Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Onderzoek toepasbaarheid (TIBER-NL) testen binnen Rijksoverheid en plan van aanpak

n.a.v. Motie van het lid Rajkowski c.s. over onderzoek naar het toepassen van TIBER-NL binnen de organisatie van de rijksoverheid (kenmerk: 35925 VII, nr. 16)

Status definitief

Colofon

DGOO/CIO-Rijk

Den Haag

Contactpersoon IBenP

Datum 16 maart 2022
Versie 1.0 definitief
Opdrachtgever CIO Rijk/CISO Rijk,
Auteur IBenP
Projectnummer Dossiernr. Digidoc: 2022-0000022418

Inhoud

Inleiding en leeswijzer

Voor u ligt het rapport naar aanleiding van Motie (35925 VII, nr. 16) over onderzoek naar het toepassen van TIBER-NL binnen de organisatie van de Rijksoverheid en de gerelateerde toezegging aan de Kamer[1]. Dit rapport geeft het onderzoek naar aanleiding van de motie weer, resultaten daarvan en het plan van aanpak om de resultaten duurzaam te borgen. De resultaten en het plan van aanpak zijn tot stand gekomen in samenwerking met de CISO-raad en andere stakeholders en het plan van aanpak is vastgesteld in het CIO-beraad.

Leeswijzer

Het rapport begint met de managementsamenvatting, waarin de reactie op de vragen en toezegging, de ambitie van de Rijksoverheid en het plan van aanpak daarnaar toe zijn opgenomen. Daaronder is bondig uitgelegd wat het doel en toepassingsgebied was van het onderzoek en hoe de aanpak is geweest die tot de antwoorden, de geformuleerde ambitie en het stappenplan heeft geleid. Tot slot vindt u in de bijlagen de tekst van de motie en toezegging en een overzicht van de directe betrokkenen bij het onderzoek en het plan van aanpak .

[1] Kamerbrief dd 28 oktober 2021: Schriftelijke antwoorden op vragen gesteld tijdens de eerste termijn van de begrotingsbehandeling van Binnenlandse Zaken en Koninkrijksrelaties (hoofdstuk VII), het gemeentefonds en het provinciefonds op 27 oktober 2021.

1 Samenvatting, antwoord, plan van aanpak

1.1 Samenvatting

Het onderzoek "Toepasbaarheid (TIBER-NL)[2] testen binnen Rijksoverheid en plan van aanpak" is in een samenwerking tussen CIO-rijk en departementale CISO's uitgevoerd om:

1. Antwoord te geven op Motie 35925 VII, nr. 16: of de TIBER-NL-testen dan wel soortgelijke testen ook binnen de organisatie van de rijksoverheid toegepast kunnen worden, de opgedane ervaringen en daaruit getrokken lessen Rijksbreed te delen.
2. In het kader van de I-strategie Rijk 2021-2025[3]: een aanpak te maken gericht op het realiseren van een Rijksbreed testprogramma om beter digitaal weerbaar worden en blijven. Dit is tevens de reactie op de gerelateerde toezegging aan de Kamer[4].

Het onderzoek is uitgevoerd middels documentstudie van onder andere de documentatie die de Nederlandsche bank (DNB) voor TIBER-NL beschikbaar heeft gesteld. Daarnaast is uitvraag gedaan en zijn gesprekken gevoerd met de departementen en gesprekken met andere stakeholders.

De vraagstelling in de motie kan worden beantwoord (zie 1.2) en er is een plan van aanpak ontwikkeld door in 3 sporen stapsgewijs (zie 1.3) een ambitie te realiseren om de feitelijke veiligheid te verhogen. Deze sporen zijn:

We hebben een gezamenlijke jaarlijkse testkalender (met o.a. red-teamingtesten).

In een veilige omgeving delen we kennis en leren we van elkaar.

We geven opvolging aan bevindingen en worden steeds beter (weerbaar).

