Testen en oefenen ter verbetering van informatiebeveiliging bij provincies, gemeenten en waterschappen

Literatuurstudie

Opdrachtgever: ICTU

Auteurs:
Dr. Marcel Spruit,
Lector Cyber Security & Safety

Dr. Emiel Kerpershoek,
Senior Onderzoeker Cybersecurity

De Haagse Hogeschool,
Kenniscentrum Cybersecurity
Lectoraat Cyber Security & Safety

Juli 2023

DE HAAGSE HOGESCHOOL

De Haagse Hogeschool
Johanna Westerdijkplein 75
2521 EN Den Haag
www.dehaagsehogeschool.nl

Auteurs:
Dr. Marcel Spruit
Dr. Emiel Kerpershoek

Foto's/illustraties omslag en binnenwerk: Shutterstock.com
Vormgeving: Desk-Hopping DTP

INHOUDSOPGAVE

1 Inleiding

1.1 Aanleiding

Testen en oefenen zijn belangrijk om inzicht te krijgen in de effectiviteit van de genomen beveiligingsmaatregelen. Daarmee draagt dit thema direct bij aan het verbeteren van de feitelijke veiligheid.

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) wil graag meer inzicht in de huidige en gewenste situatie op het gebied van testen en oefenen in het kader van informatiebeveiliging bij de medeoverheden. Met dit inzicht kan actief beleid worden gevoerd om het gebruik van testen en oefenen bij de medeoverheden te stimuleren. Bij BZK is weinig bekend over hoe de medeoverheden in Nederland testen en oefenen gebruiken om invulling te geven aan de stappen Check en Act van de PDCA-cyclus voor informatiebeveiliging.[1] [2]

1.2 Doelstelling

Het doel is dat de betrokken partijen leren van dit onderzoek. Tevens is een doel om testen en oefenen te stimuleren om zo de informatiebeveiliging te verbeteren. Door goede praktische voorbeelden op dit thema met elkaar te delen kan dit thema verder worden gestimuleerd.

Testen en oefenen vormen essentiële onderdelen van professionele informatiebeveiliging. Door te testen ontstaat een concreet beeld van de kwaliteit van de informatie-beveiliging en de verbeterpunten hierin. Door te oefenen kunnen de verbeterpunten worden aangepakt. Vanuit deze gedachte is er behoefte aan een onderzoek dat resulteert in een praktisch en gedragen advies dat antwoord geeft op de volgende onderzoeksvragen:

1. Wat is de huidige situatie van testen en oefenen in het kader van informatiebeveiliging bij de sectoren provincies, gemeenten en waterschappen?
2. Wat is op dit gebied de gewenste situatie en behoefte bij deze overheden?
3. Wat is nodig om de gewenste inzet van testen en oefenen ten behoeve van de verbetering van informatiebeveiliging door deze overheden te bereiken?

1.3 Focus literatuurstudie

Deze literatuurstudie richt zich op de volgende vijf onderzoeksvragen:

1. Wat is bekend over het gebruik van testen en oefenen door medeoverheden in Nederland en buurlanden?
   a. Techniek, middelen, frequentie.
   b. Wat gebeurt er met de resultaten van testen en oefenen?
   c. Zijn er verschillen tussen provincies, gemeenten en waterschappen?
2. Welke typen van testen en oefenen kunnen worden onderscheiden en van welke rapportagevormen wordt gebruikgemaakt?
3. Welke goede praktische voorbeelden (good practices) zijn te vinden?
4. Wat zeggen de standaarden over de uitvoering van, de eisen aan en de randvoorwaarden voor testen en oefenen en zijn hierbij verschillen tussen provincies, gemeenten en waterschappen?
5. Wat is bestuurlijk nodig om het thema ‘testen en oefenen’ goed op de agenda te krijgen en welk empirisch onderzoek is daarnaar gedaan?

1.4 Aanpak literatuurstudie

Deze literatuurstudie richt zich op testen en oefenen in het kader van informatiebeveiliging. Hiervoor zijn relevante wetenschappelijke literatuur, (inter)nationale standaarden en vakliteratuur bestudeerd. Voor sommige aspecten is veel literatuur voorhanden en hebben wij een selectie gemaakt. Voor andere aspecten is juist weinig literatuur voorhanden en kunnen we alleen een globaal beeld beschrijven. De resultaten geven inzicht in de voornaamste vormen van testen en oefenen die relevant zijn en in het werkveld (kunnen) worden toegepast. De aspecten waar de literatuur nog te weinig duidelijkheid over geeft, kunnen in vervolgonderzoek met behulp van interviews verder onderzocht worden.

1 Groot, S., & Haalem, N. (2015). *Planmatig werken aan kwaliteit*. Bijzijn XL, 3(8), 20-23.

2 Zie ook Eloff, J. H. P., & Eloff, M. M. (2005). *Information security architecture*. Computer Fraud & Security, 2005(11), 10-16.

2 Testen

2.1 Wat is testen?

Testen is het onderwerpen van een persoon, systeem, of proces aan een toetsing van kwaliteit of geschiktheid.[3] De gerealiseerde score wordt veelal, maar niet per se, gerelateerd aan een te behalen doel of norm. In de internationale literatuur over informatiebeveiliging is het nodige geschreven over testen, maar toch wordt het concept testen hierbij niet altijd nauwgezet gedefinieerd. In artikelen waarin dat wel gebeurt, wordt testen veelal op een vergelijkbare wijze gedefinieerd. Zo wordt testen bijvoorbeeld omschreven als "een proces om te evalueren of een systeem of systeemcomponenten wel of niet voldoen aan gespecificeerde criteria".[4]

In internationale standaarden voor informatiebeveiliging wordt testen als instrument vaak wat uitvoeriger uiteengezet. Hierbij valt op dat standaarden een wat andere invalshoek kunnen hanteren in de definitie van testen.[5] In sommige standaarden wordt gebruikgemaakt van een componentendefinitie van testen. Zo wordt in de ISO-vocabulaire die is gericht op informatiebeveiligingsprocessen testen omschreven aan de hand van de activiteiten die nodig zijn voor het uitvoeren van testen zoals "het belang van meten, verifiëren, analyseren en evalueren voor continue verbetering van het ISMS".[6] Toegespitst op het testen van software wordt testen gedefinieerd als activiteiten die worden uitgevoerd om de eigenschappen van een of meer testitems in kaart te brengen of te evalueren. Deze activiteiten omvatten planning, voorbereiding, uitvoering, rapportage en management van alle testgerelateerde aspecten.[7]

In andere standaarden wordt juist een meer doelgeoriënteerde definitie van testen gehanteerd. In de NIST-vocabulaire wordt testen omschreven als een proces waarin wordt vastgesteld of het functioneren van een of meerdere testobjecten overeenkomt met het verwachte functioneren van deze objecten. De uitkomst van het testen dient om ontwikkelingen in effectiviteit van informatiebeveiligingsmaatregelen over tijd bij te houden.*8* In de standaard NIST SP 800-84, die zich specifiek richt op testen en oefenen in het kader van incident respons, wordt testen omschreven als een evaluatie-instrument dat gebruikmaakt van metingen om de operabiliteit van een systeem of systeemcomponenten te verifiëren die relevant zijn in het kader van uitwijk en herstel.[9]

In de Baseline Informatiebeveiliging Overheid (BIO)[10], welke leidend is voor de inrichting van de informatiebeveiliging bij Nederlandse overheden, wordt het concept testen in het kader van informatiebeveiliging niet als zodanig gedefinieerd. Wel geeft de BIO richting aan wat moet worden getest (o.a. systeembeveiliging, systeemacceptatie, back-ups en wijzigingen aan besturingsplatforms) en wie daarvoor verantwoordelijk is (doorgaans de dienstenleverancier en/of de proceseigenaar).

In het kader van dit onderzoek wordt testen van informatiebeveiliging gedefinieerd als:
Het meten of de effectiviteit van informatiebeveiligingsmaatregelen op een gegeven moment voldoet aan vooraf gespecificeerde criteria.

2.2 Functie

In de standaard ISO/IEC 27002:2022 wordt het doel van testen in het kader van informatiebeveiliging omschreven als het "*Valideren of aan de informatiebeveiligingseisen wordt voldaan wanneer toepassingen of code in de productieomgeving worden uitgerold.*"[11] Het is namelijk van belang dat nieuwe informatiesystemen, upgrades en nieuwe versies grondig worden geverifieerd. De informatiebeveiligingseisen kunnen betrekking hebben op de volgende aspecten:[12] [13]

- **Vertrouwelijkheid**: waarmee wordt zorggedragen dat gegevens alleen toegankelijk zijn voor mensen die daartoe geautoriseerd zijn.
- **Integriteit**: waarmee wordt zorggedragen dat toegang of aanpassing van systemen, componenten en gegevens wordt verhinderd.
- **Beschikbaarheid**: waarmee wordt zorggedragen dat informatie beschikbaar en toegankelijk is.

