VNO NCW

MKB Nederland

De Onderzoeksraad voor Veiligheid
T.a.v. de heer prof. dr. mr. S. Zouridis
Postbus 95404
2509 CK DEN HAAG

Briefnummer
22-121162

Onderwerp
Reactie OvV onderzoek Citrix

Den Haag
10 juni 2022

Telefoonnummer
070-3490352

E-Mail
mallens@vnoncw-mkb.nl

Geachte heer Zouridis, beste Staven,

Op 16 december 2021 heeft de Onderzoeksraad voor Veiligheid (hierna: 'Onderzoeksraad') het rapport "Kwetsbaar door software, lessen naar aanleiding van beveiligingslekken door software van Citrix" gepubliceerd. De Onderzoeksraad onderzocht welke lessen te trekken zijn uit de wijze waarop betrokken partijen zijn omgegaan met de risico's van kwetsbaarheden in Citrix-software, en heeft ook andere voorvallen waarbij kwetsbaarheden in software werden misbruikt door aanvallers onder de loep genomen.

De Onderzoeksraad doet in het rapport aanbevelingen aan partijen die kunnen bijdragen aan oplossingen voor de gesignaleerde veiligheidstekorten. Meer concreet is aan VNO-NCW en MKB-Nederland gevraagd binnen een half jaar te reageren op de navolgende aanbevelingen:

1. *Zorg er op korte termijn voor dat alle potentiële slachtoffers van cyberaanvallen snel en doeltreffend - gevraagd en ongevraagd - worden gewaarschuwd, zodat zij maatregelen kunnen treffen voor hun digitale veiligheid.*
2. *Breng daartoe private en publieke responscapaciteit samen en zorg daarbij voor voldoende mandaat en wettelijke waarborgen.*

VNO-NCW en MKB-Nederland juichen de aanbeveling toe om alle potentiële slachtoffers middels een effectief en efficiënt systeem te waarschuwen. Informatiedeling is cruciaal voor bedrijven om zich beter te kunnen wapenen tegen cyberaanvallen. In de bijlage schetsen we wat bedrijfsleven en overheid al doen om dit te verbeteren, en wat er nog meer en beter kan.

Wat ons betreft is nadere verkenning nodig om te bezien waar en op welke wijze (respons)capaciteit effectief en efficiënt kan worden samengebracht. De respons verschilt immers van organisatie tot organisatie, mede afhankelijk van de rol en de specifieke dienstverlening van de betreffende organisatie in het digitale ecosysteem, en zal daardoor niet altijd samen te voegen zijn. In de bijlage gaan we nader in op betere samenwerking, en wat daar voor nodig is.

Een afschrift van deze brief is gestuurd naar de heer Boots, directeur-generaal Economie en Digitalisering bij het ministerie van Economische Zaken en Klimaat. Wij hopen u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

dr. Rob. J. Mulder
directeur beleid

BIJLAGE

Informatieverstrekking potentiële slachtoffers van cyberaanvallen.

De eerste aanbeveling ziet op het verstrekken van informatie aan organisaties zodat deze zich optimaal kunnen voorbereiden op mogelijke incidenten dan wel noodsituaties.
VNO-NCW en MKB-Nederland onderschrijven het belang van goede informatiedeling. In onze optiek is dit één van de belangrijkste instrumenten om de cyberweerbaarheid van organisaties te verhogen. Bedrijven zullen sneller in actie komen wanneer zij concreet en op een wijze passend bij het cybervolwassenheidsniveau van betreffende organisatie, worden geïnformeerd dat hun eigen IT-systemen kwetsbaarheden vertonen of gehackt zijn.
Het is genoegzaam bekend dat het Nationaal Cyber Security Centrum (NCSC) op dit moment niet het mandaat heeft om de bij hen bekende incident- of dreigingsinformatie te delen met niet-vitale organisaties en de daartoe opgerichte schakelorganisaties.
Als gevolg daarvan bereikt deze essentiële informatie niet de getroffen bedrijven en zijn zij als gevolg hiervan niet in de gelegenheid om tijdig beschermingsmaatregelen te nemen. Dit is een zeer ongewenste situatie.
VNO-NCW en MKB-Nederland zien op dit moment een aantal ontwikkelingen die hoopvol stemmen:

- Recent is een voorstel tot aanpassing van de Wet Beveiliging Netwerk- en Informatiesystemen (WBNI) naar de Kamer gestuurd, waarmee het mandaat van het NCSC om informatie te delen met andere organisaties dan de doelgroep wordt verruimd. Hierdoor wordt het mogelijk dat ook niet-vitale aanbieders en zogenaamde organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten voor hun netwerk- en informatiesystemen (OKTT's) van informatie worden voorzien.

