (bijv. PTES, NIST Cybersecurity Framework) bij het uitvoeren van de pentest?

### **Standaard: OWASP Firmware Security Test**

- Zal het rapport een beschrijving bevatten van hoe OWASP Firmware Security Testing is uitgevoerd voor elk scope-object?
- Kunt u bevestigen dat eventuele firmware-beveiligingstesten die tijdens uw onderzoek zijn uitgevoerd, voldeden aan relevante standaarden (bijv. PTES, NIST Cybersecurity Framework)?
- Hoe zorgt u voor naleving van de beste praktijken in de industrie bij het uitvoeren van firmware-beveiligingsbeoordelingen?
- Zal het rapport een samenvatting bevatten van bevindingen met betrekking tot firmware-veiligheidskwetsbaarheden of -zwakheden die tijdens uw onderzoek zijn geïdentificeerd?
- Kunt u bevestigen dat eventuele aanbevelingen met betrekking tot firmware-beveiligingstesten correct zijn gedocumenteerd en geprioriteerd op basis van risico?

### **Standaard: OWASP Web Application Security Testing Guide (WSTG)**



- Hoe zorgt u voor naleving van WSTG-richtlijnen bij het uitvoeren van webapplicatie-penetratietests voor elk scope-object?
- Zal het rapport een beschrijving bevatten van hoe handmatige tests zijn uitgevoerd met WSTG-technieken voor elk scope-object?
- Kunt u bevestigen dat eventuele geautomatiseerde tools die tijdens uw onderzoek zijn gebruikt (bijv. Nessus) correct zijn geconfigureerd om WSTG-best practices te volgen?
- Hoe zorgt u voor naleving van industrienormen bij het uitvoeren van webapplicatie-beveiligingsbeoordelingen voor elk scope-object?
- Bevat het rapport een samenvatting van bevindingen met betrekking tot webapplicatie-kwetsbaarheden of -zwakheden die tijdens uw onderzoek zijn geïdentificeerd?

### **Standaard: OWASP Mobile Application Security Testing Guide (MASTG)**

- Kunt u bevestigen dat eventuele mobiele applicatietesten die tijdens uw onderzoek zijn uitgevoerd, voldeden aan relevante MASTG-richtlijnen en best practices?



- Hoe zorgt u voor naleving van industrienormen bij het uitvoeren van mobiele applicatie-beveiligingsbeoordelingen voor elk scope-object?
- Zal het rapport een beschrijving bevatten van hoe handmatige tests zijn uitgevoerd met MASTG-technieken voor elk scope-object?
- Kunt u bevestigen dat eventuele geautomatiseerde tools die tijdens uw onderzoek zijn gebruikt (bijv. MobSF) correct zijn geconfigureerd om MASTG-best practices te volgen?
- Hoe zorgt u voor naleving van relevante standaarden bij het uitvoeren van mobiele applicatie-beveiligingsbeoordelingen?

### **Standaard: Common Vulnerability Scoring System (CVSS)**

- Zal het rapport een beschrijving bevatten van hoe CVSS-scores en vectorstrings worden berekend voor elke geregistreerde bevinding?
- Kunt u bevestigen dat eventuele CVSS-berekeningen die tijdens uw onderzoek zijn uitgevoerd, voldeden aan relevante industriële richtlijnen of best practices?
- Hoe zorgt u voor naleving van CVSS-standaarden bij het documenteren van bevindingen met



betrekking tot beveiligingskwetsbaarheden of -zwakheden die tijdens uw onderzoek zijn geïdentificeerd?

- Zal het rapport een samenvatting bevatten van bevindingen met betrekking tot beveiligingskwetsbaarheden of -zwakheden die tijdens uw onderzoek zijn geïdentificeerd, inclusief hun bijbehorende CVSS-scores en vector-strings?
- Kunt u bevestigen dat eventuele aanbevelingen met betrekking tot het mitigeren of verhelpen van beveiligingskwetsbaarheden correct zijn gedocumenteerd en geprioriteerd op basis van risico?

#### **Standaard: Common Weakness Enumeration (CWE)**

- Zal het rapport een beschrijving bevatten van hoe CWE-items worden gebruikt voor elke geregistreerde bevinding met betrekking tot geïdentificeerde beveiligingszwakheden tijdens uw onderzoek?
- Kunt u bevestigen dat eventuele CWE-items die tijdens uw onderzoek zijn gebruikt, voldeden aan relevante industriële richtlijnen of best practices?