3 Van Dale, *Dikke Van Dale*, 2023. **https://zoeken.vandale.nl/**
4 Kaur, N., & Bahl, K. *Performance testing of insititute website using jmeter*, International Journal of Innovative Science, Engineering & Technology, 3(4), pag. 534-537, 2016.
5 O.a. ISO/IEC 27000-reeks voor informatiebeveiliging, ISO/IEC 27701 voor privacy informatiemanagement, ISO/IEC 27035 voor incidentmanagement, ISO/IEC 29119-reeks voor software en systems engineering.
6 *NEN-ISO/IEC 27000:2014, Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Overzicht en woordenlijst*, NEN, 2014.
7 *ISO/IEC/IEEE 29119-2:2021, Software and systems engineering - Software testing - Part 2: Test processes*, ISO/IEC/IEEE, 2021.
8 *NIST SP 800-53 Rev.5, Security and Privacy Controls for Information Systems and Organizations*, NIST, 2020.
9 *NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, NIST, 2021.
10 *Baseline Informatiebeveiliging Overheid*, versie 1.04, Ministerie van BZK, 2019.
11 *NEN-ISO/IEC 27002:2022, Informatietechnologie - Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging*, NEN, 2022.
12 *NEN-ISO/IEC 27000:2014.*
13 *ISO/IEC 27001:2022, Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen,* ISO, 2022.

De uitkomsten van testen kunnen worden gebruikt om (ontwikkelingen in) de effectiviteit van informatiebeveiligingsmaatregelen die zijn gericht op mensen, techniek, of processen in kaart te brengen.[14] [15] [16] [17] Zo kunnen testen onder andere worden gebruikt voor:

- Het detecteren van defecten, tekortkomingen en kwetsbaarheden in mensen, techniek en processen.
- Het verzamelen van informatie die kan worden gebruikt voor bijvoorbeeld het verbeteren van kennis en vaardigheden van mensen, het verbeteren van technische beveiligingsmaatregelen voor software en systemen, en verbetering van beleid, procedures en plannen op het gebied van informatiebeveiliging.
- Het genereren van vertrouwen in mensen, techniek en processen op het gebied van informatiebeveiliging.
- Het ondersteunen van besluitvorming, bijvoorbeeld over livegang van systemen of componenten.

In veel gevallen hebben testen meerdere doelen.

2.3 Reikwijdte

Testen kunnen zijn gericht op de volgende toepassingsdomeinen:

- **Mensen**: de gebruikers van de informatiesystemen en degenen die zich bezighouden met het beveiligen van informatiesystemen.
- **Techniek**: de hard- en software van de informatiesystemen op het netwerk of in de cloud.
- **Processen**: de processen voor de beveiliging van de informatiesystemen die zich afspelen binnen de organisatie en bij de betrokken dienstenleveranciers.

Hiernaast kan ook onderscheid gemaakt worden op basis van de scope of reikwijdte van testen in het kader van informatiebeveiliging. Hierbij worden in het kader van dit onderzoek twee niveaus onderscheiden:[18]

- **Component testen**: Dit richt zich op het testen van individuele componenten. Deze componenten kunnen betrekking hebben op bijvoorbeeld functionarissen van een specifieke afdeling of met een specifieke functie (mensen), onderdelen van hard- en software die worden gebruikt (techniek), of onderdelen van informatiebeveiligingsprocessen (processen).
- **Omvattend testen**: Dit heeft een bredere scope, namelijk het in samenhang testen van mensen, techniek en processen.

2.4 Typen

Testen in het kader van informatiebeveiliging kunnen zowel op componentniveau gericht zijn of omvattend zijn en kunnen als volgt worden ingedeeld:[19] [20] [21] [22] [23] [24] [25]

- **Kennis/vaardigheden testen**:
  - **Kwalificaties**: Testen van kwalificaties van bijvoorbeeld sollicitanten voor IT- en informatiebeveiligingsfuncties aan de hand van functieprofielen.
  - **Risicobewustzijn**: Testen van risicobewustzijn van medewerkers, waaronder ook testen met behulp van phishing en social engineering.
  - **Bekendheid met procedures**: Testen van bekendheid met en begrip van procedures onder medewerkers.
  - **Toetsen en examens**: Testen van kennis en vaardigheden voor medewerkers in informatiebeveiligingsgerelateerde functies. Denk aan toetsen op het gebied van informatiebeveiligingscompetenties door bijvoorbeeld ISACA (CISM, CISSP, etc.), of SANS (GSEC, GPEN, etc.).

14 *NIST SP 800-53 Rev.5.*
15 Zie bijvoorbeeld *ISO/IEC/IEEE 29119-1:2021*.
16 Zie bijvoorbeeld *NIST SP 800-84.*
17 Zie bijvoorbeeld *ISO/IEC 17024:2012*, Conformity assessment - General requirements for bodies operating certification of persons, ISO/IEC, 2012.
18 In *NIST SP 800-84* worden drie niveaus onderscheiden, component, systeem en comprehensive. In dit onderzoek wordt, evenals in in *ISO/IEC 27002* wordt geen expliciet onderscheid gemaakt tussen system testing en comprehensive testing omdat de scheidingslijn tussen deze niveaus vaak dun is.
19 *ISO/IEC 27002:2022*.
20 *NIST SP 800-53 Rev.5.*
21 *ISO/IEC 27021:2017, Information technology - Security techniques - Competence requirements for information security management systems professionals*, ISO/IEC, 2017.
22 *ISO/IEC/IEEE 29119-4:2021.*
23 *ISO/IEC 27035-2:2023 - Information technology - Information security incident management - Part 2: Guidelines to plan and prepare for incident response*, International Organization for Standardization, 2023
24 *Baseline Informatiebeveiliging Overheid*.
25 Zie ook **https://owasp.org/www-project-web-security-testing-guide/stable/**

- **Reviews**:
  - **Codereviews:** Programmacode beoordelen op zwakke plekken in de beveiliging, met inbegrip van onvoorziene inputs en omstandigheden.
  - **Beleidsreviews**: Het beoordelen van informatiebeveiligingsbeleid, procedures, of plannen op tekortkomingen en uitvoerbaarheid.
  - **Audit**: Het beoordelen van informatiebeveiliging op basis van een standaard of baseline voor informatiebeveiliging, zoals de BIO.
  - **Kwetsbaarhedenscans**: Het scannen van technische systemen om onveilige configuraties en kwetsbaarheden in systemen te identificeren.

- **Technische testen**:
  - **Acceptatietest:** Om voor livegang te verifiëren of nieuwe toepassingen of code voldoen aan de informatiebeveiligingseisen.
  - **Functietest**: Het testen van de werking van specifieke software of systeemonderdelen na updates of systeemwijzigingen.
  - **Penetratietesten**: Het gebruik van een gesimuleerde aanval op de digitale systemen van een organisatie om onveilige code en ontwerpen te identificeren en systeemafhankelijk in kaart te brengen.
  - **Back-up en recoverytest:** Het testen op functioneren en toereikendheid van back-ups en het goed kunnen terugzetten van back-ups.

- **Procestesten**:
  - **Testen van uitwijk- en herstelplannen**: Het testen van de plannen voor het herstellen en zo nodig verplaatsen van (onderdelen van) de bedrijfsvoering naar een andere locatie (fysiek of in de cloud) wanneer een cyberincident is geëscaleerd naar een crisis. Zo kan bijvoorbeeld getest worden of de hersteltijddoelstelling (RTO) en het maximaal toelaatbare dataverlies (RPO) bij uitvoering worden gerealiseerd.
  - **Volwassenheidsmeting**: Het meten van de volwassenheid en weerbaarheid van de organisatie op gebied van informatiebeveiliging aan de hand van een volwassenheidsmodel.[26]
  - **Red team/Blue team**: Het simuleren van een cyberaanval op de organisatie door het 'rode team', waartegen het 'blauwe team' de organisatie moet verdedigen, om zo te bepalen of de informatiebeveiliging van de organisatie sterk genoeg is.

Tabel 2.1 Overzicht van typen testen per toepassingsdomein

Toepassingsdomein	Typen testen
Mensen	**Kennis/vaardigheidstest**: Kwalificaties, Risicobewustzijn, Bekendheid met procedures, Toetsen en examens
Techniek	**Review**: Code reviews, Kwetsbaarhedenscans **Technische test**: Acceptatietest, Functietest, Penetratietest, Back-up- en recovery-test
Processen	**Review**: Beleidsreviews, Audits **Procestest:** Testen van uitwijk- en herstelplan, Volwassenheidsmeting, Red team/Blue team

2.5 Randvoorwaarden

In de geraadpleegde literatuur over testen in het kader van informatiebeveiliging komen verschillende randvoorwaarden en richtlijnen voor het uitvoeren van testen aan bod.[27] [28] [29] [30] Deze kunnen betrekking hebben op:

1. **Het moment van testen**: Nieuwe informatiesystemen, upgrades en nieuwe versies behoren grondig te worden geverifieerd. Het testen van de informatiebeveiliging behoort een integraal onderdeel te zijn van het geheel van het testen voor systemen of componenten.
2. **De testvoorbereiding**: Voorafgaand aan het testen is een testplan nodig waarin de testdoelen zijn geformuleerd, de activiteiten die moeten worden uitgevoerd om die doelen te behalen en de beoordelingscriteria om vast te stellen of een test is geslaagd. Hiernaast kan in het testplan worden omschreven welke verdere acties naar gelang de testuitslag nodig zijn, bijvoorbeeld het informeren van management of het treffen van compenserende maatregelen.
3. **De testomgeving:** Voor de betrouwbaarheid van de testen behoren deze te worden uitgevoerd in een omgeving die zoveel mogelijk overeenkomt met de productieomgeving, maar niet in de actieve productieomgeving om te voorkomen dat er verstoringen ontstaan.
4. **De test-governance:** Testen moeten worden uitgevoerd door onafhankelijke, competente en bevoegde personen. Soms kan het echter van belang zijn om ontwikkelaars te betrekken bij het testen wanneer er behoefte is aan hun specifieke kennis en ervaring.

