Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

DEPARTEMENTAAL VERTROUWELIJK

TER INFORMATIE

Nota actief openbaar
Nee

Onze referentie

Datum
1 september 2025

Opgesteld door
[redacted]

Samengewerkt met
[redacted]

Bijlage(n)
0

Aan CISO Rijk
Van TCT Rijk

nota

Beantwoording Motie Pentesten

Aanleiding

Op 17 december 2024 heeft de Tweede Kamer een motie[1] van het lid Six Dijkstra aangenomen. In deze motie wordt de regering verzocht om overheidsbreed toe te werken naar een gestandaardiseerde methodiek voor het opdrachtgeverschap van pentests, zoals de methodiek voor Informatiebeveiligingsonderzoek met Audit Waarde (MIAUW). Tijdens de behandeling van deze motie op 11 december 2024 is door de toenmalige staatssecretaris van digitalisering en Koninkrijksrelaties aangegeven dat hij het doel achter de motie deelt, maar dit eerst wil verkennen. Hij heeft tevens toegezegd om de Tweede Kamer te informeren over de uitkomsten van deze verkenning na het zomerreces van 2025. [2]

Geadviseerd besluit

Via deze nota wordt de CISO Rijk;

- geïnformeerd over de bevindingen van de hierboven genoemde interne verkenning naar pentesten (kopje 1);
- geadviseerd om de Tweede Kamer te informeren over de conclusie en daarmee de motie af te doen, via voorgestelde passage in een aankomende verzamelbrief op digitalisering.

[1] Kamerstukken II, 2024-2025, 26 643, nr. 1254

[2] Zie voor de precieze toezegging het stenogram: https://www.tweedekamer.nl/kamerstukken/plenaire_verslagen/detail/2024-2025/35

1. Bevindingen verkenning

Er zijn verschillende initiatieven en informatieproducten op het gebied van pentesten. Deze producten helpen bij het invulling geven aan het opdrachtgeverschap voor pentesten om zo kwalitatief goede pentesten te organiseren. Overheidsorganisaties voeren zelf pentesten uit of geven hiervoor opdracht aan externe partijen. In de paragrafen hieronder wordt een overzicht gegeven van een aantal initiatieven en informatieproducten. Voordat in deze nota wordt geïnformeerd over de uitkomsten van deze verkenning wordt allereerst toegelicht wat in deze nota wordt verstaan onder het begrip penetratietest, ofwel pentest. Een Pentest is een geautoriseerde poging om een beveiligingssysteem te omzeilen of te doorbreken, om zo inzicht te krijgen in de effectiviteit van dat systeem en om verbeterpunten te definiëren in het kader van de digitale weerbaarheid. [3]

Overzicht initiatieven en informatieproducten pentesten binnen de overheid
Het Nationaal Cyber Security Centrum (NCSC) heeft verschillende publicaties op het gebied van pentesten. In de whitepaper 'Securitytesten' en de infosheet 'Securitytesten' benadrukt het NCSC het belang van een risico gebaseerde benadering. De publicatie 'Pentesten, doe je zo' uit onderstreept het belang van een heldere doelstelling, goede voorbereiding en afstemming met de opdrachtgever als voorwaarden voor een waardevolle test. [4]
In 2025 heeft het NCSC een blogpost 'Penetratietesten' uitgebracht, waarin het NCSC benadrukt dat pentesten slechts één onderdeel vormen van een bredere, integrale beveiligingsaanpak.
De CISO-rijk publiceert de 'keuzekaart securitytesten' [5] als hulpmiddel voor organisaties om de juiste securitytest te kiezen die aansluit op hun specifieke testdoelen en/of het cyber volwassenheidsniveau.
De Auditdienst Rijk (ADR) kent op het gebied van beveiligingsonderzoek verschillende producten. Dit betreft onder andere de 'klassieke' pentest waarbij door de ethical hackers van de ADR onderzoek wordt gedaan naar mogelijke kwetsbaarheden van systemen en applicaties. [6] Het type onderzoek wordt in overleg met de opdrachtgever bepaald. Daarbij wordt gezocht naar de meest passende oplossing gegeven onder andere de informatiebehoefte, het type systeem en de risico's daarvan, de volwassenheid van de beheer- en beveiligingsorganisatie en eventueel eerder uitgevoerde onderzoeken. De ADR is een auditorganisatie, waardoor de ethical hackers van de ADR vallen onder de gedrags- en beroepsregels van onder meer het Instituut voor Internal Auditors (IIA) en de Nederlandse Orde van Register EDP-auditors (NOREA). Deze organisaties stellen hoge eisen aan het uitvoeren van onderzoeken, zoals de beveiligingsonderzoeken. De ADR hanteert voor pentesten een standaard intakeproces met opdrachtgevers. Hierbij wordt gezamenlijk, op basis van de behoefte van de opdrachtgever en de kennis en kunde van de ADR, de scope en aanpak van een test bepaald. Dit mondt uit in een door de opdrachtgever en ADR ondertekende opdrachtbevestiging waarin de afspraken rondom de uitvoering zijn vastgelegd. De ADR-rapportages kennen een standaard opbouw, waarbij een inschatting wordt gemaakt van het risico van elke bevinding en de hoeveelheid

