Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Delen van Incidentmeldingen van en naar het NCSC

Publicatiedatum: 31-7-2025

TLP:CLEAR

Versie 1.0

Toegestane verspreiding van
TLP: CLEAR (Traffic Light Protocol)

Dit NCSC rapport bevat het label TLP:AMBER+STRICT en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet je met wie je deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Als u dit rapport wilt delen buiten uw eigen organisatie, neem dan contact op met het NCSC.

Inhoudsopgave

Managementsamenvatting

Incidentinformatie is een belangrijke schakel in het Nederlandse systeem van informatiedeling rondom cyberdreigingen. Tijdige en gedetailleerde informatie over een geslaagde of mislukte cyberaanval is zeer nuttige informatie voor Nederlandse organisaties om zich te wapenen tegen een nieuwe aanval. In de Toekomstvisie van het Cyberweerbaarheidsnetwerk (CWN) van 2024 is nadrukkelijk de behoefte opgenomen om in het netwerk tijdig incidentinformatie met de participanten te delen.[1] Ook het rapport over Cyclotron van 2022 stelt dat incidentinformatie onvoldoende en niet tijdig wordt gedeeld.[2]

Het onderzoek

Voor het onderzoek voerden we een korte literatuurstudie uit om inzicht te krijgen in de meest recente ontwikkelingen op onderzoeksgebied naar het doen van meldingen binnen organisaties. Opvolgend voerden we semigestructureerde interviews aan de hand van een lijst met interviewvragen met respondenten die vallen onder de Wet Beveiliging Netwerken en informatiesystemen (Wbni) en de aankomende Cyberbeveiligingswet (Cbw).[3] We hebben met 7 verschillende organisaties interviews gehouden en de interviews vervolgens getranscribeerd en geanalyseerd

Resultaten

Als eerste stap hebben we verschillende rapporten en onderzoeken bestudeerd over de behoeften rondom informatiedeling van incidenten en de situatie van incidentinformatie binnen het NCSC. Vervolgens hebben wij gekeken naar de mogelijkheden om incidentinformatie te melden bij het NCSC (zie **Error! Reference source not found.**). Uit de analyse concluderen wij dat er veel verschillende kanalen zijn om incidentinformatie bij het NCSC aan te leveren**.**

Uit de zeven gevoerde interviews geven de organisaties aan tevreden te zijn over de mogelijkheden om incidentinformatie met het NCSC te delen. Doelgroeporganisaties die meldingen onder de WBNI hebben gedaan waren tevreden over het proces.

Bijna alle geïnterviewde organisaties maken gebruik van een intern of extern SOC. Een van de diensten van het SOC is de eerste triage van incidenten die vervolgens met de securityteam(s) van de organisatie worden gedeeld. Voor de aggregatie van incidenten zou de verzameling van

[1] NCTV, Het Cyberweerbaarheidsnetwerk: Toekomstvisie voor het verbeteren van publiek-private samenwerking t.b.v. het verhogen van de cyberweerbaarheid van organisaties, 2024

[2] Oldegarm, Mooy, CYCLOTRON: Gezamenlijk sneller en gerichter delen van informatie rondom (dreigende) cyberincidenten in publiek-privaat verband, 2022

[3] De interviewvragen zijn opgenomen in Appendix A

kleine incidenten ook een zeer relevante informatiebron zijn. Hiervan kan geleerd worden van rapportagesystemen van veiligheidsincidenten waar een grote hoeveelheid van incidenten wordt verzameld en geanalyseerd.

Organisaties die al onder de WBNI vallen zijn goed op de hoogte van de sectorale drempelwaarden die verplichte meldingen vereisen bij incidenten. Verschillende organisaties hebben tot op zekere hoogte de WBNI-drempelwaarden opgenomen in hun incidentmanagementproces door de drempelwaarden intern te communiceren binnen de securityteams.

Het is niet voor alle doelgroeporganisaties duidelijk wat de informatiebehoefte is van het NCSC m.b.t. incidenten. Voor incidenten die buiten de meldplicht vallen is het voor doelgroeporganisaties in het bijzonder onduidelijk wanneer en wat zij kunnen delen met het NCSC. Duidelijke richtlijnen en criteria voor vrijwillige meldingen kunnen helpen informatiedelen te promoten.

Aanbevelingen

Aan de hand van het bovenstaande onderzoek doen wij de volgende aanbevelingen aan het NCSC om de stroom van incidentinformatie te verbeteren. Deze aanbevelingen wordenin het hoofdstuk *Aanbevelingen* verder toegelicht.