1.2 Reactie op de motie en toezegging

De digitale weerbaarheid van de Rijksoverheid is gediend bij op meer structurele basis testen van de weerbaarheid van organisaties, zodat die gericht verbeterd kan worden. Het delen van kennis uit dergelijke testen binnen de Rijksoverheid zal de weerbaarheid ook verbeteren. Onderdelen van het TIBER-NL programma die ook toepasbaar zijn bij de Rijksoverheid zijn dan o.a.:

- realistische scenario's op basis van inlichtingen vormen de testbasis;
- geavanceerde ethische hackteams voeren de test uit;
- coördinatie van de test door een white team met voldoende mandaat in de organisatie om de test te kunnen doorzetten of onderbreken;
- gericht op verbetering in een hele sector, door het vertrouwelijk delen van ervaringen zodat ervaring bij één organisatie leidt tot verbeteringen bij een grotere groep;
- vrijwillige deelname van organisaties.

---

[2] TIBER staat voor Threat Intelligence Based Ethical Red-teaming. Binnen dit programma werkt de financiële sector samen om beter bestand te zijn tegen cyberaanvallen. Het programma TIBER-NL wordt geleid door het TIBER Cyber Team van De Nederlandsche Bank (DNB). Financiële instellingen testen hoe weerbaar ze zijn tegen geavanceerde cyberaanvallen. Dit gebeurt met testaanvallen, die zijn gebaseerd op realistische dreiging.

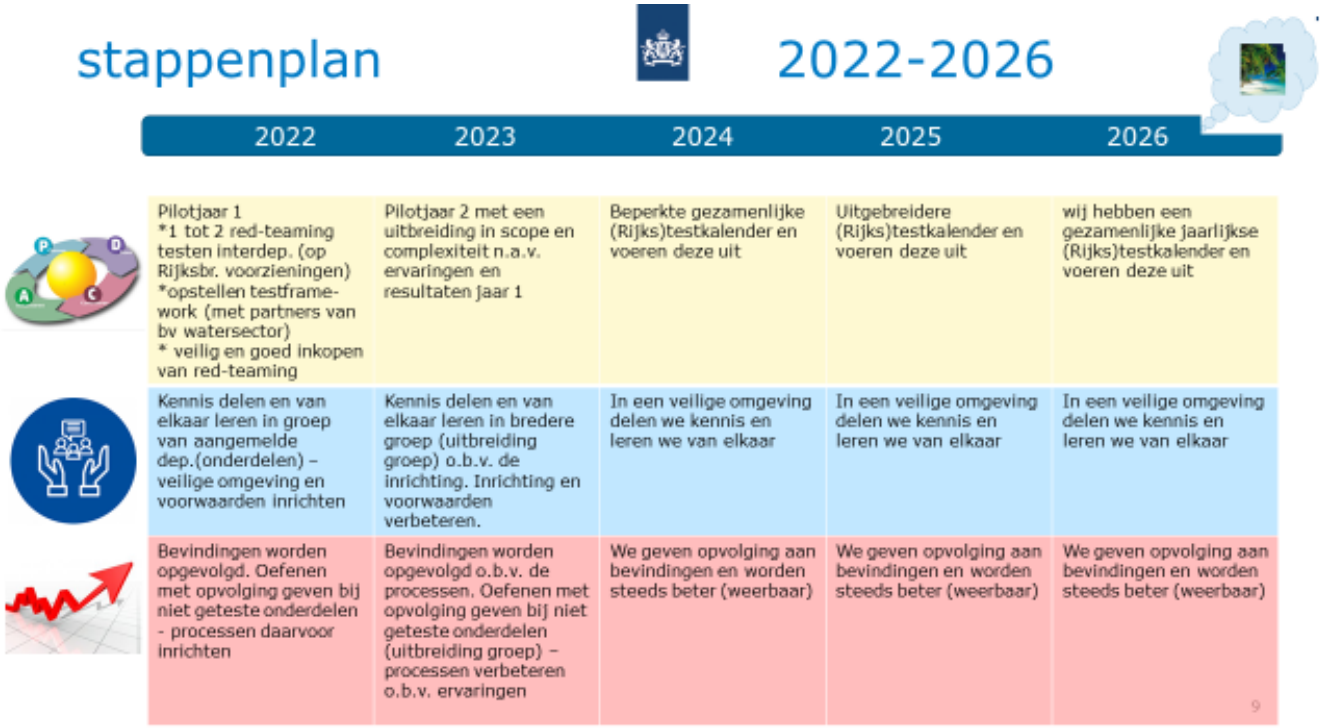
[3] I-strategie Rijk I-strategie Rijk 2021-2025 - Digitale Overheid

[4] Kamerbrief dd 28 oktober 2021: Schriftelijke antwoorden op vragen gesteld tijdens de eerste termijn van de begrotingsbehandeling van Binnenlandse Zaken en Koninkrijksrelaties (hoofdstuk VII), het gemeentefonds en het provinciefonds op 27 oktober 2021.

