Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

25 295 **Infectieziektenbestrijding**

26 643 **Informatie- en communicatietechnologie (ICT)**

Nr. 1703

BRIEF VAN DE MINISTER VAN VOLKSGEZONDHEID, WELZIJN EN SPORT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 23 december 2021

Op 24 november jl. heeft uw vaste commissie Digitale Zaken mij – naar aanleiding van het artikel van Computable.nl «VWS werkt aan supertool voor analyse kwetsbaarheden» – verzocht om een kabinetsreactie. Met deze brief ga ik graag op dit verzoek in. De Kwetsbaarheden Analyse Tool, kortweg KAT[1], is immers een instrument om trots op te zijn.

KAT is gerealiseerd in tijden van crisis, waarin de noodzaak hoog is om snel en betrouwbaar de voor de bestrijding van de pandemie ontwikkelde digitale hulpmiddelen op het juiste beveiligingsniveau te brengen en houden. Denk daarbij bijvoorbeeld aan de voortdurende monitoring van het CoronaCheck-stelsel. Aandacht voor cybersecurity in de digitale wereld is cruciaal en ook de overheid is in toenemende mate het doelwit van hackers. Om te voorkomen dat cybercriminelen netwerken binnendringen moeten kwetsbaarheden in software zo snel mogelijk worden opgespoord en gerepareerd. We stellen daarom ook hoge voorwaarden aan testaanbieders die willen aansluiten op CoronaCheck[2]. Zo moeten ze genormeerde pentestresultaten laten zien en een verklaring ten aanzien van het voldoen aan NEN-7510. Dergelijke hoge eisen stellen we ook aan de digitale middelen die we zelf ontwikkelen en daarom ook voortdurend bewaken.

De vraag is niet zijn we veilig, maar zien we kwetsbaarheden?

Zoals bekend heeft het Ministerie van VWS ter ondersteuning van het terugdringen van de COVID-19 pandemie een reeks aan digitale middelen

[1] KAT is een initiatief van het Ministerie van Volksgezondheid, Welzijn en Sport (VWS), in samenwerking met Z-Cert, het Computer Emergency Response Team voor de zorg. Z-Cert helpt mee aan de ontwikkeling in het zorgveld. KAT ondersteunt Z-Cert met de juiste contextuele informatie.

[2] Aansluiting op CoronaCheck voor aanbieders testen: www.rijksoverheid.nl/onderwerpen/coronavirus-covid-19/coronabewijs/coronacheck-voor-aanbieders-testen

kst-25295-1703
ISSN 0921 - 7371
's-Gravenhage 2021

ontwikkeld. Denk aan CoronaMelder, CoronaCheck, GGD-contact, BRBA, HKVI en ZKVI[3]. Zoals eerder toegezegd aan en mede op wens van uw Kamer[4] is deze software samen met een bredere community van deskundigen ontwikkeld in volledige transparantie, volgens de principes van open source en met de hoogste kwaliteitseisen aan toegankelijkheid, privacy en security. Al vanaf de ontwerpfase wordt daarbij nagedacht over gegevensbescherming en informatiebeveiliging gericht op het veilig toepassen van de digitale hulpmiddelen, alsook het minimaliseren van de risico's voor misbruik en fraude[5]; *privacy en security by design* dus.

Tegelijkertijd zullen er altijd risico's blijven. Het is zaak die te onderkennen, zoveel mogelijk te mitigeren, voortdurend te bewaken en in te grijpen bij (dreigende) verstoringen. De vraag die wij onszelf daarbij stellen is niet of we veilig zijn, maar waar we kwetsbaarheden zien waar we iets mee moeten. Met die invalshoek zorgen we voor betrouwbare digitale ondersteuning in deze pandemie en neemt het Ministerie van VWS ook zijn verantwoordelijkheid ten aanzien van informatiebeveiliging, mede op verzoek van de Autoriteit Persoonsgegevens (AP)[6]. Net als bij de ontwikkeling van de digitale ondersteuningsmiddelen leg ik bij de informatiebeveiliging de lat hoog en wil ik zelf in control zijn wanneer op de markt geen geschikte tools beschikbaar zijn. KAT is hiervan het resultaat.

Wat doet de Kwetsbaarheden Analyse Tool?

KAT wordt ontwikkeld door het Ministerie van VWS en combineert zelf ontwikkelde toepassingen met bestaande open source software. Denk daarbij aan toepassingen om specifieke pentesten uit te voeren. Met dit geheel wordt het mogelijk om te scannen op kwetsbaarheden in apps, software en infrastructuren en de uitslagen hiervan aan elkaar te verbinden.