1. Zorg voor een product waar kwantitatieve incidentinformatie gedeeld kan worden.
2. Zorg voor producten met informatie over behoeften van NCSC voor incidentinformatie.
3. Zorg voor een periodieke communicatiestrategie voor incidentinformatie.
4. Zorg voor eenvoudige meldsystemen van kleinere incidenten bij SOC

Introductie

Incidentinformatie is een belangrijke schakel in het Nederlandse systeem van informatiedeling rondom cyberdreigingen. Tijdige en gedetailleerde informatie over een geslaagde of mislukte cyberaanval is zeer nuttige informatie voor Nederlandse organisaties om zich te wapenen tegen een nieuwe aanval. Onder de NIS1 die in Nederland in 2019 is ingegaan onder de naam *Wet beveiliging netwerk- en informatiesystemen* (WBNI) moeten organisaties incidenten melden wanneer er "aanzienlijke gevolgen" zijn voor de verleende dienst. Om vast te stellen of een incident aanzienlijke gevolgen heeft, zijn er door de lidstaten op verschillende wijzen sectorale drempelwaarden opgesteld die bij overschrijding verplichten dat een incident gemeld wordt. Gezien de gevoeligheid van informatie die een incidentmelding kan bevatten worden incidentmeldingen onder strikte vertrouwelijkheid gemaakt bij de aangewezen autoriteit.

Het doel van incidentmelding, zoals beschreven in de memorie van toelichting van de WBNI, is "*om risico's tijdig te kunnen inschatten en te helpen bij het duiden van de aard en de ernst van de melding, mede met het oog op mogelijke gevolgen voor andere Aanbieders van Essentiele Diensten (AED's) en andere vitale sectoren in Nederland (en daarbuiten).*"[4] De WBNI-melding is bedoeld als instrument om tijdig informatie over ernstige incidenten te kunnen verzamelen.

Onder de NIS2 wordt het aantal organisaties dat onder wetgeving valt sterk uitgebreid. Voor veel organisaties die hiervoor niet onder de Wbni vallen, wordt voor het eerst gevraagd serieus naar hun informatiebeveiliging te kijken. Organisaties die onder de NIS2 vallen hebben verschillende verplichtingen. Er is bijvoorbeeld een zorgplicht waarvoor organisaties op verschillende onderwerpen, zoals de beveiliging van informatiesystemen en bedrijfscontinuïteit en risicomanagement adequaat beleid en maatregelen moeten treffen.[5]

Een van de nieuwe regels waarmee bedrijven te maken krijgen is het rapporteren van incidenten. Zo moet er in het geval van een 'significant incident' een melding worden gemaakt bij de nationale autoriteit. Volgens artikel 23 van de NIS2 moet een incident gemeld worden wanneer het "*een ernstige verstoring van de bedrijfsvoering van de diensten of financiële schade voor de betrokken entiteit veroorzaakt of kan veroorzaken*" en/of "*het andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken*."[6]

Een incident melden blijft voor een belangrijk deel afhankelijk van proactief handelen vanuit de organisatie. Uit verschillende studies blijkt dat organisaties terughoudend zijn om incidentinformatie te delen. Het doen van een incidentmelding kost een organisatie middelen, tijd

[4] Wet beveiliging netwerk- en informatiesystemen (34.883); Memorie van toelichting (TK, 3) - Eerste Kamer der Staten-Generaal

[5] Zorgplicht, ncsc.nl

[6] Article 23 - Reporting obligations - NIS2 Directive (nis2-info.eu)

en mogelijk reputatieschade en een boete. Er zijn daardoor mogelijk verschillende afwegingen die organisaties maken in het wel of niet doen van een melding en de manieren waarop zij dit doen.[7][8][9]

Gezien de doorontwikkeling van het CWN en de behoeften om via het CWN tijdig kwalitatief hoogwaardige incidentinformatie met de achterban te delen, is het zeer relevant voor het NCSC om inzicht te hebben in de houding van organisaties aangaande incidentmeldingen. Deze inzichten bieden mogelijk verbeteringen in het delen van belangrijke informatie over aanvalsmethoden en impact die een melding kan bevatten. In het Toekomstvisie Cyberweerbaarheidsnetwerk (CWN) van 2024 is nadrukkelijk de behoefte opgenomen om in het netwerk tijdig incidentinformatie met de participanten te delen.[10] Het rapport Cyclotron van 2022 stelt dat incidentinformatie onvoldoende en niet tijdig wordt gedeeld.[11]

In opdracht van *Team Relatiemanagement* en *Team Melden en Registeren* van het NCSC heeft *Team Onderzoek* gekeken naar de mogelijkheden van doelgroepen om incidenten bij het NCSC te melden en wat de ervaringen van doelgroeporganisaties zijn met het melden van incidenten.