26 Zie bijvoorbeeld M. Spruit (2017), *Volwassenheid informatiebeveiliging; 3-Pijlermodel.*
27 *ISO/IEC 27002:2022.*
28 *NIST SP 800-53 Rev.5.*
29 *ISO/IEC/IEEE 29119-1:2021.*
30 *ISO/IEC/IEEE 29119-2:2021.*

3 Oefenen

3.1 Wat is oefenen?

Oefenen is het door herhaling een of meer vaardigheden verkrijgen of verbeteren.[31] [32] [33] Oefenen heeft altijd betrekking op een persoon of een groep, al dan niet in de context van een gegeven situatie of proces.[34] In plaats van oefenen wordt ook wel de term trainen gehanteerd.[35] [36] Oefenen wordt beschouwd als een vorm van leren.

Leren kan betrekking hebben op het verkrijgen of verbeteren van vaardigheden, maar ook op het verkrijgen of verbeteren van kennis en bewustzijn.[37] Voor oefenen, het verkrijgen of verbeteren van vaardigheden, geldt dat een zekere mate van kennis randvoorwaardelijk is.[38] Veelal gaat het verkrijgen of verbeteren van kennis en vaardigheden dan ook hand in hand.

Oefenen is gebaat bij herhaling, maar ook een enkelvoudige oefening van een bepaalde vaardigheid kan al een positief effect hebben. Indien een bepaalde vaardigheid vaak wordt geoefend, kan deze vaardigheid een automatisme worden. In het pad naar een automatisme kunnen een paar stadia worden onderscheiden, te beginnen bij onbewust onbekwaam zijn, naar bewust onbekwaam zijn, naar bewust bekwaam zijn en te eindigen in onbewust bekwaam zijn. In het laatste stadium is de toepassing van de vaardigheid geautomatiseerd. Een automatisme heeft als voordeel dat de betreffende vaardigheid snel en efficiënt ingezet kan worden. Het nadeel is dat de betreffende vaardigheid minder flexibel is.

Oefenen heeft een relatie met testen. Door te oefenen verkrijgt of verbetert een persoon of groep vaardigheden. Door de gerealiseerde vaardigheden te testen kan worden beoordeeld of de beheersing van deze vaardigheden door de betreffende persoon of groep voldoende is voor een bepaalde taak of functie. Overigens kan het testen van vaardigheden gezien worden als een enkelvoudige oefening die al een positief effect kan hebben op de geteste vaardigheden.

In de internationale literatuur is het nodige geschreven over oefenen in het kader van informatiebeveiliging. De concepten oefenen zijn hierbij niet altijd duidelijk gedefinieerd. In internationale standaarden voor informatiebeveiliging wordt het concept oefenen en de wijze waarop deze kunnen worden uitgevoerd vaak nader uitgewerkt.Bekende baselines op het gebied van informatiebeveiliging, zoals de BIO[39], de ISO/IEC 27002:2022[40] en de NIST SP 800-53[41], geven aan dat geregeld oefenen nodig is om medewerkers geschikt te laten zijn voor hun taken en functies, maar laten in het midden wat er hoe vaak en met welke typen oefeningen geoefend moet worden.

3.2 Functie

In grote lijnen omschrijven de NIST- en ISO-standaarden dezelfde doelen voor het gebruik van oefenen in het kader van informatiebeveiliging. In de standaard ISO/IEC 27035-2[42] wordt aangegeven dat oefenen kan dienen om mensen te trainen in de uitoefening van hun rollen, maar ook kan dienen om te zien of nieuwe of bestaande processen en procedures werken zoals nodig is.

Het toepassingsgebied dat de standaarden aanhouden voor het oefenen in het kader van de informatiebeveiliging varieert. Zo is in de ISO/IEC 27035-2[43] en de NIST SP 800-84[44] de betekenis van oefenen gericht op het oefenen in het kader van incidentherstel- en uitwijkplannen. De betreffende NIST-standaard richt zich meer op het beoordelen van plannen en procedures, terwijl de betreffende ISO-standaard zich ook richt op het verkrijgen en verbeteren van vaardigheden.

31 *Dikke Van Dale*.
32 D. A. Bernstein, *Psychology*, Cengage Learning, 2016.
33 Zie ook NCTV Magazine 1 Juli 2021, *Oefening baart kunst,* **https://magazines.nctv.nl/nctvmagazine/2021/01/oefening-baart-kunst**
34 S.P. Robbins en T.A. Judge, *Gedrag in organisaties*, Pearson, 2020.
35 D.A. Kolb, *Experiential Learning: Experience as the source of learning and development*. Prentice-Hall, 1984
36 L.H. Lewis en Williams, C. J. *Experiential learning: Past and present*. New directions for adult and continuing education, 62, pag. 5-16, 1994.
37 B. S. Bloom en anderen, *Taxonomy of Educational Objectives, Book 1: Cognitive Domain*, David McKay, 1956.
38 *NIST SP 800-84.*
39 *Baseline Informatiebeveiliging Overheid*, versie 1.04, Ministerie van BZK, 2019.
40 *ISO/IEC 27002:2022*.
41 *NIST SP 800-53 Rev.5*.
42 *ISO/IEC 27035-2:2023*.
43 *ISO/IEC 27035-2:2023*.
44 *NIST SP 800-84*.

Oefenen kan bovendien een verbindende functie hebben.[45] Door te oefenen kan de communicatie tussen verschillende eenheden binnen de organisatie zoals het bestuur, senior management, de ICT-afdeling, de informatiebeveiligers en de communicatiemedewerkers worden verbeterd, alsook de afstemming met externe betrokkenen. Hiermee kan oefenen dienen om de interne en externe communicatie te verbeteren en om ketenafhankelijkheden inzichtelijk te maken.

3.3 Reikwijdte

De reikwijdte van oefenen kan verschillen. De reikwijdte kan enerzijds betrekking hebben op een persoon of een groep, en anderzijds op losstaande vaardigheden of (een deel van) een organisatieproces. Net als voor testen geldt dat oefenen zich kan richten op componentniveau of juist meer omvattend kan worden toegepast. Zo kan bijvoorbeeld een functionaris in een externe cursus aan bepaalde vaardigheden werken die de functionaris op de werkvloer nodig heeft. Aan de andere kant kunnen alle functionarissen die een rol hebben in het incidentmanagementproces dit proces gezamenlijk oefenen aan de hand van een hypothetisch incident.

Het oefenen kan plaatsvinden buiten de context waarin de vaardigheden nodig zijn, of juist binnen deze context. In het eerste geval spreken we van een leer- of laboratoriumomgeving. Een voorbeeld hiervan is een simulator of een serious game. In het tweede geval vindt het oefenen plaats binnen het proces en de organisatie waarin de vaardigheden nodig zijn. In dat geval gaat het om een real-life oefening.

3.4 Typen

Oefenen in het kader van informatiebeveiliging kan als volgt worden ingedeeld:[46] [47] [48] [49] [50] [51]

- **Leeroefeningen**, waarbij deelnemers zich individueel of in groepen richten op het ontwikkelen van kennis en vaardigheden. De scenario's die in deze oefeningen worden toegepast, en daarmee ook deze kennis en vaardigheden die met deze leeroefeningen worden vergaard, staan in principe los van processen in de organisatie. Leeroefeningen zijn primair gericht op persoonlijke leeropbrengsten. Voorbeelden van leeroefeningen zijn:
  - Individuele leeroefeningen:
    - **Workshop**: In een workshop wordt individueel een scenario stap voor stap doorlopen. Het biedt de mogelijkheid om de reacties en acties van individuele deelnemers te repeteren zonder tijdsdruk.
    - **Praktijkoefeningen**: Denk hierbij aan oefenen met techniek in bijvoorbeeld practica, programmeeroefeningen, lab-oefeningen of netwerkanalyses. Ook games als Hack The Box (HTB) en Capture the Flag (CtF) vallen hieronder. Bij dit soort games is het doel dat aanvallers in (gesimuleerde) ICT-systemen een vooraf bepaald doel bereiken. Hierbij is het voor de aanvaller de kunst om allerlei barrières en beveiligingsmaatregelen ongeschonden te passeren. Dit soort games is met name geschikt om aanvallende vaardigheden te oefenen.
    - **Training-on-the-job**: Hierbij begeleidt een meer ervaren medewerker een minder ervaren medewerker. Denk bijvoorbeeld aan een mentor of coach die een junior of trainee begeleidt.
  - Leeroefeningen voor groepen:
    - **Groepsdiscussie**: Aan de hand van dilemma's die gestoeld zijn op de werkvloer van de organisatie, wordt groepsgewijs een discussie gevoerd. Bij voorkeur wordt gebruikgemaakt van een moderator om de discussie goed te laten verlopen. De discussies verhogen bij de deelnemers zowel het inzicht in de besproken problematiek, alsook het draagvlak voor de voorgedragen oplossingen.

