COT | Instituut voor Veiligheids- en Crisismanagement
an Aon company

Samenvatting indrukken en leerpunten leerevaluatie respons Citrix

18 maart 2020

1. Inleiding en vraag

De minister van Justitie en Veiligheid heeft toegezegd aan de Tweede Kamer om de ervaringen naar aanleiding van het verhoogde risico rond Citrix ADC en Citrix Gateway servers te evalueren. Besloten is om een snelle evaluatie uit te laten voeren waarmee op korte termijn ervaringen en leerpunten worden geïnventariseerd vanuit verschillende sectoren (Mede-overheden, Vitaal, MKB, Rijkspartners en de zorgsector). De Nationaal Coördinator Terrorisme en Veiligheid (NCTV) heeft het COT Instituut voor Veiligheids- en Crisismanagement gevraagd deze snelle evaluatie uit te voeren. De focus ligt op het verzamelen van ervaringen binnen het zogeheten 'Landelijk Dekkend Stelsel'. Het functioneren van de nationale crisisorganisatie en van het NCSC zelf zijn geen onderdeel van de focus van deze evaluatie. De keuze voor deze scope is gemaakt om zo relevante bevindingen ten behoeve van het gehele stelsel op te halen. In deze notitie delen wij onze indrukken en leerpunten. Dit is gebaseerd op de informatie die opgehaald is tijdens de verschillende sessies.

2. Toelichting aanpak

Centraal in de uitvoering van de snelle evaluatie stonden plenaire lessensessies voor de eerdergenoemde sectoren. Tijdens deze sessies zijn meerdere thema's besproken.

De lessensessies zijn opgezet samen met de partners uit het Landelijk Dekkend Stelsel in opbouw: het NCSC, de IBD, CIO-Rijk, het DTC en Z-CERT. SURFcert (voor het onderwijs) is aangesloten bij de lessensessie van het NCSC. Elk van deze partners heeft (een selectie van) de eigen achterban uitgenodigd voor de lessensessie. Daarnaast is er apart gesproken met CSIRT Digitale Service Providers (DSP) over hun rol en ervaringen. De lessensessie over de samenwerking tussen NCSC/NCTV/CIO Rijk heeft vanwege Corona geen doorgang gevonden. Deelnemers aan die sessie zijn in de gelegenheid gesteld om schriftelijk hun indrukken en leerpunten te delen.

Tijdens de lessensessies is er intensief van gedachten gewisseld over de ervaringen en de leerpunten. De houding van de deelnemers was constructief kritisch. Ons overkoepelende beeld is dat de werkelijke impact van de verstoring rond Citrix voor de meeste organisaties beperkt is gebleven. Wel kwam duidelijk naar voren dat de gebeurtenissen en de afhandeling zelf indruk hebben gemaakt. Binnen organisaties zelf, maar ook binnen de samenwerking tussen verschillende organisaties. Er was breed waardering voor het feit dat een dergelijke evaluatie in korte tijd is opgezet en uitgevoerd. Tijdens de sessies zijn vele punten benoemd, zowel positief (trots en behouden) als mogelijke kansen voor versterking (verbeterpunten). Voor een deel van de mogelijke verbeterpunten geldt dat deze raken aan reeds langlopende discussies en voor direct betrokkenen reeds langer bekende knelpunten.

3. Context

De benoemde indrukken en leerpunten moeten bezien worden in de volgende context:

- Het Landelijk Dekkend Stelsel is 'jong' en nog vol in opbouw.
- De ontwikkelingen gaan snel: zowel in het cybersecuritydomein zelf als bij elk van de afzonderlijke organisaties die te maken krijgen met cybersecurity-uitdagingen.
- Er is een internationale setting waarin wordt gewerkt met bijbehorende afspraken en werkwijzen.
- Er is een wettelijk kader waarbinnen moet worden gewerkt.
- Er is de afgelopen tijd gewerkt aan een nieuw 'Nationaal Crisisplan Digitaal'. Dit plan was op het moment dat de Citrix-gebeurtenissen speelde nog niet afgerond, maar wel vol in ontwikkeling.

Er zijn regelmatig waarschuwingen rond cybersecurity-risico's of -incidenten. De situatie rond Citrix kende echter een aantal bijzondere kenmerken:

- De leverancier bevond zich in een situatie waarin hij heeft besloten het risico vroegtijdig openbaar te maken. Het risico was bij meerdere security-experts bekend en publiekelijke openbaarmaking van het risico dreigde en is daadwerkelijk gebeurd.