We beantwoordden de volgende onderzoeksvraag, *Welke factoren beïnvloeden de beslissing van organisaties om een cyberincident te melden bij het NCSC?*

We keken voor het beantwoorden van de hoofdvraag naar de volgende subvragen:

1. Welke mogelijkheden zijn er voor een organisatie om een incident te melden?
2. Hoeveel en welke typen cyberincidenten worden wel of niet gemeld bij het NCSC?
3. Welke interne overwegingen en processen spelen een rol bij de beslissing om een cyberincident te melden?
4. Welke verwachtingen hebben organisaties over de opvolging en terugkoppeling van incidentmeldingen?

Literatuur

Nederlandse initiatieven voor het delen van incidenten

[7] Busetti, Scanni, Evaluating incident reporting in cybersecurity. From threat detection to policy learning, 2024

[8] Patterson, et al. I don't think we're there yet": The practices and challenges of organisational learning from cyber security incidents Factors Affecting Reputational Damage to Organisations Due to Cyberattacks, 2024

[9] ENISA, Security incidents indicators - measuring the impact of incidents affecting electronic communications, 2016

[10] NCTV, Het Cyberweerbaarheidsnetwerk: Toekomstvisie voor het verbeteren van publiek-private samenwerking t.b.v. het verhogen van de cyberweerbaarheid van organisaties, 2024

[11] Oldegarm, Mooy, CYCLOTRON: Gezamenlijk sneller en gerichter delen van informatie rondom (dreigende) cyberincidenten in publiek-privaat verband, 2022

Het delen van incidentinformatie is al langere tijd een speerpunt voor de Nederlandse overheid. De wens om op een tijdige wijze informatie van incident te delen is een van de fundamenten onder de Nederlandse *Information Sharing and Analysis Centers* (ISACs), opgericht in 2006 en het delen van informatie over incidenten en dreigingen is een van de kerntaken van het NCSC.

In de WBNI zijn eisen vastgelegd wat organisaties moeten delen met de overheid in het geval van een significant incident. Zo is in de wet vastgelegd dat organisaties verplicht zijn de aard en omvang, het (vermoedelijke) tijdstip, de mogelijke gevolgen voor Nederland en een prognose van de hersteltijd te melden bij de verantwoordelijke toezichthouder en het NCSC.[12]

In het jaarlijkse Cybersecurity Beeld Nederland, dat wordt uitgegeven door het Ministerie van Justitie en Veiligheid, worden het aantal verplichte WBNI-meldingen door organisaties gepubliceerd. Sinds de invoering van de WBNI zijn er geen analyses of statistieken over dit type incidenten gepubliceerd in het CSBN.[13]

In 2022 publiceerde het Ministerie van Justitie en Veiligheid het rapport Cyclotron waarin knelpunten op het gebied van informatiedeling worden geïdentificeerd. Het rapport geeft aan dat operationele gegevens op een versnipperde manier worden uitgewisseld, tactische informatie niet voldoende gezamenlijk wordt geanalyseerd en dat het ontbreekt aan incidentregistratie en historische analyses.[14]

In 2024 publiceerde het Ministerie van Justitie en Veiligheid de Toekomstvisie CWN waar een nieuwe invulling wordt geschetst voor het bestaande Landelijk Dekkend Stelsel. Een van de behoeften voor het CWN is het tijdig delen van incidentinformatie binnen het netwerk. Het CWN moet een rol gaan spelen met zowel incidentafhandeling vlak na de gebeurtenis en het verspreiden van analyses over incidenten die hebben plaatsgevonden.[15]

In 2023 is het eerste rapport van het samenwerkingsverband Melissa gepubliceerd. Melissa is een publiek private samenwerking waar informatie over ransomware-incidenten in Nederland wordt geanalyseerd en modus operandi wordt gepubliceerd in een jaarbeeld. Eind 2024 werd een evaluatie van de samenwerking gepubliceerd. In de evaluatie wordt de samenwerking “waardevol” genoemd. En een “mooi fundament” voor het uitwisselen van incidentinformatie tussen verschillende organisaties in Nederland.[16]

Meldingen van cyberincidenten

[12] Wet beveiliging netwerk- en informatiesystemen: https://wetten.overheid.nl/BWBR0041515/2019-01-01

[13] Zie jaargangen CSBN 2020 tot 2024

[14] Oldegarm, Mooy, CYCLOTRON: Gezamenlijk sneller en gerichter delen van informatie rondom (dreigende) cyberincidenten in publiek-privaat verband, 2022

