Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

26 643 Informatie- en communicatietechnologie (ICT)

31 490 Vernieuwing van de rijksdienst

Nr. 836

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 1 april 2022

Tijdens de begrotingsbehandeling op 28 oktober 2021 is er stilgestaan bij het testen van de digitale weerbaarheid bij de rijksoverheid. Er is hierover een motie ingediend door het lid Rajkowski c.s.[1] en mijn voorganger gaf al aan dat red-teaming binnen de rijksoverheid wordt toegepast en dit binnen de I-strategie Rijk 2021 -2025 verder zal worden versterkt. Mijn voorganger zegde u toe over de voortgang op dit onderwerp te informeren. Met deze brief geef ik vervolg aan zowel de motie als de toezegging.

Versterken digitale weerbaarheid

Onder meer het Cyber Security Beeld Nederland (CSBN) 2021 laat zien dat er acute dreiging is van statelijke en criminele actoren, ook tegen de (rijks)overheid. Eerder CSBN's signaleerden ook dat de overheid achterloopt in de organisatie van digitale weerbaarheid. Cyberveiligheid heb ik daarom benoemd als essentiële randvoorwaarde van een sterk fundament in mijn hoofdlijnenbrief van 8 maart 2022. In de I-strategie 2021–2025 is beschreven hoe we de digitale weerbaarheid van de rijksoverheid gaan versterken.[2] Als Staatssecretaris voor digitalisering heb ik hierop een aanjagende en regisserende rol richting alle departementen. Robuuste stappen voor onze weerbaarheid zijn noodzakelijk.
We moeten de proactieve aanpak van informatiebeveiliging verder versnellen. Een essentieel element in die proactieve aanpak is het structureel testen van de eigen organisatie, om kwetsbaarheden en risico's te identificeren en te kunnen aanpakken. We weten immers dat ondanks alle inzet fouten gemaakt kunnen worden, nieuwe kwetsbaarheden bekend worden, en aanvallers steeds nieuwe methoden ontwikkelen.

[1] Kamerstuk 35 925 VII, nr. 16
[2] Kamerstuk 26 643, nr. 779

kst-26643-836
ISSN 0921 - 7371
's-Gravenhage 2022

Het plan van aanpak zoals verderop in deze brief genoemd, is voor de komende periode de leidraad voor de uitvoering van de toezegging. Daarbij zullen we steeds alert zijn op mogelijkheden om te versnellen en te intensiveren, en zo het plan van aanpak sneller af te ronden waar mogelijk. Waar in het uitvoeren van het plan van aanpak blijkt dat bestaande kaders en richtlijnen onvoldoende duidelijk of stevig zijn, of in de weg zitten, zal ik vanuit BZK het voortouw nemen deze aan te vullen en aan te scherpen, om het zo mogelijk te maken op het gewenste veiligheidsniveau te komen. Dit zal ik ook doen als de ontwikkelingen rondom digitale risico's en dreigingen daarom vragen, zowel voor wat betreft inzet op red-teaming als andere thema's die noodzakelijk zijn voor een veilige digitale rijksoverheid.

TIBER-onderzoek naar aanleiding van motie Rajkowski

Een goed en bekend voorbeeld van testen is het TIBER-NL programma van De Nederlandsche Bank (DNB), waar de motie van lid Rajkowski aan refereert. TIBER staat voor Threat Intelligence Based Ethical Red-teaming. Binnen dit programma testen financiële instellingen hoe weerbaar ze zijn tegen geavanceerde cyberaanvallen. Dit gebeurt met testaanvallen die zijn gebaseerd op realistische dreiging. Een klein team van DNB coördineert, maar de instellingen zelf voeren de testen uit. Dit is overigens slechts één van de soorten testen die organisaties (kunnen) uitvoeren om hun weerbaarheid te onderzoeken. Ook andere soorten testen worden bij de rijksoverheid uitgevoerd, zoals pentesten.
Het is belangrijk om op te merken dat testen geen doel op zich is. Delen van de geleerde lessen en opvolging geven aan de gevonden kwetsbaarheden en risico's zijn het uiteindelijke doel, omdat dan de digitale weerbaarheid daadwerkelijk omhoog gaat. Hiertoe is in de Baseline Informatieveiligheid Overheid (BIO) ook de verplichting tot testen en het opvolgen van bevindingen uit die testen opgenomen.
In reactie op de motie is door CIO Rijk onderzocht of en hoe TIBER toegepast kan worden binnen de rijksoverheid. Hierbij is ook gekeken naar andere vormen van red-teaming.[3] Dit onderzoek is uitgevoerd in samenwerking met onder meer De Nederlandsche Bank, de NCTV en enkele departementale CISO's. En het is besproken in de raden voor ICT en informatiebeveiliging bij de rijksoverheid, om zo gebruik te maken van de reeds aanwezige kennis binnen de rijksoverheid. Het volledige onderzoek is als bijlage bij deze Kamerbrief gevoegd[4]. Ik benoem hieronder de inhoud op hoofdlijnen en het vervolg.

