Ministerie van Economische Zaken
en Klimaat

Jaarbericht CSIRT-DSP

TLP:PUBLIC

Inhoud

Voorwoord

2021 bleek toch een meer bewogen jaar dan 2020. Corona leek even weg en kwam weer terug. Wat bleef is het gebruik en afhankelijkheid van clouddiensten. En toen mensen weer naar kantoor mochten, bleven ze gebruik maken van de gemakken die het internet en de Cloud brengt. Ook online marktplaatsen hebben geprofiteerd van de digitalisering van bedrijven, om bij de sluiting van fysieke winkels, online hun producten alsnog te kunnen aanbieden. Deze afhankelijkheid vestigt ook meer aandacht op de beveiliging van al deze diensten. Aandacht vanuit de klant, de leverancier maar ook vanuit de kwaadwillende. De kwetsbaarheden vlogen ons om de oren.

2022 en verder zal ook andere veranderingen met zich meebrengen. Zo zullen er stappen gezet worden voor de opvolger van de Netwerk- en Informatiebeveiliging-richtlijn, of te wel de NIB2-richtlijn of de Engelstalige afkorting NIS2 directive. En uiteraard gaan wij verder met de samenwerking met de toezichthouder, Agentschap Telecom om Cloud dienstverleners en online marktplaatsen te ondersteunen.

Vanuit het CSIRT voor digitale dienstverleners wensen wij u al het goeds voor 2022!

Joost Altena
Operationeel Manager CSIRT-DSP

Recap 2021

Samenwerking met NCSC en DTC

Binnen Nederland zijn er verschillende overheidsinstanties waar mensen informatie over cybersecurity kunnen vinden. De verschillende (overheid)instanties bedienen hiermee elk hun eigen doelgroep, maar werken samen om de informatie ook te benutten voor organisaties die niet onder die doelgroep vallen. Het CSIRT-DSP voor digitale dienstverleners, het NCSC voor essentiële en vitale dienstverleners en rijksoverheid en het Digital Trust Center voor het niet-vitale bedrijfsleven, met extra aandacht voor het MKB.

Met de toenemende aantallen cyberaanvallen en om zo goed mogelijk bij te dragen aan een cyberweerbaar Nederland is het van belang dat de overheid niet alleen goed samenwerkt met private partijen, maar ook met andere overheidsinstanties. Op het gebied van cyberveiligheid voor het bedrijfsleven wordt er nauw samengewerkt tussen het DTC, NCSC en CSIRT-DSP. Daarnaast werkt het CSIRT-DSP samen met sectorale CERT's zoals Z-CERT en surfCERT, maar ook met Europese nationale CERT's binnen het EU CSIRTs Network.

In 2021 zijn er flinke sprongen in de samenwerking met deze partijen gemaakt. Het Digital Trust Center is aangewezen als OKTT (objectief kenbaar tot taak)[1] en heeft een dienst opgericht om dreigingsinformatie te kunnen delen met doelgroep organisaties. Omdat zowel het DTC als het CSIRT-DSP onder het Ministerie van Economische Zaken en Klimaat vallen wordt waar mogelijk samengewerkt. Een voorbeeld hier van is de IT-infrastructuur die, gebruikt wordt voor het verwerken van cyberinformatie, in coproductie is ontwikkeld. Overlappende taken worden in goed overleg gedaan en waar mogelijk wordt er actief samengewerkt om incidenten op te lossen. Daarnaast is samenwerking essentieel om te kunnen waarborgen dat er altijd voldoende capaciteit is om cybersecurity incidenten op te kunnen pakken.

Met het NCSC als centraal publiek orgaan voor cybersecurity binnen Nederland, is samenwerking van groot belang. Zowel het NCSC als het CSIRT-DSP komt voort uit de Wbni-wetgeving[2], dat vergelijkbare taken en verantwoordelijkheden oplegt voor de eigen doelgroepen. Een voorbeeld van deze samenwerking is dat buiten kantoortijden het NCSC waakdiensten van het CSIRT-DSP overneemt en contact opneemt wanneer de urgentie daar is. Daarnaast wordt, om de samenwerking te versterken, actief gewerkt aan een (grotendeels) geautomatiseerde koppeling tussen de bronnen van het NCSC en de systemen van het CSIRT-DSP. Met deze koppeling zal de informatie uit deze bronnen nog sneller de doelgroepen bereiken. Hierover volgt binnenkort meer informatie. Deze samenwerkingen stelt het team van CSIRT-DSP in staat het dienstenpakket voor digitale dienstverleners uit te breiden en structureler relevante informatie te kunnen delen.