[15] NCTV, Het Cyberweerbaarheidsnetwerk: Toekomstvisie voor het verbeteren van publiek-private samenwerking t.b.v. het verhogen van de cyberweerbaarheid van organisaties, 2024

[16] Van den Berg et al., Samenwerken tegen Ransomware: Evaluatie Melissa, 2025

De literatuur over het melden van cyberincidenten is zeer klein, wat opmerkelijk is gezien het grote aantal cyberaanvallen waar organisaties mee te maken hebben. Er is een beperkt aantal academische papers over hoe organisaties omgaan met incidenten en hoe organisaties leren van incidenten.[17] Er bestaan ook een aantal papers gericht op het meldsysteem van de NIS. Daarnaast bestaan er een aantal grote nationale surveys waar is gekeken naar de status van cybersecurity bij bedrijven.

Er is literatuur over het melden van securityincidenten door individuen binnen een organisatie. Hoewel dit type meldingen niet een op een te extrapoleren is op het melden van incidenten door organisaties aan externe toezichthouders, zijn de afwegingen die individuen maken wel relevant voor dit onderzoek.

In de Cybersecurity Monitor van het CBS gaf in 2021 20% van bedrijven met meer dan 250 medewerkers aan te maken te hebben met een cyberincident met een externe oorzaak. Bij 8% van de deelnemende organisaties ging dit gepaard met kosten. De survey vroeg deelnemers niet hoe zij omgingen met een incident of hoe zij incidenten intern of extern meldden.[18]

Een grote survey van de Britse regering in 2023 onder meer dan 2000 bedrijven geeft aan dat van de ondervraagde bedrijven 26% richtlijnen heeft opgesteld voor het melden van een incident aan externe partijen. 21% heeft een incident response plan en 13% richtlijnen voor communicatie naar het publiek.[19]

Interviews met 34 security experts, uitgevoerd door Patterson et al., laten zien dat organisaties het delen van analyses van incidenten, met zowel toezichthouders als soortgelijke organisaties, ingewikkeld vinden vanwege de mogelijke wettelijke repercussies. De onderzoekers concluderen dat dwingende druk vanwege wetgeving bepalend is hoe er over incidenten gecommuniceerd wordt.[20]

Onderzoek naar factoren van reputatieschade toont aan dat gebrekkige communicatie naar het publiek een van de grotere negatieve factoren op de reputatie van bedrijven.[21] Duidelijk en open communiceren over een incident kan reputatieschade voorkomen of afzwakken. In Nederland zijn de Universiteit Maastricht en de gemeente Lochem voorbeelden van hoe open communicatie over het incident een belangrijke rol kan spelen in het voorkomen van reputatieschade.

Informatiedeling over dreigingen

[17] Patterson et al., Learning from cyber security incidents: A systematic review and future research agenda, 2024

[18] CBS Cybersecurity Monitor 2022, 2022

[19] NCSC UK, Cyber security breaches survey 2023, 2023

[20] Patterson, et al. I don't think we're there yet": The practices and challenges of organisational learning from cyber security incidents Factors Affecting Reputational Damage to Organisations Due to Cyberattacks, 2024

[21] Srinath Perera, X. J.-G,Factors Affecting Reputational Damage to Organisations Due to Cyberattacks. 2022. *Informatics*

Hoewel specifiek onderzoek naar meldingen van cyberincidenten gering is, is de hoeveelheid literatuur naar het delen van dreigingsinformatie uitgebreider. Dreigingsinformatie beschrijft verzamelde kennis, zoals context, methodieken, implicaties en handelingsperspectief over een bestaande of toekomstige dreiging.[22] In navolging van Ainsli definiëren we CTI als "*de kennis en het begrip van daadwerkelijke of vermeende bedreigingen die de besluitvorming van organisaties over beveiliging beïnvloeden*".

Er is een groeiende hoeveelheid literatuur over cyberaanvallen, informatie-uitwisseling en cyber threat intelligence. Hieronder vallen studies naar de fundamentele concepten van cyber threat intelligence, zoals de intelligence cycle, onderzoeken naar de effectiviteit van cyber intelligence-uitwisseling tussen groepen, en methoden en standaardisatie om taalbarrières bij informatie-uitwisseling te overwinnen.[23],[24] Theoretisch gezien wordt threat intelligence door organisaties gebruikt voor effectief situationeel bewustzijn, het inschatten van het risico op mogelijke aanvallen en het uitvoeren van strategische planning voor opkomende bedreigingen.[25]