KAT analyseert frequent de kwetsbaarheden van alle onderdelen van het bewaakte landschap en van het landschap als geheel. KAT maakt voorafgaand aan dergelijke analyses allereerst een kopie van de feitelijke werkelijkheid. Binnen deze kopie kan gezocht worden naar antwoorden op beveiligingsvraagstukken en beleidsvragen. Denk aan het opsporen van oude of kwetsbare software, het controleren welke infrastructuur er in de organisatie gebruikt wordt en het voldoen aan toegankelijkheidseisen door websites. Door frequent te monitoren worden ook veranderingen zichtbaar gemaakt, forensisch geborgd en direct met de juiste personen gedeeld. Aan de hand van de vastgelegde tijdlijn kan ook achteraf worden getoetst of onderdelen van het landschap in het verleden kwetsbaar waren voor een pas later bekend geworden kwetsbaarheid. Een toepassing die een dergelijke tijdlijn aanlegt van het gehele bewaakte landschap en over de volle breedte van de gestelde eisen en normen analyses kan maken bestond nog niet.

KAT analyseert doorlopend en stelt vast of aan beveiligingseisen en andere eisen wordt voldaan. Waar nodig worden kwetsbaarheden en wijzigingen automatisch gemeld voor opvolging door medewerkers. Tijdrovende noodzakelijke handelingen worden geautomatiseerd en

---

[3] Kamerstuk 25 295, nr. 460
Kamerstuk 25 295, nrs. 950, 995 en 1241
Kamerstuk 25 295, nr. 1638

[4] Kamerstuk 25 295, nr. 277

[5] Ter illustratie: www.nos.nl/artikel/2389818-datalek-testaanbieder-iedereen-kon-valse-testuitslagen-in-app-coronacheck-krijgen

[6] Onderzoek AP naar beveiliging GGD bij corona: autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_beveiliging_ggd_corona.pdf

daardoor sneller uitgevoerd. Zo krijgen de betrokken informatiebeveiligingsexperts met KAT gemakkelijk de juiste context aangereikt om keuzes te maken.

Naast het bereiken van efficiëntie is de overheid hiermee zelfredzamer, en minder afhankelijk van externe factoren om snel tot de kern van mogelijke kwetsbaarheden te komen. Snelheid is in deze tijd ook belangrijk om in te grijpen op mogelijke aanvallen, misstanden of onjuistheden. Zo scannen we elke dag alle testaanbieders die zijn aangesloten op CoronaCheck. Dit om te kunnen blijven garanderen dat de dienstverlening die wordt aangeboden zo min mogelijk risico's kent en voldoet aan gestelde eisen en normen. Hiermee hebben we al honderden kwetsbaarheden gedetecteerd en samen met de stelselpartners opgepakt.

KAT wordt op dit moment specifiek toegepast in het zorgdomein. Daarom is ook Z-Cert, het Computer Emergency Response Team voor de zorg, betrokken bij de ontwikkeling. Het voornemen is dat de tool in de eerste helft van 2022 als open source beschikbaar is. Op een daarvoor geopende site[7] kunnen geïnteresseerden zich aanmelden om ook nu al bij te dragen aan KAT. Dit is wat mij betreft pas het begin, want met meer ogen zien we ook meer. Met die gedachte hoop ik dat KAT een beweging op gang brengt bij een grotere community van bedrijven, (semi-)overheden en experts op het gebied van security en compliancy. KAT is overigens geen commerciële dienst, maar een open source kwetsbaarheden analysetool die door iedereen kan worden ingezet en uitgebreid. Het is mijn voornemen om KAT te blijven ondersteunen ten behoeve van de informatiebeveiliging van onder meer het Ministerie van VWS, de rijksoverheid en de zorg.

Hoe veilig is het systeemlandschap van de Tweede Kamer?

Om te illustreren wat KAT voor een organisatie kan betekenen, heb ik in afstemming met uw Chief Information Security Officer (CISO) de tool toegepast op het systeemlandschap van de Tweede Kamer. Daaruit zijn 22 bevindingen gekomen, waarvan geen bevindingen in de risicocategorie *critical* of *high*. Ik heb het rapport met bevindingen met de Tweede Kamer gedeeld conform de *Coordinated Vulnerability Disclosure*[8] procedure van het Nationaal Cyber Security Center (NCSC) en begrepen dat de Tweede Kamer hiermee aan de slag is gegaan. Ik ben blij dat ik op deze manier heb kunnen bijdragen aan het veiliger maken van het systeemlandschap van de Tweede Kamer.

De Minister van Volksgezondheid, Welzijn en Sport,
H.M. de Jonge

[7] Website KAT: www.openkat.nl
[8] Leidraad Coordinated Vulnerability Disclosure: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/cvd-leidraad