Samenwerking met Agentschap Telecom

Agentschap Telecom[3] is toezichthouder op de Wet beveiliging netwerk- en informatiesystemen (Wbni). Zowel aanbieders van essentiële diensten in de sectoren energie en digitale infrastructuur als digitale dienstverleners moeten aan deze wet voldoen. Digitale dienstverleners moeten passende maatregelen nemen om incidenten te voorkomen en incidenten met aanzienlijke gevolgen melden bij Agentschap Telecom en het CSIRT-DSP.

De EU heeft gekozen voor ex-post toezicht op digitale dienstverleners. Dit betekent dat Agentschap Telecom enkel onderzoeken kan uitvoeren nadat er een incidentmelding is binnengekomen of wanneer er signalen zijn dat een digitale dienstverlener tekort schiet in zijn zorgplicht. Een onderzoek leidt niet per definitie tot handhaving of een sanctie, Agentschap Telecom is een toezichthouder die bij incidenten onderzoekt waar zaken zijn misgegaan en digitale dienstverleners hiermee inzicht geeft in wat er verbeterd moet worden om deze incidenten in de toekomst te voorkomen.

Om meer inzicht te krijgen in generieke kwetsbaarheden binnen de digitale dienstverlener sector is informatie vanuit het CSIRT-DSP over dreigingen en ontwikkelingen zeer nuttig voor Agentschap Telecom. Ook helpt het dat het CSIRT-DSP digitale dienstverleners bij incidentmeldingen erop wijst dat incidenten met aanzienlijke gevolgen gemeld dienen te worden aan Agentschap Telecom. Voor het CSIRT-DSP is het ook zeer nuttig om informatie te ontvangen die voortkomt uit de incidentinspecties van Agentschap Telecom, dit geeft aanvullende informatie over de oorzaken van incidenten bij digitale dienstverleners. Voor zowel Agentschap Telecom als het CSIRT-DSP is deze samenwerking zeer waardevol.

Sinds begin 2020 is er regelmatig overleg tussen CSIRT-DSP en Agentschap Telecom om elkaar op de hoogte houden van relevante ontwikkelingen in deze sector. Hierbij delen we geen details over specifieke incidenten of herleidbare informatie met elkaar, omdat digitale dienstverleners incidenten in vertrouwen moeten kunnen melden bij het CSIRT-DSP en bij Agentschap Telecom.

Agentschap Telecom en het CSIRT-DSP hebben verschillende taken ten aanzien van digitale dienstverleners maar wel met een gemeenschappelijk doel: Het versterken van de digitale weerbaarheid van digitale dienstverleners.

[1] https://www.ncsc.nl/documenten/publicaties/2021/maart/29/handreiking-okttt

[2] https://wetten.overheid.nl/BWBR0041515/2021-08-01

[3] https://www.agentschaptelecom.nl/

ISIDOORIII Cyberoefening

In 2021 was het dan eindelijk zover. De grootschalige cyberoefening ISIDOOR(III) stond van origine gepland in 2020, maar vanwege de COVID-19 pandemie is deze uiteindelijk verplaatst naar 2021. De 3-dagen durende oefeningen creëert een nationale (cyber)crisis, waarbij betrokken partijen het hoofd boven water moeten houden en procedures en handboeken voor een crisissituatie kunnen testen. Met 96 deelnemende organisaties kan er dan ook echt worden gesproken van een grootschalige oefening.[4]

Ook digitale dienstverleners waren namelijk tijdens deze oefening 'getroffen' door een cybersecurity incident. Een uitdagende situatie waarbij de ernst van het incident werd onderschat door de fictieve digitale dienstverlener, het incident werd gemeld door een medewerker maar de CEO wilde niet meewerken aan het inzichtelijk maken van het incident. Omdat de CEO het onderzoek van het CSIRT-DSP actief tegenwerkte, kon de hulpverlenende taak niet worden uitgevoerd. Dit leidde er uiteindelijk toe dat het Agentschap Telecom toezichthoudend heeft opgetreden richting deze fictieve digitale dienstverlener.