45 *Handleiding en draaiboek opzetten cybercrisisoefeningen*, SURF, 2017.
46 *NIST SP 800-84.*
47 *ISO/IEC 27035-2:2023.*
48 *Handleiding en draaiboek opzetten cybercrisisoefeningen.*
49 Voor laagdrempelige oefeningen zie **https://www.linuxjournal.com/content/example-security-exercises**
50 D.A. Kolb, *Experiential Learning: Experience as the source of learning and development.*
51 L.H. Lewis en Williams, C. J. *Experiential learning: Past and present.*.

- **Procesoefeningen** zijn erop gericht om groepen medewerkers met behulp van scenario's te laten oefenen met het uitvoeren van taken en procedures. Procesoefeningen zijn primair gericht op het verbeteren van organisatieprocessen. Er kan onderscheid worden gemaakt tussen simulatie- en real-life procesoefeningen:
  - **Simulatie**: Deze eerste categorie van procesoefeningen is erop gericht een taak of proces te oefenen in een gesimuleerde werksituatie. Hierbij kunnen vereenvoudigingen in de simulatie worden doorgevoerd om niet alle complexiteit van de werksituatie tegelijk in het oefenen te betrekken. In bepaalde gevallen kan het nuttig zijn om een deeltaak of een deelproces te oefenen in plaats van de hele taak of het hele proces. Enkele voorbeelden zijn:
    - **Desk check, of walkthrough**: Een desk check of walkthrough is een groepsgesprek waarin (wijzigingen van) plannen of procedures worden besproken en beoordeeld. In dit gesprek, waarin doorgaans ook de auteur van de plannen of procedures is betrokken, worden de plannen of procedures aan de hand van een scenario stap voor stap doorlopen. Dit maakt duidelijk welke stappen nodig zijn en door wie en hoe deze uitgevoerd moeten worden.
    - **Rollenspel**, **managementgame**, of **tabletop-oefening**: Een oefening op basis van een scenario dat 'op tafel' wordt nagespeeld. Spelers krijgen van tevoren informatie over de gesimuleerde situatie en hun rol. Tijdens de oefening kunnen spelers gebruikmaken van gesimuleerde (media)berichten. Het team kan relevante informatie delen, overzicht krijgen, besluiten nemen en (communicatie) maatregelen treffen. Een dergelijke oefening is een goede optie als men in relatieve rust de onderlinge samenwerking wil oefenen en/of specifieke vaardigheden wil trainen.
    - **Distributed tabletop-oefening**: Bij de distributed tabletop-oefening worden plannen en procedures doorlopen op basis van een scenario waarbij spelers hun rol volgens routine spelen. Deze oefening is grotendeels gelijk aan een tabletop-oefening, met als verschil dat deelnemende teams van elkaar zijn gescheiden waardoor, net als in de praktijk, onderlinge afstemming wordt bemoeilijkt. Dit maakt de distributed tabletop-oefening realistischer dan de reguliere tabletop-oefening. Deelnemers moeten handelen alsof er daadwerkelijk een crisis plaatsvindt. De mogelijke reacties kunnen eventueel later in een evaluatie worden besproken. Deze oefening heeft als voordeel dat deelnemers de handelingen routinematig kunnen oefenen.
    - **Simulatieoefening** of **Command Post Exercise (CPX)**: Bij een simulatieoefening of CPX speelt men in de eigen omgeving een realistisch scenario na. Deelnemers oefenen zoveel mogelijk onder normale omstandigheden met eigen middelen in de eigen omgeving. Het scenario van de oefening ontwikkelt zich aan de hand van de eigen besluiten en acties. Een simulatieoefening is geschikt als men wil oefenen onder druk en de reacties van deelnemers in de eigen omgeving wil testen en trainen. De intensiteit en de ontwikkeling in het scenario hangen af van het aantal deelnemers en hun ervaringsniveau. Ook is het van belang of alleen interne of ook externe partijen deelnemen.

- **Real-life**: Deze categorie procesoefeningen is er op gericht om een taak of proces te oefenen in de actuele werksituatie. Er wordt niet geacteerd en iedere oefenende functionaris doet zijn of haar eigen taken, zoals in de werksituatie. Om eventuele negatieve impact door fouten te voorkomen, kunnen maatregelen worden getroffen.
  Enkele voorbeelden zijn:
  - **Comms check**: Bij een Comms check worden bestaande communicatiemethoden of kennisgevingssystemen ingezet om te oefenen en te checken of alles werkt.
  - **Oproepoefening**: Bij deze oefening oefent een crisisteam om zo snel mogelijk bij elkaar en op gang te komen. Deze oefening neemt de vorm van een test aan wanneer hier een normtijd aan wordt verbonden.
  - **Red Team/Blue Team**: Bij een Red Team/Blue team-oefening valt het 'rode team' het IT-netwerk of een bepaald IT-systeem van de organisatie aan en moet het 'blauwe team' de aanval proberen te verijdelen. Deze oefening vergroot het bewustzijn van mogelijke risico's en het effect van de geïmplementeerde maatregelen. Ook geeft de oefening inzicht in de mogelijke kwetsbaarheden en manieren om hiermee om te gaan. Bovendien geeft de oefening inzicht in strategieën om een aanval te detecteren en erop te reageren.

Tabel 3.1 Overzicht van typen oefening per toepassingsdomein

Toepassingsdomein	Typen oefeningen
Mensen	**Individuele Leeroefeningen:** Workshop, praktijkoefeningen (denk aan: Capture the Flag- of Hack The Box-games, maar ook oefenen met tools en technieken om in te breken op servers en netwerken en phishing- en social engineering-oefeningen), training on the job **Leeroefeningen voor groepen:** groepsdiscussie
Techniek	Niet van toepassing
Processen	**Procesoefeningen Simulatie**: Desk check of Walkthrough, Rollenspel, Managementgame, Tabletop-oefening, Distributed tabletop-oefening, CPX **Procesoefeningen Real-life:** Comms check, Oproepoefening, Red Team/Blue Team

3.5 Randvoorwaarden

In de geraadpleegde literatuur over oefenen in het kader van informatiebeveiliging komen ook verschillende randvoorwaarden en richtlijnen voor het uitvoeren van testen aan bod.[52] [53] [54] Deze kunnen betrekking hebben op:

1. **De oefenvoorbereiding:**
   - Voorafgaand aan oefenen is een oefenplan nodig waarin het doel van de oefening, scenario's en eventuele informatie die tijdens de oefening kan worden ingebracht is beschreven.
   - Rollen en verantwoordelijkheden voor het uitvoeren van IT-plannen en aanverwante procedures moeten zijn vastgesteld en duidelijk zijn gecommuniceerd.
   - Betrokken medewerkers moeten over een voldoende niveau van kennis en vaardigheden beschikken voor het uitvoeren van hun taken en verantwoordelijkheden.
2. **De oefenomgeving:**
   - Draag zorg voor de veiligheid van alle deelnemers.
   - Adequate begeleiding bij het uitvoeren van de oefening.
   - Alle deelnemers weten dat het scenario dat wordt gebruikt een oefening is en geen werkelijke gebeurtenis en ze kennen het doel van de oefening.
   - Zorg ervoor dat de oefening ruimte biedt voor discussie tussen de deelnemers, maar niet zo veel dat de oefening er door uit koers raakt.
   - De oefening wordt uitgevoerd in een gecontroleerde omgeving waardoor wordt voorkomen dat effecten van de oefening kunnen doorwerken in de operationele praktijk.
3. **Opvolging van de oefening:**
   - Na afloop van de oefening is het van belang dat er voldoende tijd en ruimte is om de deelnemers te debriefen en feedback op te halen naar aanleiding van de oefening.
   - Hiernaast moet een rapportage van de oefening worden opgesteld die kan worden gedeeld met senior management en eventueel externe stakeholders.

52 *NIST SP 800-53 Rev.5.*
53 *ISO/IEC 27002:2022.*
54 *ISO/IEC 27035-2:2023.*

4 Testen en oefenen op de bestuurlijke agenda

Testen en oefenen in het kader van informatiebeveiliging zijn noodzakelijke onderdelen van informatiebeveiliging en geen op zichzelf staande onderwerpen. In het kader van integraal management kan de integrale verantwoordelijkheid voor een proces of systeem worden gedelegeerd. De strategische top van de organisatie kan ervoor kiezen om verticaal of horizontaal te delegeren naar een lagere manager.[55] Deze verantwoordelijkheid omvat niet alleen de strategie en planning voor het betreffende proces of systeem, maar ook het managen van de daarvoor benodigde mensen en middelen en het realiseren van de informatiebeveiliging ervan. In de meeste gevallen wordt de verantwoordelijkheid voor processen en systemen die specifiek zijn voor bepaalde organisatorische eenheden verticaal gedelegeerd naar lijnmanagers. De verantwoordelijkheid voor organisatiebrede processen en systemen wordt juist vaker horizontaal gedelegeerd naar stafmanagers. Dit neemt niet weg dat de eindverantwoordelijkheid voor de digitale weerbaarheid van de organisatie bij de strategische top van de organisatie blijft liggen. Dit houdt in dat doorlopend sturing moet worden gegeven aan het formuleren, implementeren en handhaven van het informatiebeveiligingsbeleid.[56] [57]

De manager die door verticaal of horizontaal delegeren verantwoordelijk is geworden voor een proces of systeem wordt aangeduid als de proces- of systeemeigenaar.[58] Het eigenaarschap omvat ook de verantwoordelijkheid voor informatiebeveiliging van het betreffende proces of systeem. Doordat testen en oefenen een integraal onderdeel is van informatiebeveiliging is de proces- of systeemeigenaar ook daarvoor verantwoordelijk.[59] [60] Dat testen en oefenen in het kader van informatiebeveiliging een verantwoordelijkheid is van de eigenaar van het betreffende proces of systeem betekent dat deze het testen en oefenen initieert en organiseert, daarvoor budget en ondersteuning beschikbaar stelt, en erop toeziet dat opvolging wordt gegeven aan de resultaten van het testen en oefenen.