- Hoe zorgt u voor naleving van CWE-standaarden bij het documenteren van bevindingen met betrekking tot beveiligingskwetsbaarheden of -zwakheden die tijdens uw onderzoek zijn geïdentificeerd?
- Zal het rapport een samenvatting bevatten van bevindingen met betrekking tot beveiligingskwetsbaarheden of -zwakheden die tijdens uw onderzoek zijn geïdentificeerd, inclusief hun overeenkomstige CVSS-scores en vectorstrings?
- Kunt u bevestigen dat eventuele aanbevelingen met betrekking tot het mitigeren of verhelpen van beveiligingskwetsbaarheden correct zijn gedocumenteerd en geprioriteerd op basis van risico?

### **Gebruikte tools tijdens het onderzoek**

- Zal het rapport een beschrijving bevatten van alle tools die tijdens uw onderzoek zijn gebruikt (bijv. Nessus, nmap)?
- Hoe zorgt u voor naleving van industrienormen bij het gebruik van geautomatiseerde tools om



kwetsbaarheidsbeoordelingen uit te voeren voor elk scope-object?

- Kunt u bevestigen dat eventuele bevindingen met betrekking tot beveiligingskwetsbaarheden of -zwakheden die tijdens uw onderzoek zijn geïdentificeerd, correct zijn gedocumenteerd en geprioriteerd op basis van risico?
- Zal het rapport een samenvatting bevatten van bevindingen met betrekking tot beveiligingskwetsbaarheden of -zwakheden die tijdens uw onderzoek zijn geïdentificeerd, inclusief hun overeenkomstige CVSS-scores en vectorstrings?
- Hoe zorgt u voor naleving van industrienormen bij het documenteren van bevindingen met betrekking tot beveiligingskwetsbaarheden of -zwakheden die tijdens uw onderzoek zijn geïdentificeerd?

## Bijlagen en woordenlijst

- Bevat het rapport alle bijlagen (bijv. screenshots) die tijdens uw onderzoek zijn gegenereerd?
- Kunt u bevestigen dat eventuele SHA-1-hashes die in het rapport zijn opgenomen, correct zijn berekend voor elke bijlage?



- Hoe zorgt u voor naleving van industrienormen bij het documenteren van bevindingen met betrekking tot beveiligingskwetsbaarheden of - zwakheden die tijdens uw onderzoek zijn geïdentificeerd?
- Zal het rapport een woordenlijst bevatten van termen die door het document heen worden gebruikt (bijv. technische termen)?
- Kunt u bevestigen dat eventuele aanbevelingen met betrekking tot het mitigeren of verhelpen van beveiligingskwetsbaarheden correct zijn gedocumenteerd en geprioriteerd op basis van risico?

### **Scanresultaten, bewijs en checklists**

- Zal het rapport scanresultaten bevatten van scans die tijdens uw onderzoek zijn uitgevoerd?
- Hoe zorgt u voor naleving van industrienormen bij het documenteren van bevindingen met betrekking tot beveiligingskwetsbaarheden of - zwakheden die tijdens uw onderzoek zijn geïdentificeerd?



- Kunt u bevestigen dat eventueel bewijs dat door uw team is gegenereerd of gecreëerd, correct is gedocumenteerd (bijv. SHA-1-hashes)?
- Zal het rapport een samenvatting bevatten van bevindingen met betrekking tot beveiligingskwetsbaarheden of -zwakheden die tijdens uw onderzoek zijn geïdentificeerd, inclusief hun overeenkomstige CVSS-scores en vector-strings?
- Hoe zorgt u voor naleving van industrienormen bij het documenteren van bevindingen met betrekking tot beveiligingskwetsbaarheden of -zwakheden die tijdens uw onderzoek zijn geïdentificeerd?

### **Technische ontoegankelijkheid**

- Kunt u bevestigen dat eventuele scope-objecten die technisch ontoegankelijk bleken te zijn op het moment van onderzoek correct schriftelijk zijn gedocumenteerd?
- Zal het rapport een beschrijving bevatten van hoe technische ontoegankelijkheid is vastgesteld voor elk betroffen scope-object?
- Hoe zorgt u voor naleving van industrienormen bij het documenteren van bevindingen met betrekking tot beveiligingskwetsbaarheden of -



zwakheden die tijdens uw onderzoek zijn geïdentificeerd?

- Kunt u bevestigen dat eventuele aanbevelingen met betrekking tot het mitigeren of verhelpen van beveiligingskwetsbaarheden correct zijn gedocumenteerd en geprioriteerd op basis van risico?
- Zal het rapport een samenvatting bevatten van bevindingen met betrekking tot beveiligingskwetsbaarheden of -zwakheden die tijdens uw onderzoek zijn geïdentificeerd, inclusief hun overeenkomstige CVSS-scores en vectorstrings?