Conclusies van het onderzoek

De belangrijkste, en positieve, conclusie is de bevestiging dat red-teamingtesten al binnen onderdelen van de rijksoverheid worden toegepast en dat daarbij in een aantal gevallen ook de TIBER-aanpak wordt gehanteerd. Omdat red-teaming breder is dan TIBER zal vanaf nu steeds gesproken worden over red-teaming, in plaats van alleen specifiek TIBER.
Omdat de vraag óf de TIBER-aanpak toepasbaar is daarmee is beantwoord, is in het onderzoek vooral gekeken naar het structureel borgen en versterken van soortgelijke (red-teaming) testen en hoe resultaten ervan breder gedeeld kunnen worden. De conclusie is dat dit mogelijk is als wordt voldaan aan enkele randvoorwaarden voor vertrouwelijkheid en de wijze van omgaan met de resultaten.

---

[3] Een red-teamingtest is een vorm van aanvalssimulatie. Het team dat in deze simulatie de aanvallende partij speelt (red team) probeert de organisatie zo realistisch mogelijk aan te vallen. Dit gebeurt aan de hand van aanvalsscenario's.
[4] Raadpleegbaar via www.tweedekamer.nl

Als eerste moet er een vertrouwde omgeving (fysiek, digitaal en sociaal) beschikbaar zijn. Verder is het van belang dat de uitkomsten en bevindingen zo worden geformuleerd dat ze voor andere organisaties binnen de rijksoverheid dan de geteste organisatie bruikbaar zijn. Informatie over specifieke kwetsbaarheden zal daarmee in principe vertrouwelijk blijven. De betrouwbaarheid van de partij die de red-teaming uitvoert is daarbij ook belangrijk en wordt in het traject meegenomen.
Een fictief voorbeeld is een kwetsbaarheid in emailservers. Als deze informatie in verkeerde handen zou komen, zou die gebruikt kunnen worden om daadwerkelijke aanvallen uit te voeren op het emailsysteem van de betrokken organisatie, zolang de verbetermaatregel nog niet is doorgevoerd.
Door het risico van de kwetsbaarheid generiek te formuleren, is dit in een veilige omgeving wel deelbaar. Andere organisaties kunnen checken of dit in hun omgeving ook aan de hand is en een risico vormt. Zij kunnen dan gericht verbeteren zonder ook zelf getest te zijn.

Vervolg en randvoorwaarden

De bevindingen van het onderzoek bieden een goede basis voor verdere borging en versterking van inzet van red-teaming binnen de rijksoverheid. Daarvoor is een plan van aanpak opgesteld dat rekening houdt met de invulling van geschetste randvoorwaarden. De ambitie – het verhogen van de feitelijke veiligheid – wordt langs drie sporen uitgewerkt:

1. Een gezamenlijke jaarlijkse testkalender, die ook wordt uitgevoerd.
2. Een veilige omgeving waarbinnen kennis (opgedaan vanuit de testen) gedeeld kan worden.
3. Een proces om bevindingen deelbaar te maken.

De planning is om rijksbreed in 2022 de basis te realiseren en daarna verder door te groeien vanuit uitgevoerde testen. Uiterlijk in 2025 zal de ambitie volledig zijn ingebed in de rijksbrede manier van werken en zijn red-teamingtests vast opgenomen in de testplanning en begrotingscyclus. Het streven is om dan een normenkader beschikbaar te hebben voor securitytesten, waarbij ook naar ketens gekeken wordt. De uitvoering van het plan van aanpak wordt opgepakt vanuit CIO Rijk, in samenwerking met de departementen. De departementen zullen tevens zelf periodiek testen blijven uitvoeren.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
A.C. van Huffelen