Om eigenaren bij hun verantwoordelijkheden op het gebied van informatiebeveiliging te ondersteunen, is een staffunctie nodig voor deskundige ondersteuning en coördinatie op het gebied van informatiebeveiliging.[61] Dit kan bijvoorbeeld een CISO zijn, al dan niet met een CISO-office. Aan deze staffunctie kunnen door het topmanagement ook voorschrijvende, monitorende en controlerende taken op het gebied van informatiebeveiliging worden toegekend.

We hebben geen literatuur kunnen vinden die specifiek ingaat op het goed op de bestuurlijke agenda krijgen van testen en oefenen in het kader van informatiebeveiliging. Daar staat tegenover dat de literatuur over het goed op de agenda krijgen van informatiebeveiliging hier onverkort op van toepassing is. Veel standaarden op het gebied van informatiebeveiliging, waaronder ISO/IEC 27001[62], NIST SP 800-12[63], BIO[64], gaan ervan uit dat de strategische top van een organisatie zelf informatiebeveiliging op de agenda zet, informatiebeveiliging integreert in de organisatieprocessen, ondersteunende staf voor informatiebeveiliging inricht en voldoende middelen voor informatiebeveiliging vrijmaakt en hier waar mogelijk afspraken over maakt met dienstenleveranciers. In binnen- en buitenland gaat dat bij veel organisaties nog niet goed, zij het dat er de laatste jaren enige verbetering te zien is.[65] [66]

Als bestuurders bij zichzelf constateren dat ze onvoldoende inzicht hebben in hoe ze de informatiebeveiliging van hun organisatie zouden moeten aansturen, dan kunnen ze de 7-driveraanpak van het Centrum Informatiebeveiliging en Privacybescherming (CIP) gebruiken.[67] Deze aanpak is een leervorm die is gebaseerd op brainstorms en is gericht op een zevental onderwerpen die belangrijk zijn voor goede informatiebeveiliging. De bestuurders kunnen de brainstorms houden met bijvoorbeeld de CIO of de CISO van hun organisatie.

55 H. Buurma & C. Jacobs (red.), *Integraal management, inspirerend leiderschap in de publieke sector*, Lemma, 2007.
56 Cyber Security Raad CSR (2019), *Handreiking Cybersecurity voor de bestuurder*, 2019., **https://www.cybersecurityraad.nl/documenten/handreikingen/2019/10/01/handreiking_bestuurders**
57 Zie ook **https://bio-overheid.nl/media/e2lpzcpq/20220713-flyer-sturen-op-informatieveiligheid.pdf**
58 M. Spruit, *Informatie onder controle*, MS, 2018.
59 *NEN-ISO/IEC 27002:2022*.
60 H. Buurma & C. Jacobs (red.), *Integraal management, inspirerend leiderschap in de publieke sector.*
61 *NIST SP 800-39, Managing Information Security Risk*, NIST, 2011.
62 *ISO/IEC 27001:2022, Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen,* ISO, 2022.
63 *NIST SP 800-12 Rev 1 - An introduction to information security*, NIST, 2017.
64 *BIO versie 1*, Ministerie van BZK, 2019.
65 *The EY Global Information Security Survey 2021*, EY, 2022.
66 *2022 Global Digital Trust Insights Survey*, PwC, 2021.
67 **https://bio-overheid.nl/media/e2lpzcpq/20220713-flyer-sturen-op-informatieveiligheid.pdf**

Van binnenuit een organisatie kan de motivatie van de strategische top voor informatiebeveiliging worden versterkt door goede informatie te verstrekken over informatiebeveiligingsdreigingen, -risico's en -incidenten.[68] Het ligt voor de hand dat dit met name wordt opgepakt door informatiebeveiligers van de organisatie.

Bij organisaties waar de strategische top het onderwerp informatiebeveiliging desondanks nog niet goed op de agenda zet, kunnen toezichthouders, accountants en auditors druk op het management uitoefenen door om nadere onderbouwing van de inrichting van informatiebeveiliging te vragen bij inspecties, goedkeuring van financiële verslagen of auditrapporten. De motivatie voor informatiebeveiliging kan ook worden versterkt door de strategische top van verwante organisaties die zelf op dit gebied al verder gevorderd zijn. Bestuurders van andere organisaties kunnen dan dienen als ambassadeurs. Zij kunnen testen en oefenen in het kader van informatiebeveiliging bestuurlijk agenderen en de bestuurders die nog niet zover zijn proberen te overtuigen van het belang ervan.

68 M. Spruit, *Bewust veilig?*, De IT-Auditor 4, pag. 15-21, 2010.

5 Goede voorbeelden

De Rijksoverheid en medeoverheden in Nederland hebben in de afgelopen jaren diverse initiatieven ontplooid om het belang van testen en oefenen in het kader van informatiebeveiliging bij overheidsinstellingen onder de aandacht te brengen en het gebruik er van te stimuleren en te faciliteren. In dit hoofdstuk lichten we enkele goede voorbeelden van initiatieven toe die overheidsbreed, of door provincies, gemeenten, of waterschappen zijn ontwikkeld.

5.1 Overheidsbreed

5.1.1 Baseline Informatiebeveiliging Overheid (BIO)

Per 1 januari 2019 is het landelijk beleid dat alle overheidsorganisaties in Nederland moeten voldoen aan de Baseline Informatiebeveiliging Overheid (BIO). De BIO biedt een uniform normenkader voor de informatiebeveiliging bij Nederlandse overheidsorganisaties. De BIO geeft onder meer aan dat testen en oefenen nodig zijn op diverse terreinen van de informatiebeveiliging en specificeert wie verantwoordelijk is voor het plannen en uitvoeren van diverse testen en oefeningen.[69]

5.1.2 Nederlandse Cybersecuritystrategie[70]

Een van de doelen die zijn geformuleerd in de Nederlandse Cybersecuritystrategie 2022-2028 is dat organisaties in staat zijn om snel te kunnen reageren op cyberincidenten en daar ook snel van kunnen herstellen. Om dit doel te kunnen bereiken is in het bijbehorende actieplan[71] opgenomen dat het Ministerie van BZK er zorg voor draagt dat centrale en medeoverheden jaarlijks oefenen aan de hand van een gesimuleerde hackaanval. Hiernaast worden er gedurende het jaar ook diverse webinars georganiseerd waarbij publieke en private organisaties kennis delen.

5.1.3 Overheidsbreed Cyberprogramma[72]

Uit de Nederlandse Cybersecuritystrategie volgt het Overheidsbreed Cyberprogramma. De overheid heeft een grote verantwoordelijkheid voor het beveiligen van de gegevens van burgers en ondernemers. Om bestuurders, managers en medewerkers van overheidsinstellingen bewust te maken van digitale dreigingen en risico's is het Ministerie van BZK het Overheidsbreed Cyberprogramma gestart dat zich richt op het oefenen met realistische scenario's van cyberincidenten en het delen van kennis. In 2018 is een interbestuurlijke actie-agenda opgesteld om op het gebied van informatiebeveiliging alertheid, kennis en vaardigheden van bestuurders, managers en medewerkers te vergroten, onder andere door de introductie van de jaarlijkse Overheidsbrede Cyberoefening.

5.1.4 ISIDOOR[73]

ISIDOOR is een grootschalige cyberoefening, georganiseerd door het NCSC en de NCTV, die zich richt op een digitaal incident met impact voor vitale sectoren. Hierbij oefent de Rijksoverheid met publieke en private organisaties die een rol hebben in de reactie op een (dreigende) digitale crisis. Dit zijn organisaties binnen de vitale infrastructuur, maar ook veiligheidsregio's en organisaties uit het Landelijk Dekkend Stelsel. Tijdens ISIDOOR worden afspraken, structuren en processen uit het Landelijk Crisisplan Digitaal (LCP-Digitaal)[74] geoefend. Door te oefenen beoogt ISIDOOR bij te dragen aan een snellere en adequatere reactie van partijen wanneer zich een werkelijke digitale crisis voordoet. De derde ISIDOOR cyberoefening vond plaats in 2021 en telde meer dan 1500 deelnemers van 96 organisaties.

5.1.5 Keuzekaart Securitytesten Rijksoverheid[75]

In maart 2023 heeft het Ministerie van BZK een keuzekaart ontwikkeld die centrale en medeoverheden ondersteunt bij het kiezen van de juiste securitytest bij het gestelde testdoel. Gerelateerd aan deze keuzekaart is in dezelfde periode ook de Gereedschapskist Red-teaming[76] gepubliceerd. Deze biedt een raamwerk voor het uitvoeren van een Advanced Red Teaming (ART) of een meer complexe Threat Intelligence Based Ethical Red-teaming (TIBER) test. Hiernaast biedt de gereedschapskist ook inkooprichtlijnen voor een Red-teamingtest.