Hoewel het CSIRT-DSP en het Agentschap Telecom rond incidenten een strikt gescheiden rol hebben, kan er vanuit het CSIRT-DSP contact worden gezocht met het Agentschap Telecom indien er wordt geconstateerd dat een digitale dienstverlener de adviezen van het CSIRT-DSP moedwillig niet of onvoldoende opvolgt.
Een goede test of onze protocollen ook aansluiten op dergelijk voorkomende situaties. Binnen het ministerie werd de interne opschaling en crisisstructuur van EZK geoefend en op de proef gesteld. Zowel het CSIRT-DSP als het overkoepelende ministerie EZK maken deel uit van het Nationaal Crisisplan Digitaal.[5]

Door deelnemende digitale dienstverleners is ook het incident meldproces bij het CSIRT-DSP getest, waarbij er de gelegenheid is geweest voor DSP's om te testen hoe dit meldproces in zijn werk gaat en naar wat voor gegevens we op zoek zijn bij een incident melding. Vanuit de oefening zijn verschillende evaluatiepunten naar voren gekomen voor het CSIRT-DSP. Er is geadviseerd om het Nationaal Crisisplan Digitaal aan te passen om de rol van het CSIRT-DSP te verduidelijken en te versterken, zodat deze meer in lijn staat met de werkzaamheden van het CSIRT-DSP. Ook wordt er gewerkt aan het beter en sneller kunnen schalen van (menselijke) capaciteit.

NIB2-richtlijn aankondiging

De Europese Netwerk en Informatiebeveiliging-richtlijn 1 (NIB1[6]) dateert uit 2016. Uit deze richtlijn is in mei 2018 de Wet Beveiliging Netwerk- en Informatiesystemen[7] voortgekomen. Het CSIRT-DSP en het NCSC voeren haar wettelijke taak uit vanuit deze wetgeving. Door het veranderende cyber landschap is de huidige richtlijn volgens de EU commissie alweer toe aan vervanging. Zodoende wordt er gewerkt aan de NIB2-richtlijn[8]. Een nieuwe richtlijn die meer aandacht heeft voor bijvoorbeeld de supply chain, nieuwe sectoren zoals datacenters en meer harmonisatie tussen de lidstaten. Uiteindelijk zal de aangenomen NIB2-richtlijn moeten worden omgezet in Nederlandse wetgeving. Het voorstel voor de NIB2-richtlijn is eind 2020 gepubliceerd door de commissie.
In 2021 is er een publieke consultatie geweest, waarbij organisaties en personen de mogelijkheid hebben gekregen om feedback te geven op het voorstel. Verder is er veel onderhandeld wat heeft geresulteerd in een aantal aanpassingen op het voorstel. Zo wordt er mede door de grootte, omzet en balans van een organisatie bepaald of deze als essentiële of belangrijke organisatie wordt aangemerkt of dat de organisatie buiten de richtlijn valt.
Het traject is nog niet helemaal rond en de volgende stap is een zogenoemd triloog[9]. Als dit is afgerond en de richtlijn is aangenomen volgt nog een periode om de richtlijn om te zetten in nationale wetgeving.

Het is op dit moment dan ook nog niet duidelijk hoe de NIB2-richtlijn vorm gaat worden gegeven in Nederland. Zodra dit concreter is, zal het CSIRT-DSP u hier over informeren.

[4] https://www.ncsc.nl/actueel/nieuws/2021/juni/10/isidoor-2021-nctv-en-ncsc-organiseren-grootste-cybercrisisoefening-ooit

[5] https://www.nctv.nl/documenten/publicaties/2020/02/21/nctv-nationaal-crisisplan-digitaal-_-webversie

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[7] https://wetten.overheid.nl/BWBR0041515/2021-08-01

[8] https://www.consilium.europa.eu/en/press/press-releases/2021/12/03/strengthening-eu-wide-cybersecurity-and-resilience-council-agrees-its-position/

[9] https://www.europa-nu.nl/id/vhczmr1tlyxw/triloog

Cases 2021

Webshells en nog meer webshells – Hoe een Exchange kwetsbaarheid de wereld op zijn kop zette

Er zijn weinig organisaties die geen gebruik maken van Microsoft Exchange of Microsoft 365. In maart 2021 werd de wereld opgeschrikt met een serie ernstige kwetsbaarheden in Microsoft Exchange waar al maanden door de Hafnium groep[10] misbruik van werd gemaakt. Hoewel Hafnium misbruik maakte van deze kwetsbaarheden voor spionage doeleinden, werd er na bekendheid van de kwetsbaarheden in zeer rap tempo misbruik gemaakt van deze kwetsbaarheden door ook andere kwaadwillende actoren[11].

Het misbruik gebeurde zo snel, dat de dag na de publicatie van de kwetsbaarheden het mogelijk al te laat was. Zo werd er al vanaf de vroege ochtend misbruik geconstateerd. Hierbij werd het internet gescand door kwaadwillende actoren met het einddoel Exchange servers te identificeren. Bij de identificatie van een kwetsbare Exchange server werd er een webshell[12] geplaatst. Een achterdeurtje in Microsoft Exchange die op een later moment kon worden benut om malware te downloaden of gevoelige informatie te bemachtigen.