Red-teaming en andere testen worden al bij onderdelen van de Rijksoverheid toegepast. Hierbij wordt in een aantal gevallen ook de TIBER-NL aanpak gehanteerd. Het onderzoek heeft zich daarom vooral gericht op het structureel borgen van dergelijke testen als resultaat van de I-strategie Rijk. Onderdeel hiervan is het delen van resultaten, zoals par. 1.1. weergegeven. De randvoorwaarden hiervoor zijn opgenomen onder 1.4 bullet 3.

1.3 Plan van aanpak,

Op basis van het onderzoek en de conclusies daaruit is een plan van aanpak[5] ontwikkeld voor de periode 2022 – 2026 om te komen tot die structurele basis voor testen en het delen van kennis over de resultaten. In het plan van aanpak is het volgende stappenplan opgenomen:



1.4 Randvoorwaarden, advies

Om te komen tot de structurele basis voor testen, zijn een aantal kritische succesfactoren, randvoorwaarden die ingevuld moeten worden om de ambitie te kunnen realiseren. Het advies is om te zorgen dat deze blijvend zijn ingevuld bij ieder departement door samenwerking tussen bestuur, CIO's en CISO's en binnen de realisatie van de I-strategie Rijk.
De randvoorwaarden zijn onderdeel van de het plan van aanpak.
De belangrijkste randvoorwaarden zijn:
1/ Bestuurlijk commitment

- De departements- en organisatieleiding committeert zich aan en investeert in de testen en het opvolging geven aan bevindingen, is betrokken en stuurt op volwassenheid van het verbeterproces.
- Accepteert dat er in eerste periode (jaren) mogelijk met regelmaat (ernstige) bevindingen naar boven komen en draagt uit dat dit

[5] Plan van aanpak Tiber red-teaming Rijk

een logische en noodzakelijke fase is om de weerbaarheid structureel te verbeteren..

2/ Voldoende capaciteit en (financiële) middelen om:
- Bij de departementen en ICT dienstverleners testen te kunnen uitvoeren.
- Oefeningen en testen te begeleiden en te ondersteunen.
- Geschikte (externe) partijen te selecteren die oefeningen en testen kunnen voeren bij de departementen en ICT dienstverleners.
- In de (IT) uitvoering bevindingen op te kunnen lossen (niet alleen correctie/incidenteel (eenmalig), maar ook corrigerend/structureel (gericht op het voorkomen van herhaling).

3/ Invullen van de randvoorwaarden voor veilig kennis delen (uit 1.2):
- Beschikbaar zijn van een vertrouwde omgeving (fysiek, digitaal en sociaal).
- Herkenbaarheid/herbruikbaarheid van bevindingen in andere omgevingen dan waarop de test direct betrekking had. (dit betekent ook dat de meest gevoelige specifieke details niet worden gedeeld).