In 2020 deed de Haagse Hogeschool in opdracht van het NCSC onderzoek naar succesfactoren voor informatie delen in een keten. Hieruit kwam naar voren dat vertrouwen de belangrijkste factor voor informatiedeling was. Op de tweede plaats stond expertise van de deelnemers.[26]

Een enquêteonderzoek van Oxford naar opvattingen van security experts over dreigingsinformatie heeft een aantal stellingen voorgelegd aan 67 deelnemers. De respondenten aan dat het delen van dreigingsinformatie bijdraagt aan inbraakdetectie en herstel. De op een na meest gewaardeerde stelling was dat het delen van dreigingsinformatie bijdraagt aan irrelevante informatie. Volgens de deelnemers is dreigingsinformatie alleen bruikbaar mits deze tijdig wordt gedeeld en opties geeft om te handelen.[27]

Een enquête van MIT onder 25 security experts over de motivaties en barrières om informatie te delen laat zien dat de meeste deelnemers wettelijke obstakels als belangrijkste barrière zien, gevolgd door technologische obstakels.

Methode

Om de onderzoekvragen te beantwoorden hebben we gekozen voor een aantal methoden om zicht te krijgen op het ecosysteem rondom het NCSC over cyberincidentmeldingen. Wij hebben gekeken naar de ontvangst van incidentmeldingen, de registratie en duiding binnen het NCSC en de

[22] Wagner et al., Cyber Threat Intelligence Sharing: Survey and Research Directions, 2019

[23] Scott Ainsli, D. T. Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security*, 2023

[24] Wagner et al., Cyber Threat Intelligence Sharing: Survey and Research Directions, 2019

[25] Kayode-Ajala, O. Applications of Cyber Threat Intelligence (CTI) in Financial Institutions and Challenges in Adoption. 2023

[26] Bakkers et al, Verkenning best practices informatiedeling, 2020

[27] Zibak, Cyber Threat Information Sharing: Perceived Benefits and Barriers, 2019

communicatie naar de doelgroeporganisaties van het NCSC om zo een beter begrip te krijgen voor de wisselwerking en stroom van informatie in het ecosysteem.

Voor het onderzoek voerden we een korte literatuurstudie uit om inzicht te krijgen in de meest recente ontwikkelingen op onderzoeksgebied naar het doen van meldingen binnen organisaties. De bevindingen van de literatuurstudie zijn hierboven gedeeld.

Om zicht te krijgen op de informatiestroom over incidentmeldingen bestudeerden wij documenten en processen omschreven binnen het NCSC. Hiervoor keken wij naar de systemen en processen die betrokken zijn bij de ontvangst, registratie en delen van informatie over cyberincidenten.

Opvolgend voerden we semigestructureerde interviews aan de hand van een lijst met interviewvragen met respondenten die vallen onder de WBNI en de aankomende NIS2 wetgeving.[28] We hebben met 7 verschillende organisaties interviews gehouden en de interviews vervolgens getranscribeerd en geanalyseerd.

Resultaten

In dit hoofdstuk worden per onderdeel van het onderzoek de belangrijkste resultaten beschreven. We beginnen met een analyse van de informatiestroom van incidentinformatie binnen het NCSC. Vervolgens beschrijven wij de bevindingen uit de interviews met de doelgroeporganisaties.

[28] De interviewvragen zijn opgenomen in Appendix A

Als eerste stap probeerden we de vraag te beantwoorden, **welke mogelijkheden zijn er voor een organisatie om een incident te melden?** Het NCSC ontvangt uit een groot aantal bronnen meldingen over (mogelijke) incidenten in Nederland en in het buitenland. Hieronder staan een aantal van de kanalen beschreven waar organisaties incidentinformatie met het NCSC kunnen delen. In deze lijst probeerden wij zo volledig mogelijk te zijn. In ***Error! Reference source not found.*** hebben we een overzicht van de incidentinformatie geschetst.

Voor dit onderzoek hebben we interne documenten bestudeerd over de kanalen met betrekking tot incidentmeldingen.

Het NCSC hanteert voor de meldplicht de definities voor cyberincidenten zoals omschreven in de WBNI en binnenkort de CBW. Er geldt een meldplicht voor *'significante incidenten'*. Dit zijn incidenten die een ernstige operationele verstoring van de diensten of financiële verliezen voor de organisatie (kunnen) veroorzaken.