- Het bekendmaken van het risico ging gepaard met een eerste advies over het mitigeren van het risico.
- Vervolgens bleek dat het advies niet afdoende was om het risico weg te nemen. Dit mede op basis van inschattingen van inlichtingeninformatie. Hierbij was de inschatting dat de kwetsbaarheid ook daadwerkelijk zou worden misbruikt en waarschijnlijk zelfs al werd misbruikt.
- Dit leidde tot het dringende advies Citrix uit te schakelen. Indien dit niet mogelijk was, was het advies om aanvullende maatregelen te treffen.

4. Behouden

Er zijn vele leerpunten benoemd. We hebben bewust gevraagd naar waar de deelnemers trots op waren en wat zij wilden behouden. Dit waren de belangrijkste punten per doelgroep:

- **Mede-overheden** De mede-overheden waren trots op de snelheid van communiceren, de wijze van informatiedeling en de interne besluitvorming. De contacten tussen mede-overheden en de computercrisisteams verliepen goed en er was sprake van onderling vertrouwen.
- **MKB** Binnen de MKB-sector heerste het gevoel dat cybersecurity beter op de agenda staat dan voorgaande jaren. Het bewustzijn in de keten neemt toe en er werd goed informatie uitgewisseld via bijvoorbeeld het CIO-platform. De meeste organisaties hebben de impact beperkt kunnen houden.
- **Rijkspartners** Bij de Rijkspartners was er sprake van een snelle interne besluitvorming en korte lijnen en er was veel onderling vertrouwen. CIO Rijk heeft in het IAO een volwaardige crisisrol kunnen vervullen.
- **Vitaal** In de vitale sector vonden organisaties het advies van het NCSC moedig. Het NCSC wordt daarnaast gezien als betrouwbare en veilige gesprekspartner. Het NCSC is trots op de intrinsieke motivatie en inzet van medewerkers. Intern bij de organisaties was er sprake van snelle besluitvorming en werden maatregelen vaak vroegtijdig uitgevoerd (na het eerste advies van het NCSC in december). De samenwerking en informatiedeling in de sectoren en het netwerk (CIO-platform) verliepen snel en goed.
- **Zorgsector** In de zorgsector verliep de samenwerking tussen Z-CERT en de deelnemers goed. De deelnemers waren tevreden over het kennisniveau van Z-CERT en de communicatie verliep snel en gemakkelijk. De organisaties hebben daarnaast een gedegen eigen risicoafweging gedaan. Het was niet binnen alle organisaties nodig om in de crisisstructuur op te schalen.

5. Overkoepelende lessons learned Landelijk Dekkend Stelsel

De overkoepelende lessons learned die we naar aanleiding van de evaluatie meenemen zijn onder andere het verschil in opvatting over het gegeven advies vanuit het NCSC en de impact die het had op de sectorale partijen (en eventuele achterban). Enerzijds vonden organisaties het advies gedurfd, anderzijds was er behoefte aan meer informatie om te kunnen vertrouwen op het gegeven advies van het NCSC. Hierbij ontstond een extra moeilijkheid voor internationale organisaties die met meerdere NCSC's dan wel met private partijen te maken hebben die andere (of geen) adviezen gaven.

Bij veel organisaties leeft de vraag hoe het Landelijk Dekkend Stelsel werkt en dan met name de verschillende rollen en de wettelijke mandaten die daarmee samenhangen. Daarbij spelen vooral vragen over 'het wel of niet mogen delen' van informatie (met name buiten de vitale sector), de vraag wie de nationale regie voert en wat de rol van de sectorale computercrisisteams is. De meer algemene risico-informatie kan breed worden gedeeld. De discussie gaat vooral over meer specifieke informatie: over de onderbouw van de duiding, specifieke technische informatie en/of specifieke informatie over bedreigde/kwetsbare organisaties. Binnen de sectoren zien organisaties ook graag een nauwere sectorale samenwerking tussen de verschillende ISAC's en het NCSC. De verwachtingen van de verschillende onderdelen van het stelsel kloppen niet altijd met de werkelijkheid: het stelsel is in opbouw. De rol in de koude fase (voorbereiding) en lauwe fase (risico's) is helder: respectievelijk het voorbereiden en opbouwen van een community, en daarnaast het delen van (risico)informatie. Het is vooral belangrijk om duidelijk te zijn over de rol in de 'warme' fase: als er daadwerkelijk problemen zijn, wat mogen organisaties dan verwachten qua snelheid en type informatie en vanuit wie ontvangen ze deze?