2 Doel en toepassingsgebied

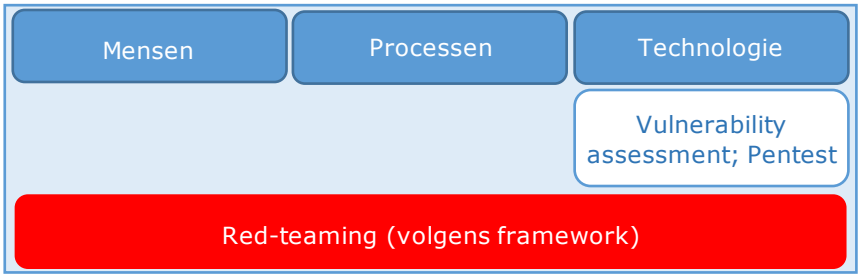
2.1 Doel

het doel van het onderzoek is:
1/ invulling te geven aan de onderzoeksvraag van Motie 35925 VII, nr. 16: verzoekt de regering na te gaan of de TIBER-NL testen dan wel soortgelijke testen ook binnen de organisatie van de Rijksoverheid toegepast kunnen worden, de opgedane ervaringen en daaruit getrokken lessen Rijksbreed te delen, en de Kamer daarover te informeren voor 1 april 2022.
2/ Bijdragen aan de invulling van een van weerbaarheidsdoelstellingen uit I-strategie Rijk 2021-2025: Ontwikkelen en doen uitvoeren van een Rijksbreed testprogramma gericht op het beter digitaal weerbaar worden en blijven van het Rijk.

2.2 Toepassingsgebied en definities

Organisatorisch toepassingsgebied:
Het onderzoek is gericht op de Rijksoverheid: de ministeries en de daaronder ressorterende dienstonderdelen.

Inhoudelijk toepassingsgebied:
Technische testen die tot doel hebben de feitelijke weerbaarheid tegen (digitale) aanvallen te verhogen. Er zijn verschillende soorten technische testen met verschillende reikwijdte en diepgang. De keuze van het meest geschikte type test is afhankelijk van met name de te testen omgeving en (volwassenheid van) de betrokken organisatie(s)



Figuur: reikwijdte van divers typen technische testen[6]

1/ Kwetsbaarhedenstest (vulnerability assessment) en pentest.

- Een **vulnerability assessment** is een door tools ondersteunde handmatige controle waarbij men zwakke plekken in een systeem opspoort.
- Een **pentest** (penetration test) is een technisch onderzoek waarbij wordt geprobeerd om zo diep mogelijk het systeem binnen te dringen door middel van kwetsbaarheden en zwakheden in de configuratie.

2/ Red-teaming

Een **red-teamingtest** is een vorm van aanvalssimulatie. Het team dat in deze simulatie de aanvallende partij speelt probeert de organisatie zo realistisch mogelijk aan te vallen. Dit gebeurt aan de hand van aanvalsscenario's die kunnen worden opgesteld op basis van actuele dreigingsinformatie.
Er is sprake van een aanvallend team (red-team) een verdedigend team (blue team). Daarnaast is er ook een team dat de oefening coördineert (white team). Een actueel dreigingsscenario wordt beoefend er zijn meerdere varianten mogelijk passend bij budget en volwassenheid van de organisatie (een bepaalde mate van volwassenheid is vereist).

- Er wordt uitgegaan van scenario's, gericht op het beoefenen van maatregelen van de organisatie (blue team)
- Afhankelijk van het budget en beschikbare tijd keuze om te gaan voor volledig scenario of een gegeven startpositie met bepaalde toegang.
- Keuze om oefening wel of niet vooraf bekend te maken bij de betrokken (IT) organisatie.
- Keuze om wel of niet te werken met externe begeleiding.

3/ Red-teaming volgens een framework

Het Threat Intelligence Based Ethical **Red-teaming** (TIBER) **framework** is oorspronkelijk ontwikkeld voor organisaties in de financiële sector. Op dit moment wordt het framework in Nederland ingezet voor de financiële kerninfrastructuur en in de pensioen en verzekeraarssector. Een TIBER test vindt in Nederland altijd plaats onder begeleiding van het TIBER Cyber Team (TCT) van DNB (De Nederlandsche Bank).
TIBER staat bekend als een betrouwbare maar stevige test.
We gaan nu bij dit onderzoek niet uit van een officiële TIBER test maar wel de zwaarte/complexiteit ervan, aanpak conform het TIBER framework.

- Het is te beschouwen als de zwaarste variant van red-teaming, waarbij kritische systemen getest worden in de operationele omgeving. Deze variant vraagt een volwassen organisatie.
- Er wordt uitgegaan van 2 scenario's (op basis van dreigingen) en een 3de scenario (scenario X, op basis van een toekomstperspectief), gericht om vanuit een reëel aanvalsscenario de weerbaarheid van de organisatie (blue team) te testen.
- Volledig scenario inclusief purple teaming na afronding van de feitelijke test. Hierbij worden red- en blue team samengevoegd.
- Oefening is niet vooraf bekend bij de betrokken (IT) organisatie.
- Kostbaar en (arbeids)intensief; er is altijd een externe partij betrokken bij opgezet en uitvoering. De test wordt begeleid door een TIBER Cyber Team (TCT).