Echter, het NCSC ontvangt ook nog vele andere meldingen die als incidentmelding gedefinieerd kunnen worden. We hanteren de definitie van cyberincident gegeven door NIST om te achterhalen welke informatie als incidentmelding geclassificeerd kan worden. Een *incidentmelding* is het verstrekken van informatie over:

- Een cybersecuritygebeurtenis die gevolgen heeft voor een organisatie en een reactie en herstel vereist.
- Een afwijkende of onverwachte gebeurtenis tijdens de levenscyclus van een project, product, service of systeem.
- Een gebeurtenis die de vertrouwelijkheid, integriteit of beschikbaarheid van een informatiesysteem in gevaar brengt of in strijd is met het beveiligingsbeleid.[29]

Om meer zicht te krijgen op de meldprocessen van doelgroeporganisaties richting het NCSC hebben wij gekeken naar de mogelijkheden van doelgroepen om incidenten bij het NCSC te melden en wat de ervaringen van doelgroeporganisaties zijn met het melden van incidenten.

Kanalen voor meldingen richting het NCSC

Figuur 1: Kanalen voor meldingen richting het NCSC

[29] https://csrc.nist.gov/glossary/term/incident

- WBNI-melding MijnNCSC: Via MijnNCSC kunnen doelgroepen een verplichte of vrijwillige melding doen over een incident. Voor het doen van een melding wordt een webformulier ingevuld over onder andere het type en de impact van het incident. Op dit moment is alleen een vrijwillige melding beschikbaar.
- WBNI-melding Telefonisch: Via het KCC kunnen organisaties telefonisch een incident melden.
- WBNI-melding via Mail: Via de mail cert@ncsc.nl of info@ncsc.nl kunnen organisaties een incident melden. Wanneer dit een melding onder de WBNI betreft maken zij gebruik van het meldformulier. Hierbij moet worden opgemerkt dat de velden het meldformulier *NCSC Melding WBNI* niet precies overeenkomen met de velden op het webformulier van MijnNCSC.

- Rondje Rood in ISAC: De periodieke ISAC-bijeenkomsten hebben regelmatig een Rondje Rood waar ISAC leden onder TLP-RED protocol informatie delen. In onderdeel worden ook incidenten besproken door deelnemers die niet verder worden gedeeld.
- Informeel gesprek met NCSCer: Medewerkers van doelgroeporganisaties spreken regelmatig NCSC-collega's. Hier wordt in sommige gevallen ook op informele wijze informatie over incidenten met NCSC'ers gedeeld.
- Bericht in Mattermost NCSC: Het NCSC beheert een afgesloten Mattermost kanaal met een groot aantal verschillende organisaties. Mogelijk wordt ook hier informatie over incidenten met elkaar gedeeld op laagdrempelige manier. Wij hadden voor het onderzoek geen toegang tot het Mattermost kanaal. Echter uit de interviews kwam naar voren dat hier incidentmeldingen worden gemaakt.

Het perspectief van Doelgroeporganisaties

Om beter te begrijpen hoe de doelgroeporganisaties van het NCSC omgaan met incidenten, het melden van incidenten en het delen van informatie richting het NCSC zijn zeven interviews gehouden met doelgroeporganisaties. De interviews zijn getranscribeerd en vervolgens gecodeerd. Om een beter beeld te krijgen van de incidentmanagementprocessen van de organisaties gaan we eerst dieper in op verschillende stappen in dit proces. Vervolgens gaan we in op het beantwoorden van de onderzoeksvragen:

- Hoeveel en welke typen cyberincidenten worden wel of niet gemeld bij het NCSC?
- Welke interne overwegingen en processen spelen een rol bij de beslissing om een cyberincident te melden?

- Welke verwachtingen hebben organisaties over de opvolging en terugkoppeling van incidentmeldingen?

Geïnterviewde organisaties

Voor dit onderzoek hebben we gesproken met zeven organisaties uit verschillende sectoren. Zes van de organisaties vallen reeds onder de doelgroep van het NCSC, een organisatie is geen doelgroeporganisatie van het NCSC. We hebben gesproken met security officers en CISO's met uiteenlopende werkervaring bij hun organisaties en kennis van de processen op het gebied van incidentmanagement binnen de organisatie.

Tabel 1: Respondenten

Respondent	**Rol Respondent**	**Sector**	**NCSC Doelgroep**
1	CISO	Financien	Ja
2	Manager cybersecurity	Transport	Ja
3	Senior Information Security Officer	Transport	Ja
4	Security Officer	Drinkwater	Ja
5	Compliance Officer	Rijksoverheid	Ja
6	Information Security Officer	Rijksoverheid	Ja
7	CISO	Voedselproductie	Nee

Identificatie van incidenten

Opvallend is het geringe aantal noemenswaardige incidenten dat tijdens de interviews naar voren kwam. De geïnterviewde organisaties gaven aan dat er geen PRIO1-incidenten hebben plaatsgevonden in de afgelopen drie jaar. Twee partijen gaven aan dat zij in deze periode te maken hebben gekregen met incidenten die zij als PRIO2 inschaalden. Dit ging in een geval om een kwetsbaar edge device.