Er ontstonden veel vragen over de opschaling van de crisisstructuur bij een ICT-crisis. Op welke structuur dient met terug te vallen? Was hier überhaupt sprake van een crisis? En wie is verantwoordelijk voor deze duiding? Sommige organisaties hebben hun eigen crisisstructuur opgeschaald en zochten aansluiting met andere crisisteams, terwijl andere organisaties de Citrix-kwetsbaarheid als 'business as usual' hebben ervaren. Vaak werd de media-aandacht als

escalerende factor genoemd rondom de kwetsbaarheid; deze heeft er volgens velen voor gezorgd dat de situatie rondom Citrix 'groter' werd dan dat hij feitelijk was. Deze dynamiek zorgde weer voor bestuurlijke druk binnen organisaties; er werd uitgeschakeld omdat men – ondanks eigen technische inschattingen – niet het risico durfde te nemen om achteraf uit te moeten leggen waarom een 'advies van de overheid' niet is opgevolgd.

6. Bijzonderheden per sector: wat kan er beter?

Tijdens de verschillende lessensessies is er een aantal sectorspecifieke lessons learned opgehaald.

- ✓ **Mede-overheden** Een belangrijke les is dat er geen centraal informatieknooppunt voor provincies is en er tevens geen computercrisisteam is ingeregeld. Verder gaven de mede-overheden aan vaker cyber te willen beoefenen. Dit past ook bij de inspanningen van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en de Vereniging Nederlandse Gemeenten (VNG) om tot cyberoefenpakketten te komen. Wat het voor sommigen lastig maakte gedurende de Citrix-gebeurtenissen is het feit dat de situatie een politieke lading kreeg. Hierdoor raakten bestuurlijke aspecten en meer operationele informatie en acties verweven.
- ✓ **Rijkspartners** Bij de Rijkspartners willen de organisaties de contacten in de koude fase verder aanhalen, zodat er sneller contact wordt gelegd gedurende een incident/crisis en men elkaar beter weet te vinden. Het CIO Rijk werkt nog aan zijn interne crisisproces, met Citrix is hier flink wat ervaring opgedaan. Het is daarnaast belangrijk om binnen het IAO scherp te hebben wie in welke rol aanwezig is vanuit CIO Rijk en de departementen die aansluiten.
- ✓ **MKB** Bij de niet-vitale organisaties is er waardering voor de inspanningen maar ook kritiek; vooral op de meer specifieke informatievoorziening en de onderbouwing van adviezen. Vooral als er informatie is die aangeeft dat een organisatie daadwerkelijk gevaar loopt: 'de deur staat open en we weten dat inbrekers dit kunnen misbruiken.' Dergelijke informatie is via verschillende publieke bronnen en soms vertrouwelijke bronnen al wel beschikbaar, maar kan niet worden gedeeld vanuit de overheid vanwege beperkingen vanuit onder meer geldende (privacy-)regelgeving. Tegelijkertijd is er geen arrangement waarin anderen dan het NCSC hier wel een rol in kunnen spelen om heel gericht organisaties te informeren, real time en specifiek. De verschillen tussen organisaties in aanpak en volwassenheid zijn groot. Veelal hebben organisaties de IT-organisatie opgeschaald maar niet per se met een crisisteam gewerkt. Er zijn steeds meer samenwerkingsverbanden rond cyber waarin informatie en voorbeelden worden gedeeld. Naast regionale samenwerking is er ook behoefte aan sectorale samenwerking om in de 'warme fase' (gevaar/incident/crisis) ervaringen te delen.
- ✓ **Vitaal** In de vitale sector deden organisaties met name een oproep aan het NCSC om actief de sector op te zoeken om daar aanwezige kennis te benutten: juist ook in de warme fase. Voor het NCSC en organisaties was het prettig geweest als het NCSC zelf diepgaander technisch onderzoek kan uit voeren en hier niet voor afhankelijk is van andere partijen. Indien het NCSC aan sector om bepaalde informatie vraagt en een terugkoppeling verwacht of ruggespraak wil houden, is het belangrijk dat het NCSC zelf goed bereikbaar is. Daarnaast is het voor het NCSC een les om nog meer aandacht te hebben voor de precieze woorden in het advies en de impact die het advies heeft.
- ✓ **Zorgsector** In de zorgsector hadden organisaties behoefte aan meer duiding omtrent het advies van het NCSC. Dit maakte dat het lastig was om intern uitleg te geven over de impact van de situatie, en daarbij werd het als lastig ervaren de impact van het afschakelen te duiden. Tot slot was het voor organisaties lastig om te bepalen wanneer het weer 'veilig; was. De beslisboom vanuit het NCSC werd niet als duidelijk genoeg gezien. Een les voor het Z-CERT is om de communicatiemiddelen te reduceren.