3 Aanpak van het onderzoek

[6] Afgeleid van CIP Whitepaper: Red-teaming in de praktijk, oktober 2021

Hieronder staat beschreven hoe het onderzoek in fasen is aangepakt en het plan van aanpak om de ambitie te realiseren tot stand is gekomen gedurende de periode [november 2021] tot en met maart 2022.

3.1 Fase 1 voorbereiding

Om komen tot gedragen onderzoeksresultaten en plan van aanpak zijn volgende randvoorwaarden ingevuld:

1. Organisatorisch (bemensing):
   Een werkgroep is ingericht bestaande uit departementale CISO's (chief information security officers) en adviseurs van CIO (chief information officer) Rijk, met onderzoeksleider vanuit CIO rijk.
   Voor het plan van aanpak (opvolging van de resultaten) wordt afgestemd met de CISO-raad en CTO-raad (chief technology officer).
2. Fasering:
   Het onderzoek is gepland en uitgevoerd in nov en december, met een uitloper naar januari. Voor het vaststellen plan van aanpak geldt de periode januari-maart 2022.
3. Inhoud van het onderzoek is uitgevoerd in 3 sporen, middels een vragenlijst aan de CISO's (november) en verdiepende gesprekken op onderdelen (januari) en op basis van literatuur.[7][8][9]
   - 1/ Testen
     kwetsbaarhedenscanning/pentesten; red-teaming; conform TIBER
     Wat doen we al – hoe willen we ontwikkelen naar de toekomst en wat betekent dat?
   - 2/ Kennis en bevindingen delen
     Wat doen we al – wat zijn de randvoorwaarden (vertrouwen etc.) en wat hebben we nog nodig?
   - 3/ Opvolging van bevindingen
     Hoe zit het met de verbeterprocessen – wat is de huidige volwassenheid en (wat) moeten we nog verder ontwikkelen verbeteren?

3.2 Fase 2 Uitvoeren onderzoek

Het uitvoeren van het onderzoek kende de volgende stappen.

- Een inventarisatie bij de departementen middels vragen om grofmazig inzicht te krijgen in:
  * wat men nu al aan testen doet;
  * de ambitie van het departement op het vlak van testen;
  * 'capabilities' op het vlak van de opvolging;
  * bereidheid/mogelijkheid om kennis over resultaten te delen.
  De vragen zijn 15-11-2021 verstuurd uit met een reactietermijn van 2 weken. Op 7 december zijn de resultaten geanalyseerd in de werkgroep.
- Gesprek(ken) met TCT van DNB en een deelnemende organisatie over de verschillen/overeenkomsten tussen de financiële sector en het Rijk, do's en don'ts i.v.m. ambitie voor het Rijk.
- Gesprekken met stakeholders waar vergelijkbare trajecten worden geïnitieerd.

3.3 Fase 3 Rapportage, plan van aanpak

Om vanuit de resultaten van het onderzoek naar een gedragen plan van aanpak te komen, zijn de volgende activiteiten uitgevoerd:

- De ambitie is beschreven en getoetst bij de werkgroep, besproken met stakeholders en de opdrachtgever
- De resultaten van de uitgezette vragen zijn geanalyseerd en daaruit conclusies getrokken om te komen tot een plan van aanpak en een realistisch stappenplan.

---

[7] Whitepaper Securitytesten | Whitepaper | Nationaal Cyber Security Centrum (ncsc.nl)
[8] TIBER: samen tegen cybercrime (dnb.nl); link naar TIBER-NL documenten
[9] OCW_Whitepaper_Red-Teaming-in-de-praktijk_v1.3.pdf (digitaleoverheid.nl)

- Een aantal verdiepende gesprekken heeft nadere verheldering gegeven op het concept stappenplan en concretisering voor 2022.
- Het concept plan van aanpak is ter toetsing en advies voorgelegd aan de CISO-raad en de CTO-raad (februari 2022) en ter vaststelling in het CIO-beraad (maart 2022).