Het bleek al snel om een serieus aantal besmette systemen te gaan[13], niet alleen in Nederland, maar wereldwijd[14]. Vrijwel elke organisatie die iets met cybersecurity doet zat er bovenop, welke webshells waren er geplaatst op de kwetsbare systemen, welke groeperingen zaten hierachter en wat waren de gevolgen hiervan. Hoe konden organisaties hiertegen beschermd worden? Het duurde dan ook niet lang voordat de eerste lijsten met kwetsbare systemen bij het CSIRT-DSP werden aangeleverd. Een korte periode van informeren ging voornamelijk om het informeren over kwetsbare systemen en het controleren op misbruik van kwetsbare systemen. Vanwege het snelle en grootschalige misbruik sloeg de informatie al snel over naar gecompromitteerde systemen, met daarin concretere informatie welke webshells er gedetecteerd waren op een kwetsbare server.

Ook organisaties die dachten op tijd te hebben geüpdatet kwamen er achter dat systemen alsnog gecompromitteerd waren, met alle gevolgen van dien. Van het uitrollen van ransomware, tot het stelen van contactgegevens, het misbruik varieerde enorm en de hoeveelheid getroffen organisaties zorgde voor een internationale druk op incident response partijen en nationale CSIRTs.

Na enkele dagen sloeg het advies dan ook om, van controleren op misbruik naar ga uit van misbruik, controleer of er al pogingen zijn door kwaadwillende actoren om zich in het netwerk te verspreiden, schakel waar nodig tijdelijk de Exchange server uit.
Het CSIRT-DSP heeft hierbij veel geïnformeerd over kwetsbare systemen, maar ook organisaties geadviseerd die reeds misbruik hadden geconstateerd. Er zijn Exchange servers gezien die tot wel 32 individuele webshells hadden, wat serieuze consequenties had voor het onderliggende bedrijf. Verschillende organisaties zijn ook getroffen door ransomware.

Enkele maanden later was het weer raak, met een nieuwe serie aan ernstige kwetsbaarheden in Exchange[15]. Hoewel hier minder media aandacht voor is geweest, had zich ook met deze kwetsbaarheden een (stille) ramp voltrokken, waarbij veel organisaties slachtoffer waren. Ook bij deze kwetsbaarheden werd er een webshell geplaatst om vervolgens willekeurige code uit te voeren, met wederom een divers aantal vormen van misbruik.
Wederom een zorgwekkende situatie waarbij er gelukkig door genoeg organisaties tijdig en alert gehandeld werd.

Nog steeds ontvangt het CSIRT-DSP regelmatig lijsten met kwetsbare Exchange systemen, die soms maandenlang niet zijn geüpdatet, waardoor misbruik gemakkelijk wordt gemaakt.
Van Exchange misbruik hebben we zeker het laatste nog niet gezien.

Fysieke beveiliging

Een software kwetsbaarheid die zorgt voor een gat in de fysieke beveiliging. Die zien wij niet heel vaak voorbij komen. Toch werd het CSIRT-DSP in april dit jaar geattendeerd op een ernstige kwetsbaarheid die nog wel eens enkele (klant-)organisaties van onze doelgroep kon treffen. Een ernstige kwetsbaarheid in ABUS Secvest alarmsystemen[16]. Een systeem waarbij het voor te stellen is dat deze nog wel eens wordt vergeten met de patchrondes. Misbruik van deze kwetsbaarheid laat een kwaadwillende toe het alarmsysteem uit te schakelen, waardoor een fysieke inbraak gemakkelijker wordt gemaakt. Toch wel vervelend als het alarmsysteem even op afstand wordt uitgeschakeld.

Uit onderzoek van Eye Security bleek dat, hoewel de kwetsbaarheid al uit 2020 was, 90% van de via internet gevonden systemen nog steeds kwetsbaar was[17]. Een zorgwekkend aantal met duizenden kwetsbare systemen binnen Europa. Het blijft dan ook van belang dat organisaties die dergelijke onderzoeken uitvoeren nationale CERT's of andere relevante instanties weten te vinden

[10] https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Hafnium&n=1

[11] https://www.ncsc.nl/actueel/nieuws/2021/maart/4/kwetsbaarheden-in-microsoft-exchange-server-in-nederland-actief-misbruikt

[12] https://en.wikipedia.org/wiki/Web_shell

[13] https://www.ncsc.nl/actueel/nieuws/2021/maart/16/schade-microsoft-exchange

[14] https://www.shadowserver.org/news/shadowserver-special-reports-exchange-scanning-4/

[15] https://www.rapid7.com/blog/post/2021/08/12/proxyshell-more-widespread-exploitation-of-microsoft-exchange-servers/

[16] https://www.abus.com/nl/Huisbeveiliging/Alarminstallatie/Secvest-draadloze-alarminstallatie/Draadloze-alarmcentrale-sets/Secvest-Draadloze-Alarmcentrale

[17] https://eye.security/nl/blog/breaking-abus-secvest-internet-connected-alarm-systems-cve-2020-28973

en benaderen, zodat er waar nodig geassisteerd kan worden met het informeren van organisaties over deze kwetsbaarheid.