- In de nieuwe meldplicht van de Telecomwet 11a.2 lid 4 is de verplichting opgenomen dat aanbieders van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten hun gebruikers, die de gevolgen van een specifieke en aanzienlijke dreiging kunnen ondervinden, informeren over mogelijke beschermingsmaatregelen of oplossingen die zij kunnen toepassen. Waar passend informeert de aanbieder de gebruikers tevens over de dreiging zelf.

- In Brussel wordt onderhandeld over een herziening van de richtlijn voor netwerk- en informatiebeveiliging (NIB). De NIB-2 brengt een groot aantal organisaties in scope die via CSIRTs van informatie over dreigingen, kwetsbaarheden en incidenten moeten worden voorzien. Het NCSC en mogelijk nog andere op te richten CSIRTs zullen hier een centrale rol gaan vervullen.

- Ook is het Digital Trust Center (DTC) gestart met informatiedeling. Bedrijven die niet tot de vitale infrastructuur behoren worden door het DTC gevraagd en ongevraagd voorzien van informatie. Het gevraagd informatiedelen

gebeurt echter nog slechts op zeer beperkte schaal. Wij vinden het van groot belang dat deze functionaliteit snel wordt verbreed zodat alle potentiële slachtoffers snel en doeltreffend worden geïnformeerd. VNO-NCW en MKB-Nederland zijn van mening dat nauwe samenwerking tussen NCSC en DTC in dit verband gewenst en noodzakelijk is.

- Er vindt op verzoek van de NCTV een verkenning plaats naar de ontwikkeling van een nieuw samenwerkingsplatform voor het (door-)delen van data, informatie en kennis over kwetsbaarheden en incidenten. Belangrijk onderdeel van deze verkenning is het in kaart brengen aan welk type informatie behoefte is. Waar cybervolwassen bedrijven, waaronder bedrijven in de vitale infrastructuur, vooral behoefte hebben aan snelle, liefst zo specifiek mogelijke dreigingsinformatie (ruwe data) die niet direct vergezeld behoeft te gaan van duiding, is voor minder cybervolwassen bedrijven juist een concreet handelingsadvies noodzakelijk. Beide groepen zullen op maat van informatie moeten worden voorzien.

Deze ontwikkelingen stemmen hoopvol, maar zijn tegelijkertijd nog niet alle geeffectueerd. Dit betekent dat de door de Onderzoeksraad geconstateerde feilen in de informatiedeling vooralsnog blijven bestaan.
Dit is voor VNO-NCW en MKB-Nederland een grote zorg.

Alleen het ontvangen van informatie maakt bedrijven en onze samenleving overigens nog niet veiliger. Er moet ook gehandeld worden op basis van de ontvangen informatie. Hier nu zien we een groeiende cyberweerbaarheidskloof tussen organisaties die mee kunnen komen en incidentinformatie kunnen verwerken ten opzichte van organisaties die hiertoe niet in staat zijn omdat zij de benodigde kennis en capaciteiten missen om de maatregelen uit te voeren. Ook is er een groep bedrijven die de urgentie om maatregelen te nemen onvoldoende onderkent.
VNO-NCW en MKB-Nederland zetten zich op een aantal fronten in om de weerbaarheid van het bedrijfsleven tegen digitale dreigingen te versterken vanuit de gedachte dat alleen als de cybersecurity op orde is, de vruchten van digitalisering daadwerkelijk kunnen worden geplukt.
Via voorlichting zetten wij in op het activeren van brancheorganisaties om digitale veiligheid actief bij hun leden onder de aandacht te brengen. Hiertoe trekken wij op met het DTC en het NCSC. Wij zien hier dat een toenemend aantal brancheorganisaties de handschoen oppakt en actief is richting de leden met voorlichting en het verlenen van ondersteuning.
Speciaal voor brancheorganisaties zijn wij onlangs gestart met het platform "Samen Digitaal Veilig". Dit project is vooral -maar niet uitsluitend- gericht op kleinere bedrijven, en richt zich op bewustwording en concrete actie om de 'basis op orde te brengen'.
Ook zijn wij gestart met het geven van voorlichting voor de brancheorganisaties over ketenveiligheid en informatiedeling binnen de keten. Immers, een cyberincident ergens

in de keten kan een bedreiging vormen voor de continuïteit van andere bedrijven.
Wij constateren dat diverse grote bedrijven de rol van ketenregisseur op zich hebben genomen en kleinere bedrijven ondersteunen met informatie en advies.
Een ontwikkeling die wij van harte ondersteunen.