69 BIO versie 1, Ministerie van BZK, 2019. Zie de paragrafen 12.1 Bedieningsprocedures en verantwoordelijkheden; 12.3 Back-up; 14.2 Beveiliging in ontwikkelings- en ondersteunende processen; 17.1 Informatiebeveiligingscontinuïteit; en 18.2 Informatiebeveiligingsbeoordelingen.

70 https://open.overheid.nl/documenten/ronl-82f59d66894e136f786c3a34e62d1ce52d26b1c8/pdf

71 https://open.overheid.nl/documenten/ronl-c98affdac7fc3cb0d389bb4e0e18def898d09315/pdf

72 https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/oefenen-en-kennisdelen/overheidsbreed-cyberprogramma/

73 https://www.ncsc.nl/onderwerpen/isidoor

74 https://www.nctv.nl/documenten/publicaties/2022/12/23/landelijk-crisisplan-digitaal

75 https://www.digitaleoverheid.nl/wp-content/uploads/sites/8/2023/03/75856-BZK-Keuzekaart-securitytesten-Rijksoverheid_PDFUA.pdf

76 https://www.digitaleoverheid.nl/nieuws/gereedschapskist-red-teaming-vanaf-nu-online/

5.2 Provincies

5.2.1 Interprovinciale Digitale Agenda[77]

Provincies beheren onderdelen van de Nederlandse vitale infrastructuur zoals bruggen en sluizen en leveren digitale diensten aan ondernemers en burgers. Vanuit deze rol geven zij hoge prioriteit aan cyberweerbaarheid en werken provincies nauw samen om cyberdreigingen het hoofd te bieden. Binnen het programma Interprovinciale Digitale Agenda (IDA)[78] werken de provincies aan de oprichting van een eigen Informatieknooppunt Cyber Security, waarmee provincies onderdeel gaan uitmaken van het Landelijk Dekkend Stelsel en direct NCSC-informatie over cyberdreigingen kunnen gaan ontvangen. In dat kader werken alle provincies toe naar volledige implementatie van de BIO en compliance met de standaard ISO/IEC 27001 voor informatiebeveiliging. Deze aanpak sluit aan bij de door de Cyber Security Raad (CSR) geadviseerde integrale aanpak van en regie op cyberweerbaarheid.

5.2.2 Certificeerbaar voor ISO/IEC 27001[79]

Alle provincies streven ernaar om voor 2024 certificeerbaar te zijn voor de standaard ISO/IEC 27001. In 2018 hebben de provincies zich gecommitteerd aan de doelstelling om voor 2024 te voldoen aan het normenkader van de ISO/IEC 27001, waar ook testen en oefenen in het kader van informatiebeveiliging onderdeel van uit maakt. Door hierin gezamenlijk op te trekken willen provincies voorkomen dat zij ieder voor zich het wiel moeten uitvinden. Met de certificering willen provincies laten zien dat zij informatiebeveiliging op orde hebben, goed monitoren en daarmee het goede voorbeeld geven aan leveranciers aan wie zij hoge kwaliteitseisen stellen.

5.2.3 Project Troje[80]

De provincie Gelderland heeft in het kader van het Project Troje haar gemeenten een vrijwillige cyberweerbaarheidstest (nulmeting) aangeboden die werd uitgevoerd door een externe partij.[81] De deelnemende gemeenten doorliepen de nulmeting om in kaart te brengen hoe weerbaar ze zijn tegen cyberdreigingen. Na afloop van de nulmeting ontving iedere deelnemende gemeente een rapportage met verbeterpunten en een managementsamenvatting. De drie best scorende gemeenten kregen bovendien een diepgaandere vervolgtest aangeboden in de vorm van een Red-teaming.

5.2.4 Testen software en inkoopeisen[82]

Het Interprovinciaal Overleg (IPO) geeft in het position paper Online veiligheid en Cybersecurity (april 2022) aan dat zij gebruikte software periodiek laat testen door middel van ethical hacking. Hiernaast maken provincies gebruik van de Inkoopeisen Cybersecurity Overheid, de ICO-wizard. Hiermee kunnen vooraf passende beveiligingseisen worden bepaald die worden meegegeven bij een aanbesteding en aanschaf van software.

77 https://www.ipo.nl/media/ytxdvcjg/pp-online-veiligheid-en-cybersecurity.pdf
78 https://www.ipo.nl/thema-s/digitalisering/#:~:text=De%20Interprovinciale%20Agenda%2C%20IDA%2C%20wil,Samen%20doen%2C%20wat%20samen%20moet
79 https://www.bij12.nl/nieuws/provincies-bereiden-zich-voor-op-iso-27001-in-2023/
80 https://www.weerbaredigitaleoverheid.nl/visuele-notule/project-troje-hoe-vergroot-je-de-digitale-weerbaarheid-in-het-overheidsdomein/
81 https://media.gelderland.nl/Factsheet_Project_Troje_6c40692681.pdf
82 https://www.ipo.nl/media/ytxdvcjg/pp-online-veiligheid-en-cybersecurity.pdf

5.3 Gemeenten

5.3.1 Overleg cyberburgemeesters[83]

In maart 2021 heeft een groep van 17 burgemeesters zich georganiseerd in het overleg cyberburgemeesters. Het overleg cyberburgemeesters heeft als doel om kennis en ervaringen op het gebied van informatiebeveiliging uit te wisselen en gezamenlijk aandacht en middelen te genereren voor digitale veiligheidsvraagstukken op regionaal en lokaal niveau. Hierbij zetten zij zich onder andere in voor een betere voorbereiding op cyberincidenten en -crisis. Zij roepen dan ook op om meer te oefenen om zo de burgemeesters meer bekend te maken met digitale dreigingen.[84]

5.3.2 Cyberoefenpakket VNG / COT[85]

De Vereniging van Nederlandse Gemeenten (VNG) heeft in samenwerking met het Instituut voor Veiligheids- en Crisismanagement (COT) een pakket ontwikkeld met interactieve cyberoefeningen. In het pakket zijn drie oefenvarianten voorhanden die door gemeenten zelf, en indien gewenst met aansluiting van partners, kunnen worden uitgevoerd. De drie oefenvarianten richten zich op:

- Continuïteit van de organisatieprocessen in een oefening gericht op het crisisteam.
- Criminaliteit in een oefening gericht op de samenwerking tussen het crisisteam en de gezagsdriehoek (burgemeester, politie, OM).
- Maatschappelijke impact in een oefening gericht op de samenwerking tussen gemeente, gezagsdriehoek en regionaal operationeel team.

De oefenvarianten betreffen interactieve crisissimulaties, waarbij de deelnemers aan de hand van een scenario een crisis 'beleven' en daarop moeten reageren. Voor de uitvoering wordt gebruikgemaakt van de bestaande crisisstructuur en het crisismanagement van de gemeente en partners.

5.3.3 IBD 7 scenariokaarten[86]

In het kader van Bedrijfscontinuïteitsbeheer (BCM) heeft de informatiebeveiligingsdienst (IBD) van de VNG een zevental scenariokaarten ontwikkeld. De scenariokaarten beschrijven ieder een crisisscenario en zijn bedoeld om crisisteams te helpen in de reactie op een crisis en specifieke kenmerken van het type crisis te doorzien. De scenariokaarten kunnen ieder ook de basis vormen voor het oefenen van de reactie op een type cybercrisis. De zeven scenariokaarten richten zich op:[87]

1. Uitval gebouw.
2. Uitval door stroomstoring.
3. Uitval ICT.
4. Cybercrisis.
5. Uitval datacommunicatie.
6. Uitval telefonie.
7. Uitval personeel.

5.3.4 IBD-games en -producten[88] [89]

In de productencatalogus van de IBD zijn diverse digitale en fysieke games te vinden die gemeenten kunnen gebruiken als oefenmateriaal op het gebied van informatiebeveiliging en crisismanagement. Enkele voorbeelden van deze producten zijn een Crisisgame, een Privacy Pubquiz (incl. nieuwe editie 2023), een serious boardgame over informatiebeveiliging voor gemeenten genaamd 'Spion op je pad' en een serious game waarmee kan worden geoefend met de uitval van ICT en de gevolgen voor de interne organisatie.

Naast genoemde producten is de IBD ook bezig met het ontwikkelen van een IBD table top crisisoefening, een training voor CISO's en online cursussen voor lijnmanagers en proceseigenaren.[90]

5.3.5 Diverse games van gemeenten[91]

In de productencatalogus van de IBD zijn ook een aantal serious games opgenomen die zijn ontwikkeld door gemeenten en ter beschikking worden gesteld aan andere gemeenten. Deze games betreffen de iBewustzijn game (gemeenten Tiel, Culemborg en Geldermalsen), het grote datalekkenspel (Gemeente Nieuwegein) en Mobiele escaperooms (gemeenten Smallingerland en Versnellingsagenda Noordoost-Fryslân).

5.3.6 Hack The Gemeente

Verschillende gemeenten, waaronder Den Haag en Rotterdam, testen de informatiebeveiliging van hun systemen door het inzetten van ethische hackers. Zo krijgen ethische hackers in Hâck The Hague, dat sinds 2017 viermaal heeft plaatsgevonden, de kans om de ICT-systemen van de gemeente Den Haag en haar toeleveranciers onder de loep te nemen[92] en worden in Rotterdam, Hack 010, studenten van de IT-campus Rotterdam ingezet om systemen van de gemeente ethisch te hacken.