Jaaroverzicht 2021 en vooruitblik 2022

Om de werkzaamheden van het CSIRT-DSP allemaal nog even op een rijtje te zetten kunnen er geen statistieken ontbreken. In 2021 heeft het CSIRT-DSP meer focus gelegd op het in contact komen met de verschillende digitale dienstverleners binnen Nederland. Dit in combinatie met het toenemende aantal incidenten en kwetsbaarheden die behandeld worden zorgt voor een sterke stijging van verwerkte informatie. In de bijgaande tabel zijn de belangrijkste cijfers van de afgelopen twee jaar opgenomen.

Tabel 1 *Overzicht vergelijking statistieken 2020 en 2021*

Overzicht	2020	2021
Behandelde casussen	46	62
Incidenten met meldplicht binnen Nederland	0	1
Incidenten met meldplicht vanuit EU	2	3
Totaal aantal systemen waarover is geïnformeerd	n/a	5746
Operationele doelgroep berichten	0	13
Aantal digitale dienstverleners bereikt	120+	280+

In 2019 heeft het CSIRT-DSP 6 casussen behandeld (een casus kan een incident melding zijn waarbij ondersteuning is verleend of dreigingsinformatie betreffen waar naar is gehandeld). In 2020 steeg dit aantal al naar 46 casussen en voor 2021 staat dit aantal op 62. Dit betreft een stijging van 35% ten opzichte van 2020. De verwachting is door de toenemende automatisering en het aansluiten van meer bronnen dat deze aantallen ook in 2022 zullen stijgen. Ook lijken digitale dienstverleners het CSIRT-DSP beter te kunnen vinden, waardoor de verwachting is dat het aantal vrijwillige meldingen ook zal stijgen.

Van deze casussen betrof dit één incident met meldplicht[18] binnen Nederland en drie incidenten met meldplicht die zijn binnengekomen vanuit een ander EU-lidstaat. In 2020 betrof dit twee incidenten met meldplicht die zijn binnengekomen vanuit een ander EU-lidstaat en geen incidenten met meldplicht binnen Nederland. Vanwege de hoge drempelwaarden voor een incident met meldplicht is het niet de verwachting dat in 2022 dit aantal veel zal stijgen.

Er is in 2021 door het CSIRT-DSP over 5.746 (mogelijk) kwetsbare of gecompromitteerde systemen (IP-adressen) geïnformeerd richting in onze doelgroep. Daarnaast is er ook verschillende beschikbare informatie verstrekt aan het EU CSIRTs Network[19], het NCSC en het Digital Trust Center. De verwachting is dat dit aantal stijgt in 2022, mede omdat er meer bronnen worden aangesloten bij het CSIRT-DSP.

Het CSIRT-DSP is in 2021 gestart met het bij ernstige kwetsbaarheden en dreigingen een operationeel doelgroep bericht uit te sturen. Dit heeft het CSIRT-DSP in 2021 dertien keer gedaan en bereikt daar inmiddels meer dan 280 digitale dienstverleners mee. Met het toenemende aantal kritieke kwetsbaarheden zal dit in 2022 waarschijnlijk vaker worden benut. Het doel voor 2022 blijft om met meer digitale dienstverleners in contact te komen.

Voor 2022 wordt er naast het werken aan de uitbreiding van dreigingsinformatie en het aantal digitale dienstverleners wat we bereiken ook gewerkt aan het opzetten van een chatplatform voor digitale dienstverleners, het opzetten van een ISAC[20] en best practices en factsheets.

[18] https://csirtdsp.nl/meldplicht

[19] https://csirtsnetwork.eu/

[20] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/start-een-isac

Dit jaarbericht is een uitgave van:

Ministerie van Economische Zaken en Klimaat
Bezuidenhoutseweg 73 | 2594 AC Den Haag
Postbus 20401 | 2500 EK Den Haag

csirt@csirtdsp.nl | https://www.csirtdsp.nl

Januari 2022 | Publicatie-nr. 0122-014