3.4 Fase 4 Nazorgfase

Het onderzoek en alle te archiveren gegevens zijn opgeslagen in het archiefsysteem Digidoc De uitvoering van het plan van aanpak is onderdeel van de realisatie van de I-strategie Rijk; Het CIO-beraad heeft "red-teaming" tot één van hun 5 focuspunten voor 2022 bestempeld. Voor het uitvoeren van een red-teaming test in 2022 op een Rijksbrede voorziening is een begrotingspost opgenomen.

4 Resultaten

Het onderzoek heeft geleid tot conclusie dat red-teaming (conform een framework) als TIBER toepasbaar is bij de Rijksoverheid. Om dit structureel te borgen als resultaat van de I-strategie is een plan van aanpak ontwikkeld zoals benoemd onder 1.3.. Hieronder staan de hoofdpunten uit het onderzoek en plan van aanpak, alsmede een aantal aandachtpunten, kritische succesvoorwaarden.

4.1 Ambitie in 3 sporen

4.2 De huidige situatie

De IST situatie – resultaten status departementen

(nav uitvraag- 11 van de 12 departementen hebben gereageerd)

- >80% heeft of wil een formeel departementaal testplan
- pentesten worden uitgevoerd maar nog niet overal structureel - komt overeen met rode draden ADR (verbeterproces)
- muv 1 dep. (ivm geen eigen IT) hebben alle departementen in meer of mindere mate intentie tot redteaming of doen het al (gedeeltelijk)
- 3 departementen doen redteaming conform TIBER aanpak. – de meesten willen hierop groeien. Voor een beperkt aantal lijkt dit nog niet haalbaar.
- Bestuurlijk commitment tav structureel testen wordt bij ca 35% van de departementen nog niet als voldoende (deels) ervaren.
- Alle departementen hebben zicht op hun dreigingslandschap
- Alle departementen zijn bereid tot kennisdelen maar voor het merendeel (ca 65%) beperkt (dat betekent in beperkte vertrouwde kring en niet de meest gevoelige details)
- Het opvolgen van bevindingen loopt bij ca 50% van de departementen matig en ca 50% goed (verbeterproces voor 50% van de departementen – relatie met bestuurlijk commitment)

8

4.3 Stappenplan 2022-2026

stappenplan 2022-2026

	2022	2023	2024	2025	2026
	Pilotjaar 1 *1 tot 2 red-teaming testen interdep. (op Rijksbr. voorzieningen) *opstellen testframe-work (met partners van bv watersector) * veilig en goed inkopen van red-teaming	Pilotjaar 2 met een uitbreiding in scope en complexiteit n.a.v. ervaringen en resultaten jaar 1	Beperkte gezamenlijke (Rijks)testkalender en voeren deze uit	Uitgebreidere (Rijks)testkalender en voeren deze uit	wij hebben een gezamenlijke jaarlijkse (Rijks)testkalender en voeren deze uit
	Kennis delen en van elkaar leren in groep van aangemelde dep.(onderdelen) – veilige omgeving en voorwaarden inrichten	Kennis delen en van elkaar leren in bredere groep (uitbreiding groep) o.b.v. de inrichting. Inrichting en voorwaarden verbeteren.	In een veilige omgeving delen we kennis en leren we van elkaar	In een veilige omgeving delen we kennis en leren we van elkaar	In een veilige omgeving delen we kennis en leren we van elkaar
	Bevindingen worden opgevolgd. Oefenen met opvolging geven bij niet geteste onderdelen - processen daarvoor inrichten	Bevindingen worden opgevolgd o.b.v. de processen. Oefenen met opvolging geven bij niet geteste onderdelen (uitbreiding groep) – processen verbeteren o.b.v. ervaringen	We geven opvolging aan bevindingen en worden steeds beter (weerbaar)	We geven opvolging aan bevindingen en worden steeds beter (weerbaar)	We geven opvolging aan bevindingen en worden steeds beter (weerbaar)

9

4.4 Conclusies, reactie motie en toezegging

De digitale weerbaarheid van de Rijksoverheid is gediend bij op meer structurele basis testen van de weerbaarheid van organisaties, zodat die gericht verbeterd kan worden. Het delen van kennis uit dergelijke testen binnen de Rijksoverheid zal de weerbaarheid ook verbeteren. Onderdelen van het TIBER-NL programma die ook toepasbaar zijn bij de Rijksoverheid zijn dan ook o.a.:

- realistische scenario's op basis van inlichtingen vormen de testbasis;

- geavanceerde ethische hackteams voeren de test uit;
- coördinatie van de test door een white team met voldoende mandaat in de organisatie om de test te kunnen doorzetten of onderbreken;
- gericht op verbetering in een hele sector, door het vertrouwelijk delen van ervaringen zodat ervaring bij één organisatie leidt tot verbeteringen bij een grotere groep;
- vrijwillige deelname van organisaties.

Red-teaming en andere testen worden al bij onderdelen van de Rijksoverheid toegepast. Hierbij wordt in een aantal gevallen ook de TIBER-NL aanpak gehanteerd. Het onderzoek heeft zich daarom vooral gericht op het structureel borgen van dergelijke testen als resultaat van de I-strategie Rijk. Onderdeel hiervan is het delen van resultaten, zoals par. 1.1. weergegeven. De randvoorwaarden hiervoor zijn opgenomen onder 4.5 bullet 3. In 2022 gaan we deze randvoorwaarden binnen het plan van aanpak realiseren en daarmee oefenen in een beperkte setting. Daarna wordt het verder uitgebouwd en onderdeel van 'continue verbeteren'.

4.5 Kritische succesfactoren, aandachtspunten op hoofdlijnen

Het succes van structureel technisch testen (pentesten, red-teaming, red-teaming conform framework is afhankelijk van een aantal factoren.
De Belangrijkste zijn:

1/ Bestuurlijk commitment
- De departements- en organisatieleiding committeert zich aan en investeert in de testen en het opvolging geven aan bevindingen, is betrokken en stuurt op volwassenheid van het verbeterproces
- Accepteert dat er in eerste periode (jaren) mogelijk met regelmaat (ernstige) bevindingen naar boven komen en draagt uit dat dit een logische en noodzakelijke fase is om de weerbaarheid structureel te verbeteren.

2/ Voldoende capaciteit en (financiële) middelen om:
- Bij de departementen en ICT dienstverleners testen te kunnen uitvoeren.
- Oefeningen en testen te begeleiden en te ondersteunen.
- Geschikte (externe) partijen te selecteren die oefeningen en testen kunnen voeren bij de departementen en ICT dienstverleners.
- In de (IT) uitvoering bevindingen op te kunnen lossen (niet alleen correctie/incidenteel (eenmalig), maar ook corrigerend/structureel (gericht op het voorkomen van herhaling).

3/ Invullen van de randvoorwaarden voor veilig kennis delen (uit 4.4):
- Beschikbaar zijn van een vertrouwde omgeving (fysiek, digitaal en sociaal).
- Herkenbaarheid/herbruikbaarheid van bevindingen in andere omgevingen dan waarop de test direct betrekking had. (dit betekent ook dat de meest gevoelige specifieke details niet worden gedeeld).

Het advies is om te zorgen dat deze blijvend zijn ingevuld bij ieder departement door samenwerking tussen bestuur, CIO's en CISO's.

Bijlage A Motie en toezegging

MOTIE VAN HET LID RAJKOWSKI C.S.

Voorgesteld 28 oktober 2021

De Kamer,
gehoord de beraadslaging,

overwegende dat onze vitale infrastructuur, waaronder die van de rijksoverheid, doelwit is van cyberaanvallen;

overwegende dat de NCTV in het Cybersecuritybeeld Nederland 2021 aangeeft dat digitale processen het «zenuwstelsel» vormen van de maatschappij, omdat ze onmisbaar zijn voor het ongestoord functioneren daarvan, en dat cyberaanvallen dit zenuwstelsel aantasten en uiteindelijk kunnen leiden tot verlamming, ook bij de rijksoverheid;

constaterende dat De Nederlandsche Bank gebruikmaakt van het programma TIBER-NL, waarmee door middel van realistische dreigingen wordt getest hoe financiële instellingen bestand zijn tegen cyberaan-vallen, met als doel om inzicht te krijgen in sterke en zwakke onderdelen van digitale systemen, daarvan te leren, vervolgens de systemen te verbeteren en de ervaringen te delen;

van mening dat de TIBER-NL-testen een bijdrage kunnen leveren aan de digitale veiligheid van de rijksoverheid;

verzoekt de regering na te gaan of de TIBER-Nederland-testen dan wel soortgelijke testen ook binnen de organisatie van de rijksoverheid toegepast kunnen worden, de opgedane ervaringen en daaruit getrokken lessen rijksbreed te delen, en de Kamer daarover te informeren voor 1 april 2022,