[3] Zie hierover de publicatie van het Nationaal Cyber Security Centrum (NCSC) ´Whitepaper Pen-testen doe je zo´
[4] De publicaties zijn te vinden via: https://www.ncsc.nl/
[5] De publicaties zijn te vinden via Keuzekaart securitytesten Rijksoverheid
[6] Meer informatie is te vinden op: https://www.auditdienstrijk.nl/documenten/2024/april/16/pentesten

inspanning die het de kost om de bevinding op te lossen. Dit helpt opdrachtgevers bij het prioriteren van te nemen verbeteracties.

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) gebruikt de Baseline Security Product Assessment (BSPA) als pentest methodiek voor beveiligingsproducten. BSPA, met bijbehorende ondersteuning van de Unit Weerbaarheid van de AIVD, is beschikbaar voor organisaties uit de overheid en voor Nederlandse vitale sectoren, high-tech bedrijven en kennisinstellingen. Zij kunnen een BSPA laten uitvoeren op voor hen relevante beveiligingsproducten. Met BSPA worden de (beveiligings-) functies van een beveiligingsproduct in een geformaliseerd fixed-time proces getoetst door een deskundig en onafhankelijk (pen-) testlaboratorium, onder toezicht van de AIVD. [7]

Ook zijn er verschillende initiatieven bij de medeoverheden op het gebied van pentesten. Zo is na een uitvraag bij de Provincies aangegeven dat er ook bij de provincies pentesten worden uitgevoerd, soms gezamenlijk of met meerdere ketenpartners. Ook hebben de provincies een gezamenlijk inkoopbeleid op pentesten. De Provincies hebben aangegeven dat zij bij het inrichten van hun inkoopproces kijken naar bestaande kwaliteitseisen.
De Vereniging van Nederlandse Gemeente (VNG) biedt via Gemeentelijke Gemeenschappelijke Infrastructuur (GGI)-Veilig een collectieve inkoopmogelijkheid aan, waarin kwaliteitseisen aan leveranciers van pentesten zijn opgenomen. Het vervolgtraject, de aanbesteding Cyberweerbaarheid, is ook inmiddels gestart. De Informatiebeveiligingsdienst (IBD) verwijst bij advisering naar de NCSC handreikingen. In de praktijk constateert de VNG dat Gemeenten werken met leveranciers die het CCV/KIWA-keurmerk bezitten. De VNG juicht gestandaardiseerde methodieken toe, NIST SP 800-115, OSSTMM of PTES.

Openbare Methodieken & standaarden
Er zijn verschillende openbare methodieken en standaarden die toezien op pentesten. In de motie wordt specifiek als voorbeeld de Methodiek voor Informatiebeveiligingsonderzoek met Audit Waarde, afgekort MIAUW, genoemd. MIAUW is een werkwijze voor het plannen uitvoeren en rapporteren van pentesten. Het biedt handvatten voor verbetering van kwaliteit en structuur in pentestopdrachten. Het primaire doel is om pentests transparanter, reproduceerbaar en auditeerbaar te maken. MIAUW legt nadruk op duidelijke opdrachtformulering, zorgvuldige documentatie en expliciete vermelding van testers en kwaliteitscontroleurs. MIAUW verwijst naar en maakt gebruik van diverse bewezen open standaarden voor de uitvoering van pentesten, zoals van het Open Web Application Security Project (OWAPS), de Penetration Testing Execution Standard (PTES) en het Common Vulnerability Scoring System (CVSS). MIAUW vervangt dergelijke standaarden niet, maar integreert deze in een methodiek.

Keurmerk pentesten
In het kader van deze verkenning is het keurmerk van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) van belang om te vermelden. Om ervoor te zorgen dat aanbieders van pentesten kwalitatief goed werk leveren is

[7] Meer informatie is te vinden op: https://www.aivd.nl/onderwerpen/informatiebeveiliging/certificeringen/baseline-security-product-assessment

door het CCV het keurmerk Pentesten ontwikkeld. Organisaties die Pentest opdrachten geven aan leveranciers voor de uitvoering van pentesten kunnen naar dit keurmerk vragen, met als doel dat de aanbieder van de pentest kan aantonen dat het kwalitatief goed werk kan leveren. Keurmerk [8].