Uit de interviews bleek dat de ondervraagde organisaties allen een gestandaardiseerd incidentmanagementproces hebben ingericht om cybersecurity incidenten te definiëren. Incidenten worden geïdentificeerd aan de hand van meldingen uit het Security Operations Center (SOC), meldingen van medewerkers via een servicedesk, kwetsbaarhedeninformatie van de leveranciers of het NCSC. Alle organisatie hanteren een definitie voor cyberincidenten, al maken sommige organisaties geen onderscheid tussen cyberincidenten en andersoortige incidenten binnen de organisatie.

Alle organisaties nemen diensten af van een SOC. De helft van de organisaties heeft een eigen SOC en de andere helft neemt diensten af van een securitydienstverlener oftewel een 'extern' SOC. Voor dit onderzoek hebben we geen SOC-medewerkers geïnterviewd, maar uit de

gesprekken komt naar voren dat het SOC een belangrijke rol speelt in de initiële triage en afhandeling van (mogelijke) securityincidenten. SOC-medewerkers beoordelen het merendeel van de events voor de geïnterviewde organisaties.

Uit een onderzoek naar Zweedse security professionals komt naar voren dat kleinere organisaties met een extern SOC een informatieachterstand kunnen ervaren.[30] Dit sentiment komt niet uit de gevoerde interviews naar voren, maar er is niet expliciet gevraagd naar een eventuele informatieachterstand. Organisaties met een extern SOC gaven in de interviews wel aan geen incidentinformatie te missen.

Alle van de zeven geïnterviewde partijen geven aan dat zij gebruik maken van het ITIL incident management framework om incidenten op te delen in vier prioriteitscategorieën, van Prioriteit of PRIO 4, de laagste categorie tot PRIO 1, de hoogste categorie. ITIL heeft een afwegingskader met twee assen, impact van het incident en urgentie. Beide assen hebben vier categorieën van Laag tot Kritiek. Een incident met lage impact betreft een enkele gebruiker terwijl een kritiek incident een kern IT-service uitschakelt.[31] De inschatting van de categorie wordt gedaan door experts binnen de organisatie. De initiële triage ligt in veel gevallen bij het SOC maar de duiding wordt door een security officer of securityteam van de eigen organisatie gedaan.

Het ITIL-afwegingskader geldt voornamelijk voor incidenten met betrekking op IT-systemen. Organisaties die gebruik maken van OT-systemen hanteren daarvoor een afwijkende afweging die meer gebaseerd is op de inschatting van de expert.

Veel incidenten worden bij de initiële triage afgevangen en door SOC-medewerkers niet gedeeld met securityteams om de beperkte capaciteit niet aan onbelangrijke meldingen te verspillen.

In deze structuur proberen organisaties *alert fatigue* bij de securityteams te voorkomen. Pas bij incidenten die vanuit het SOC en/of de servicedesk relevant worden geacht voor het securityteam of de securityteams worden deze gedeeld. Opvallend lijkt hier een verschil te zijn tussen de interactie van interne SOCs en externe SOCs.

The ITIL Incident Management Priority Matrix

Priority Matrix					
		Impact			
		Critical	High	Medium	Low
Urgency	Critical	1	1	2	3
	High	1	2	3	3
	Medium	2	3	3	4
	Low	3	3	4	5

Figuur 2: ITIL Incident Management Matrix

Een respondent gaf aan dat het externe SOC weinig kennis had over de organisatie en er goed gekeken moest worden door de manager of de incidentclassificatie klopte. Een andere respondent gaf aan dat hun interne SOC juist veel autonomie had in het communiceren van oplossingen

[30] Mis een bron.

[31] Buildahelpdesk.com, ITIL Incident Management Priority Matrix, 2022

richting teams binnen de organisatie. Dit SOC heeft ook het mandaat om systemen uit te schakelen om cascade effecten binnen de organisatie te voorkomen.

Afhandeling & Evaluatie van Incidenten

Alle geïnterviewde organisaties gaven aan dat zij een vorm van een incident response plan hebben om op incidenten te reageren. De invulling van het incident response plan verschilt wel erg per organisatie. Een organisatie gaf aan dat zij bezig zijn met delen van response op incidenten te automatiseren op basis van playbooks. Incidentmeldingen worden via de MITRE-taxonomie gelabeld en automatisch gekoppeld aan een oplossing en gedeeld met de relevante stakeholder(s).