---

Toezegging 28 oktober 2021 Kamerbrief –beantwoording vragen tijdens de begrotingsbehandeling 27 oktober 2021:

Vraag:
Welke onderdelen van methoden als TIBER kunnen in Nederland worden ingezet?

Antwoord:
TIBER staat voor Threat Intelligence Based Ethical Red-teaming. De Nederlandsche Bank heeft deze gerichte oefen- en testmethode ontwikkeld en deze is geadopteerd door de Europese Centrale Bank om instellingen beter cyber-weerbaar te maken. Het proberen te voorkomen van incidenten met preventieve maatregelen is al lang niet meer voldoende en er is een meer proactieve aanpak nodig. Red-teamingoefeningen worden al bij onderdelen van de Rijksoverheid uitgevoerd, met goede resultaten, en het TIBER-programma kan kennisuitwisseling hierover verbeteren. In de I-Strategie Rijk heeft de staatssecretaris aangegeven dat onderdelen van een red-teaming programma zoals het TIBER-programma interessante inzichten in kwetsbaarheden kunnen geven en daarom zullen worden onderzocht voor toepassing binnen de Rijksoverheid. Het gaat hierbij dan ook om het versterken van de onderlinge uitwisseling van good practices en oefenen binnen organisaties. Over de voortgang hiervan zal de staatssecretaris uw Kamer in het voorjaar van 2022 informeren.

Bijlage B Overzicht direct betrokkenen en versie beheer

Overzicht van betrokkenen

organisatie	naam	Rol/functie
BZK/DGOO	CIO/(CISO) Rijk	(gemandateerd) opdrachtgever (eindverantwoordelijk voor de kwaliteit van het onderzoek, rapport), vaststellen rapport
BZK/DGOO	Beleidsadviseur	Onderzoeker trekker, rapporteur (verantwoordelijk voor de kwaliteit van het onderzoek, rapport)
BZK/DGOO	Beleidsadviseur	Adviseur, werkgroep lid onderzoeker (betrokken in alle fasen van het onderzoek o.a. in de rol 'consulted')
DEP A en B /CISO	CISO	Adviseur, werkgroep lid onderzoeker (betrokken in alle fasen van het onderzoek o.a. in de rol 'consulted')
NCTV/NCSC/DNB	divers	Leveren input gezien de relatie met gerelateerde ontwikkelingen op het gebied van red-teaming en testen.
CISO- raad en CTO-raad	CISO's en CTO's departementen	bespreken plan van aanpak
DT DIO Rijk	directieteam	Bespreken plan van aanpak en beoordelen rapport en kamerbrief
CIO-beraad	CIO's departementen en grote uitvoeringsorganisaties	Stellen het plan van aanpak vast, als gevolg van dit onderzoek en kennis nemen van rapport en kamerbrief.

Versiebeheer van het onderzoeksrapport

versienr	datum	wijzigingen
Conc 0.2	20-01-2022	Eerste volledige concept obc aanzet 0.1 en het uitgewerkte plan van aanpak concept 6
Conc 0.3	02-02-2022	Feedback eerste review verwerkt
Conc 0.4	08-02-2022	Feedback CISO Rijk verwerkt
Conc 0.5	09-02-2022	Tekst aanpassing consistentie brief en rapport
Conc 0.6	15-02-2022	Review DNB (op TIBER teksten) verwerkt
Conc 0.7	17-02-2022	Tekst ambitie aangescherpt tav achterliggend doel
Def 1.0	16-03-2022	Def gemaakt na CIO-beraad, akkoord via e-paraferen, geanonimiseerd en dossiernr. aangepast. Geen inhoudelijke wijzigingen