83 https://www.burgemeesters.nl/themas/openbare-orde-en-veiligheid/cyberburgemeesters/
84 https://vng.nl/artikelen/digitale-veiligheid-de-vlucht-van-de-cyberburgemeester
85 https://www.informatiebeveiligingsdienst.nl/project/cyberoefenpakket-vng-oefenscenarios-digitale-incidenten/
86 https://www.informatiebeveiligingsdienst.nl/product/scenariokaart-1-uitval-gebouw/
87 Voor de overige scenariokaarten zie https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/
88 https://www.informatiebeveiligingsdienst.nl/project/bewustwording/
89 https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/
90 https://www.informatiebeveiligingsdienst.nl/project/producten-in-ontwikkeling/
91 https://www.informatiebeveiligingsdienst.nl/project/bewustwording/
92 https://www.denhaag.nl/en/in-the-city/safety/hack-the-hague-1.htm

5.4 Waterschappen

5.4.1 Digitaliseringsberaad[93]

Bestuurders, (secretaris-)directeuren, Chief Information Officers (CIO's) en Chief Digital Officers (CDO's) van alle 21 waterschappen zijn vertegenwoordigd in het Digitaliseringsberaad. In het Digitaliseringsberaad wordt op strategisch niveau over digitaliseringsvraagstukken gesproken. Doel van het beraad is om waterschappen in staat te stellen om van elkaar te leren, om het delen van kennis en ervaringen te vereenvoudigen, om de bestuurlijk-ambtelijke dialoog te faciliteren en om de digitale transformatie bij de waterschappen te stimuleren. Het Digitaliseringsberaad stimuleert samenwerking, kennisdeling en oefening met ketenpartners om risico's in de keten te identificeren en een geharmoniseerde aanpak mogelijk te maken.[94]

5.4.2 Meerjarenplan digitale informatie-huishouding[95]

In juli 2020 heeft de Unie van Waterschappen (UvW) in samenwerking met experts vanuit de waterschappen een meerjarenplan opgesteld om de digitale informatiehuishouding duurzaam en toegankelijk te maken en te houden. Directe aanleiding hiervoor was het wetgevingstraject rondom de Wet open overheid (Woo) en het inzicht dat de informatie-huishouding van de waterschappen gefragmenteerd was ingericht. Op basis van een enquête heeft de themagroep Diwanet een nulmeting onder de waterschappen uitgevoerd om vast te stellen in hoeverre zij voldoen aan de Archiefwet 1995.

Hiernaast is vanuit het Waterschapshuis, de regie- en uitvoeringsorganisatie voor de 21 waterschappen op het gebied van ICT, een meerjarenprogramma Informatieveiligheid en Privacy (IV&P) 2020-2024 ontwikkeld.[96] Dit programma ondersteunt de waterschappen om te voldoen aan de BIO. Alle waterschappen en Rijkswaterstaat hebben zich in het meerjarenprogramma IV&P 2020-2024 ten doel gesteld om voor 2025 over de gehele linie (mens, proces, technologie en assets) aantoonbaar een procesvolwassenheid van niveau 4 te behalen.[97] In het kader van IV&P 2020-2024 stimuleert en faciliteert het Waterschapshuis samenwerking, kennisdeling en oefeningen om de digitale weerbaarheid te vergroten.[98]

5.4.3 Computer Emergency Response Team – Watermanagement (CERT-WM)[99]

In 2016 hebben de 21 waterschappen, in samenwerking met Rijkswaterstaat, CERT-WM opgezet. Het doel van CERT-WM is om te zorgen dat de waterschappen voldoende weerbaar zijn tegen potentieel maatschappij-ontwrichtende cyberincidenten. Hiertoe werkt CERT-WM aan het verbeteren van de informatiebeveiliging in de waterketen. Gedetacheerde medewerkers van de waterschappen werken voor CERT-WM vanuit het Security Operations Centre (SOC) van Rijkswaterstaat. Onderdeel van de dienstverlening is dat waterschappen software door CERT-WM kunnen laten testen op malware of ander ongewenst gedrag.

5.4.4 CyberSecurity ImplementatieRichtlijn (CSIR)[100]

De CSIR is een implementatierichtlijn voor de BIO en de IEC 62443-normen. De CSIR helpt de waterschappen om deze normen te implementeren door het geven van praktische handvatten voor zowel medewerkers die werken aan het beveiligen van de administratieve automatisering (conform de BIO) als medewerkers die werken aan het beveiligen van de procesautomatisering[101] (conform de IEC 62443). De CSIR zorgt ervoor dat de informatiebeveiliging van de administratieve automatisering en die van de procesautomatisering beide en in samenhang op een geschikt niveau kunnen komen. Hiernaast draagt CSIR bij aan een betere onderlinge vergelijkbaarheid van de informatiebeveiliging bij organisaties binnen de keten, waardoor uitslagen van toetsing en audits beter met elkaar kunnen worden vergeleken en kennisdeling binnen de sector wordt vereenvoudigd.

5.4.5 Leer-oefentraject digitale weerbaarheid[102]

Voor de zeven aangesloten waterschappen organiseert het Platform Crisisbeheersing Waterschappen Midden-Nederland (PCWMN) een leer- en oefentraject op het gebied van digitale weerbaarheid. Sinds 2020 organiseert PCWMN voor deelnemende organisaties webinars, trainingen en oefeningen die gericht zijn op de reactie op een cybercrisis. Het doel is om de samenwerking tussen de waterschappen en crisispartners (zoals de veiligheidsregio) te verbeteren, maar ook de bewustwording ten aanzien van digitale kwetsbaarheid te vergroten.

93 https://unievanwaterschappen.nl/themas/digitalisering/
94 https://www.hetwaterschapshuis.nl/veilige-data
95 https://unievanwaterschappen.nl/wp-content/uploads/2023/05/Meerjarenplan-digitale-informatiehuishouding-waterschappen-juli-2020.pdf
96 https://www.hetwaterschapshuis.nl/veilige-data
97 https://www.hetwaterschapshuis.nl/veilige-data
98 https://www.hetwaterschapshuis.nl/veilige-data
99 https://www.cert-wm.nl/over
100 https://www.cert-wm.nl/csir
101 Procesautomatisering wordt ook wel aangeduid als Operationele Technologie (OT) of Industrial Control Systems (ICS).
102 https://www.digitaleoverheid.nl/nieuws/geen-traditionele-hoogwatercrisis-maar-cybercrisis/

6 Conclusies

In deze literatuurstudie worden de volgende vijf onderzoeksvragen beantwoord:

1. **Wat is bekend over het gebruik van testen en oefenen door medeoverheden in Nederland en buurlanden?**
   a. **Techniek, middelen, frequentie**.
   b. **Wat gebeurt er met de resultaten van testen en oefenen?**
   c. **Zijn er verschillen tussen provincies, gemeenten en waterschappen?**

   De wetenschappelijke en niet-wetenschappelijk literatuur biedt weinig tot geen inzicht in het gebruik van testen en oefenen in het kader van informatiebeveiliging door medeoverheden. Dit geldt zowel voor Nederland als voor buurlanden. Met dit onderzoek zijn wel enkele goede voorbeelden opgehaald over initiatieven en ontwikkelingen die het gebruik van testen en oefenen in het kader van informatiebeveiliging door provincies, gemeenten en waterschappen stimuleren en ondersteunen. Dit geeft echter geen inzicht in hoe de medeoverheden in eigen huis gebruikmaken van testen en oefenen als onderdeel van de informatiebeveiliging, met welke frequentie zij dit doen, welke technieken zij daarvoor inzetten of hoe zij gebruikmaken van de resultaten van testen en oefenen. Op basis van dit onderzoek kunnen daarom ook geen uitspraken gedaan worden over verschillen tussen provincies, gemeenten en waterschappen.

2. **Welke typen van testen en oefenen kunnen worden onderscheiden en van welke rapportagevormen wordt gebruikgemaakt?**
   Bij de inzet van testen op het gebied van informatiebeveiliging kan onderscheid worden gemaakt tussen vier typen testen, die kunnen variëren in reikwijdte (componentgericht of omvattend) en toepassingsdomein (mensen, techniek, of processen):
   1. **Kennis/vaardigheden testen**, gericht op het verifiëren van het kennis- of vaardighedenniveau van sollicitanten, medewerkers met een specifiek functieprofiel, of van groepen medewerkers.
   2. **Reviews**, gericht op het detecteren van zwakke plekken in techniek of processen.
   3. **Technische testen** om kwetsbaarheden in software en hardware in kaart te brengen en om functieherstel na cyberincidenten te verifiëren.
   4. **Procestesten**, gericht op het in kaart brengen van de cyberweerbaarheid, de uitvoerbaarheid, of de geschiktheid van processen in de organisatie.