Raamovereenkomst Pentesten Rijk
De Rijksoverheid heeft categoriemanagement ingericht voor de gezamenlijke of gecoördineerde inkoop van goederen en diensten, waar veel ministeries behoefte aan hebben. De categorie ICT-Professionals is een van deze rijksbrede inkoopcategorieën, gepositioneerd bij het ministerie van Economische Zaken. Deze categorie maakt via diverse raamovereenkomsten afspraken met bedrijven die externe ICT/IV[9]-professionals aan de ministeries kunnen leveren. De categorie is voornemens om medio 2026 een raamovereenkomst voor pentesten te sluiten. Bijna alle ministeries, diverse hoge colleges van staat en enkele zelfstandige bestuursorganen hebben aangegeven hieraan te willen deelnemen. De aanbesteding voor deze raamovereenkomst pentesten wordt in 2025 uitgevoerd. In deze aanbesteding en raamovereenkomst pentesten zal een vaste set inkoopeisen en contractuele voorwaarden worden toegepast, die zullen gelden als de gecontracteerde bedrijven na opdrachtverstrekking binnen deze raamovereenkomst pentesten gaan uitvoeren. De eisen en voorwaarden zijn gebaseerd op MIAUW en zijn deels gewijzigd en aangevuld om beter tegemoet te komen aan de behoeftes van de deelnemers aan de raamovereenkomst. Ook is rekening gehouden met reacties van marktpartijen, die hebben deelgenomen aan een (openbare) marktconsultatie over onder meer de inkoopeisen en voorwaarden voor het uitvoeren van pentesten.

Cyberbeveiligingswet
Verder ben ik voornemens om de Baseline Informatiebeveiliging Overheid 2 (BIO2) overheidsbreed[10] te verplichten via een ministeriële regeling onder de Cyberbeveiligingswet en -besluit (Cbw en Cbb)[11]. In BIO2 is het uitvoering van penetratietesten een van de voorgenomen 'O-maatregelen'[12].

2. Conclusie
Om opvolging te geven aan de toezegging van de Stass BZK om de Tweede Kamer te informeren over de uitkomsten van deze verkenning, na het zomerreces van 2025, wordt voorgesteld om de volgende passage op te nemen in een bredere Kamerbrief inzake digitalisering.

¨Op 17 december 2024 heeft de Tweede Kamer een motie van het lid Six Dijkstra aangenomen. In deze motie wordt de regering verzocht om overheidsbreed toe te werken naar een gestandaardiseerde methodiek voor het opdrachtgeverschap van pentests, zoals de Methodiek voor Informatiebeveiligingsonderzoek met Audit Waarde (MIAUW). Tijdens de behandeling van deze motie is door de toenmalige staatssecretaris van digitalisering en Koninkrijksrelaties aangegeven dat hij het

[8] https://www.securify.nl/en/blog/hoera-wij-hebben-het-ccv-keurmerk-behaald-met-frisse-tegenzin/
[9] Informatievoorziening wordt hier als IV afgekort.
[10] Voor zover een overheidsorganisatie kan als zodanig worden gekwalificeerd in de context van de Cbw. Hiervoor hanteert de Cbw (als gevolg van NIS2) vier criteria. Zie art 1 Cbw onder 'overheidsinstantie'.
[11] De minister van Justitie en Veiligheid heeft onlangs de Cbw en Cbb naar uw Kamer gestuurd. De ministeriële regeling is nog in voorbereiding. Zie *Kamerstukken II* 2024-2025, 36 764, nr. 2, nr. 3 en nr. 6.
[12] Specifiek bij beheersmaatregel 8.8 van ISO27002.

doel achter de motie deelt, maar dit eerst wil verkennen. Inmiddels is er intern verkend en op basis daarvan kan ik aangeven dat voor de Rijksoverheid invulling wordt gegeven aan de motie door het voornemen om in 2026 een raamovereenkomst voor pentesten te sluiten waaraan bijna alle ministeries, diverse hoge colleges van Staat en enkele zelfstandige bestuursorganen zullen deelnemen. Als een opdrachtgever binnen deze raamovereenkomst een pentest laat uitvoeren door een van de contracteerde bedrijven, zal hierop een vaste set inkoopeisen en contractuele voorwaarden van toepassing zijn. De eisen en voorwaarden zijn gebaseerd op MIAUW en doorontwikkeld om beter tegemoet te komen aan de behoeftes van de opdrachtgevers binnen de raamovereenkomst en vele marktpartijen die hebben deelgenomen aan een openbare marktconsultatie. Informatie over deze marktconsultatie en de aanbesteding voor pentesten is en wordt openbaar gedeeld via TenderNed, het aanbestedingsplatform voor de Nederlandse overheid. Daarmee is de informatie ook beschikbaar voor mede-overheden. Deze initiatieven dragen bij aan de invulling van kwalitatief goed opdrachtgeverschap voor pentesten en zijn in lijn met het doel achter de motie.

Informatie die niet openbaar gemaakt kan worden
Alle persoonsgegevens van ambtenaren geanonimiseerd.