Samenbrengen responscapaciteit.
Om te kunnen beoordelen of de tweede aanbeveling daadwerkelijk een bijdrage levert aan de eerstgenoemde aanbeveling en/of een nuttige bijdrage levert aan het minimaliseren van cyberincidenten is het nodig te begrijpen hoe de Onderzoeksraad responscapaciteit definieert.
Hoewel er in het rapport veel over capaciteit gesproken wordt is er echter geen definitie opgenomen wat er verstaan wordt onder responscapaciteit.

VNO-NCW en MKB-Nederland gaan ervan uit dat de Onderzoeksraad bij deze aanbeveling niet alleen de respons in enge zin voor ogen heeft die elke individuele organisatie moet geven bij een cyberincident, maar doelt op een bredere definitie van responseapaciteit, waarvan het organiseren en samenbrengen van publieke en private capaciteiten op het vlak van informatiedeling, analyse, duiding, kennis en het geven van handelingsperspectief kernelementen zijn.

VNO-NCW en MKB-Nederland constateren dat het NCSC, verschillende sectorale CSIRTs en in toenemende mate ook het DTC, door het verstrekken van informatie over het specifieke incident, een belangrijke bijdrage leveren waarmee publieke en private organisaties de concrete respons ook daadwerkelijk invulling kunnen geven. Op basis van de verstrekte -verrijkte- informatie en evt. een handelingsperspectief, kunnen organisaties een, op de organisatie toegespitste, risicoanalyse uitvoeren en indien nodig aan de 'knoppen draaien' in het IT landschap. Kleinere organisaties zullen in dit proces veelal op hun IT dienstverlener leunen, de partij die het IT landschap voor hen geïnstalleerd heeft en beheert.

VNO-NCW en MKB-Nederland zijn -onder voorwaarden- voorstander van het dichter bij elkaar brengen van in ieder geval het NCSC en het DTC. Wij zien dit, mede gelet op de schaarste aan cybersecurity professionals, als een logische stap waarmee een impuls kan worden gegeven aan de versterking van de operationele samenwerking en de bredere informatiedeling. Dit ten behoeve van de respons van alle organisaties.
Nauwere samenwerking met bestaande en nieuw te vormen sectorale CSIRTs en andere schakelorganisaties door invulling van de liaisonfunctie en wellicht op termijn door colocatie zou in onze optiek een goed voorstelbare vervolgstap kunnen zijn.
Een verkenning hiernaar zou wenselijk zijn. De wenselijkheid en haalbaarheid van formele afspraken over de gezamenlijke inzet van responscapaciteiten van overheid en (cybersecurity)bedrijven in specifieke gevallen waarin de nationale responscapaciteit tekort schiet, zouden in deze verkenning moeten worden meegenomen.

Wij kunnen ons voorstellen dat individuele bedrijven, afhankelijk van hun cybervolwassenheid, een rol spelen bij de informatieverstrekking en -duiding ten behoeve van de respons. Wij zien een toenemende bereidheid tot samenwerking en het delen van dreigingsinformatie tussen publieke en private partijen.
De samenwerking zoals die plaatsvond in de log4j crisis is een goed voorbeeld van publiek-private samenwerking. Verschillende (publieke en private) partijen, hebben nauw samengewerkt door het gezamenlijk bijhouden van een lijst met (al dan niet kwetsbare) software en beschikbare patches, in het bundelen van responscapaciteit via het Nationaal Respons Netwerk en in informatiedeling en afstemming (zowel strategisch, tactisch als operationeel). Uiteraard kan dit nog verder verbeterd en uitgebouwd worden, maar het is wel een mooi voorbeeld van hoe een dergelijke samenwerking bij een (software-gerelateerd) cyberincident kan werken, met het NCSC als partij waar informatie en duiding samenkomt - maar waarbij vele partijen hun verantwoordelijkheid nemen en bijdragen aan het onder controle krijgen van de crisis.

Een digitale infrastructuur die de informatie gecombineerd met duiding en handelingsperspectief snel en zo doeltreffend mogelijk, al dan niet via schakelorganisaties, bij de individuele bedrijven en organisaties brengt die de uiteindelijke respons moeten uitvoeren, is vanzelfsprekend noodzakelijk. Ook kan deze infrastructuur worden gebruikt om informatie over incidenten en kwetsbaarheden vanuit de individuele organisaties snel en efficiënt naar het NCSC te sturen (zoals vitale aanbieders nu reeds doen op basis van de WBNI). Dit ter versterking van het situationele beeld en een betere duiding van ontwikkelingen.