Tabel 2.1 Overzicht van typen testen per toepassingsdomein

Toepassingsdomein	Typen testen
Mensen	**Kennis/vaardigheidstest:** Kwalificaties, Risicobewustzijn, Bekendheid met procedures, Toetsen en examens
Techniek	**Review**: Code reviews, Kwetsbaarhedenscans **Technische test**: Acceptatietest, Functietest, Penetratietest, Back-up- en recovery-test
Processen	**Review**: Beleidsreviews, Audits **Procestest:** Testen van uitwijk- en herstelplan, Volwassenheidsmeting, Red team/Blue team

Bij de inzet van oefenen op het gebied van informatiebeveiliging kan onderscheid worden gemaakt tussen drie typen oefeningen:

1. Leeroefeningen, waarbij deelnemers zich – los van scenario's – individueel of in groepen richten op het ontwikkelen van kennis en vaardigheden.
2. Procesoefeningen met gebruik van simulatie, gericht op het oefenen van een taak of proces in een omgeving die een nabootsing vormt van de werksituatie van de organisatie. Hierbij kunnen vereenvoudigingen in de simulatie worden doorgevoerd om niet alle complexiteit van de werksituatie tegelijk in het oefenen te betrekken.
3. Procesoefeningen real-life, gericht op het oefenen van een taak of proces in de actuele werksituatie. Er wordt niet geacteerd en iedere deelnemer voert taken uit vanuit de eigen rol, zoals in de gangbare werksituatie het geval zou zijn.

Net als testen kunnen ook oefeningen variëren in reikwijdte (componentgericht of omvattend). Anders dan bij testen is oefenen in principe niet toepasbaar op het technische toepassingsdomein. Oefeningen voor de domeinen mensen en processen kunnen wel gericht zijn op de omgang met de techniek. Denk bijvoorbeeld aan het oefenen van een back-up- en recoveryprocedure in het domein processen.

Tabel 3.1 Overzicht van typen oefening per toepassingsdomein

Toepassingsdomein	Typen oefeningen
Mensen	**Individuele Leeroefeningen:** Workshop, praktijkoefeningen (denk aan: Capture the Flag- of Hack The Box-games, maar ook oefenen met tools en technieken om in te breken op servers en netwerken en phishing- en social engineering-oefeningen), training on the job **Leeroefeningen voor groepen:** groepsdiscussie
Techniek	Niet van toepassing
Processen	**Procesoefeningen Simulatie**: Desk check of Walkthrough, Rollenspel, Managementgame, Tabletop-oefening, Distributed tabletop-oefening, CPX **Procesoefeningen Real-life:** Comms check, Oproepoefening, Red Team/Blue Team

3. **Welke goede praktische voorbeelden zijn te vinden?**
   In de analyse van de praktijkgerichte literatuur zijn diverse goede voorbeelden van ontwikkelingen en initiatieven aan het licht gekomen die het gebruik van testen en oefenen faciliteren. Grofweg zijn deze goede voorbeelden op het niveau van overheidsbreed, provincie, gemeente, of waterschap in te delen in drie categorieën:
   1. **Beschikbaar stellen van hulpmiddelen**
      Denk hierbij aan de landelijke keuzekaart Securitytesten Rijksoverheid die is ontwikkeld om overheidsorganisatie te ondersteunen bij de keuze van de juiste securitytest. Andere voorbeelden zijn de baseline die is ontwikkeld voor en door de waterschappen, het aanbieden van periodieke testen voor software en een ruim online aanbod van scenario's en spellen waarmee overheidsorganisaties eigen testen of oefeningen kunnen organiseren en uitvoeren. Het aanbod van scenario's en spellen lijkt vooral te zijn toegespitst op gemeenten. Mogelijk speelt de relatief grote omvang van de groep gemeenten in vergelijking met provincies en waterschappen hierbij een rol.
   2. **Samenwerking op bestuurlijk niveau binnen het eigen domein**
      Landelijk kan bij deze categorie worden gedacht aan het Overheidsbreed Cyberprogramma en de Nederlandse Cybersecuritystrategie. Voor de sectoren van de medeoverheden omvatten deze initiatieven zoals de inrichting van digitaliseringsberaden, het opstellen van digitale agenda's, bestuurlijk commitment aan certificeerbaarheid of aan het behalen van een zeker volwassenheidsniveau in meerjarenplannen op het gebied van informatiebeveiliging, of het inrichtingen van een overleg van cyberburgemeesters die als ambassadeurs kunnen dienen voor het gebruik van testen en oefenen.
   3. **Samenwerking in de praktijk**
      Een voorbeeld is het Project Troje waarbij de informatiebeveiliging bij gemeenten uit de provincie Gelderland wordt getest in een nulmeting en later drie gemeenten deelnemen aan een Red-teaming-oefening. Andere sectorspecifieke voorbeelden zijn het leer- en oefentraject Digitale Weerbaarheid waaraan waterschappen in de regio Midden-Nederland deelnemen en lokale hack-de-gemeente-oefeningen in samenwerking met onderwijs- en kennisinstellingen. Een sectoroverstijgend voorbeeld is de landelijke cyberoefening ISIDOOR die wordt georganiseerd door NCSC en NCTV.

      Al met al kan worden geconcludeerd dat er binnen de sectoren ontwikkelingen zijn te vinden die de samenwerking in de praktijk met betrekking tot het gebruik van testen en oefenen kunnen stimuleren of soms al ondersteunen. De waterschappen lijken hierin voorop te lopen. Sectoroverstijgende ontwikkelingen en initiatieven op het gebied van testen en oefenen zijn op dit moment nog beperkt, zeker als het gaat om de praktische invulling ervan.

4. **Wat zeggen de standaarden over de uitvoering van, de eisen aan en de randvoorwaarden voor testen en oefenen, en zijn hierbij verschillen tussen provincies, gemeenten en waterschappen?**
   In de geraadpleegde literatuur zijn enkele randvoorwaarden en richtlijnen voor het uitvoeren van testen en oefenen aan bod gekomen. Een indicatief overzicht hiervan voor testen omvat:
   - Testen dienen te worden uitgevoerd in een niet-operationele omgeving die zoveel mogelijk overeenkomt met de productieomgeving. Dit om verstoringen te voorkomen.
   - Voorafgaand aan het testen is een testplan nodig. Hierin zijn vastgelegd:
     - de testdoelen;
     - de activiteiten die moeten worden uitgevoerd om die doelen te behalen;
     - het criterium of de criteria waarmee kan worden vastgesteld of een test is geslaagd;
     - welke verdere acties nodig zijn naar gelang de testuitslag bijvoorbeeld het informeren van management of het treffen van compenserende maatregelen.
   - Testen moeten worden uitgevoerd door onafhankelijke competente en bevoegde personen.

Een indicatief overzicht van randvoorwaarden en richtlijnen voor het uitvoeren van oefeningen omvat:

- Voorafgaand aan het oefenen is een oefenplan nodig waarin het doel van de oefening, scenario's en eventuele informatie die tijdens de oefening kan worden ingebracht is beschreven.
- Rollen en verantwoordelijkheden voor het uitvoeren van plannen en procedures moeten vastgesteld en duidelijk gecommuniceerd zijn.
- Betrokken medewerkers moeten over een voldoende niveau van kennis en vaardigheden beschikken.
- Adequate begeleiding is nodig bij het uitvoeren van de oefening.
- Alle deelnemers weten dat het scenario dat wordt gebruikt een oefening is en geen werkelijke gebeurtenis en ze kennen het doel van de oefening.
- Uitvoeren van de oefening in een gecontroleerde omgeving om te voorkomen dat effecten van de oefening kunnen doorwerken in de operationele praktijk.
- Debriefen van de deelnemers en ophalen feedback naar aanleiding van de oefening.
- Opstellen van een rapportage van de oefening voor management en eventueel externe stakeholders.

5. **Wat is bestuurlijk nodig om het thema 'testen en oefenen' goed op de agenda te krijgen en welk empirisch onderzoek is daarnaar gedaan?**
   Er is geen wetenschappelijke of niet-wetenschappelijke literatuur gevonden die zich specifiek richt op bestuurlijke inbedding of agendering van testen en oefenen. Testen en oefenen vormen essentiële onderdelen van de inrichting van de informatiebeveiliging en zijn geen op zichzelf staande onderwerpen. De bestuurlijke inbedding van testen en oefenen zal dan ook onderdeel zijn van de bestuurlijke inbedding van informatiebeveiliging als geheel. Hoewel de literatuur ervan uitgaat dat het topmanagement van een organisatie informatiebeveiliging, en ook het daarvoor benodigde testen en oefenen, zelf op de agenda zet en de realisatie ervan borgt, blijkt de praktijk weerbarstig.

Verbetering van deze situatie kan vanuit de organisaties zelf komen van brainstorms over informatiebeveiliging van bestuurders met bijvoorbeeld CIO's en CISO's, en onder andere betere communicatie over informatiebeveiligingsdreigingen, -risico's en -incidenten door informatiebeveiligers.

Bij organisaties waar de strategische top het onderwerp informatiebeveiliging desondanks nog niet goed op de agenda zet, kunnen toezichthouders, accountants en auditors druk op het management uitoefenen door om nadere onderbouwing van de inrichting van informatiebeveiliging te vragen bij inspecties, goedkeuring van financiële verslagen of auditrapporten.

De motivatie voor informatiebeveiliging kan ook worden versterkt door de strategische top van verwante organisaties die zelf op dit gebied al verder gevorderd zijn. Bestuurders van andere organisaties kunnen dan dienen als ambassadeurs. Zij kunnen testen en oefenen in het kader van informatiebeveiliging bestuurlijk agenderen en de bestuurders die nog niet zover zijn proberen te overtuigen van het belang ervan.

Adres- en contactgegevens

Johanna Westerdijkplein 75
2521 EN Den Haag

dehaagsehogeschool.nl