Andere organisaties werken op basis van uitgeschreven scenario's waar handelingen per scenario zijn toegelicht. Een organisatie geeft aan dat ze bezig zijn hun documentatie op het gebied van incident response uit te breiden. Ook in de incident responseplannen komt het ITIL-proces terug. Zo hebben meerdere organisaties de oplostijden van een incident gekoppeld aan de prioritering van het incident.

De ticketingsystemen zijn een belangrijke tool voor securityteams om de voortgang van een incident bij te houden. Incidenten worden bij het grootste deel van de geïnterviewde organisaties via een ticketingsysteem bijgehouden zoals ServiceNow of TopDesk. Hierin wordt door een aantal organisaties afgedongen wat de beheerders van het ticket over het incident moeten noteren, zoals getroffen systeem, impact, urgentie en oplostijden.

Drie organisaties dwingen naast toelichting over het incident in het ticketingsysteem dat er een root cause analysis moet worden opgenomen. Andere organisaties geven aan dat er na afloop van een PRIO1 incident een 'Lessons learned' moet worden opgenomen in de ticket. Omdat er bij de geïnterviewde partijen in de periode geen PRIO1-incidenten hebben plaatsgevonden hebben we in de interviews niet besproken met de organisaties of dit systeem goed functioneert. De organisaties konden zonder het raadplegen van documentatie eenvoudig de processen voor het evalueren van incidenten voor hun organisatie uitleggen. Incidenten lager dan een PRIO1 worden niet standaard geëvalueerd. De evaluatie van kleinere incidenten is niet opgenomen in incidentafhandelingsproces. Een aantal organisaties gaf aan op ad hoc basis incidenten onder PRIO1 af en toe te evalueren. Een organisatie gaf aan minder impactvolle incidenten standaard te evalueren en gaf aan de parameters voor de evaluatie beter te willen definiëren.

Drie organisaties geven aan dat zij ook te maken hebben met de afhandeling van incidenten zonder specifiek cybercomponent. De securityteams hebben daardoor ervaring met grotere incidenten met andere oorzaken dan cyberaanvallen of incidenten en zijn getraind in het incidentafhandelingproces binnen de organisatie.

Een minderheid van de geïnterviewde organisaties heeft de classificatie van het ITIL-incidentmanagementproces gekoppeld aan een melding richting het NCSC. Bij de organisaties die de melding hebben meegenomen in hun incidentmanagementproces gaat dit in alle gevallen over incidenten die als PRIO1 worden aangeduid. Twee organisaties geven aan dat in gevallen van PRIO1 incidenten, informatie over het incident wordt gedeeld met het NCSC en/of autoriteiten zoals de toezichthouder.

Incidentinformatie uit andere bronnen

De geïnterviewden is ook gevraagd of zij incidentinformatie haalden uit andere bronnen zoals samenwerkingsverbanden of nieuwsberichten. Alle organisaties waren lid van in ieder geval 1 ISAC en de meerderheid was lid van twee of meer ISACs. Alle organisaties vonden de deelname aan de samenwerkingsverbanden waardevol.

Wel waren er observaties uit de interviews dat deelnemers tijdens de bijeenkomsten van bijvoorbeeld de ISACs terughoudend waren om incidentinformatie te delen. Deelnemers gaven bijvoorbeeld alleen een korte terugkoppeling over een incident of deelden geen details over de aanval. Een respondent gaf aan dat hijzelf ook terughoudend was in het delen van incidenten vanwege de houding van andere deelnemers. Twee respondenten gaven aan te worstelen met de groei van de ISAC of brancheorganisatie. De intrede van nieuwe organisaties en de groei van de deelnemers maakte het lastiger om specifieke incidentinformatie te delen, omdat de respondenten geen sterke vertrouwensband hebben met alle deelnemers. Uit verschillende onderzoeken blijkt dat het ontbreken van vertrouwen een belangrijke barrière is om informatie over gevoelige onderwerpen, zoals incidenten gedetailleerd te delen met anderen.[32],[33] Een platform waarbij veel partijen elkaar niet vertrouwen, door bijvoorbeeld de instroom van nieuwe deelnemers, kan het delen van incidentinformatie compliceren.

Wanneer er wel gedetailleerde incidentinformatie werd gedeeld, gaven respondenten aan dat dit zeer nuttige informatie is die door de organisaties werd gebruikt om te toetsen of eenzelfde type incidenten ook bij hen mogelijk is. Een respondent gaf aan het toetsen van incidentinformatie in een proces te hebben gevangen door gebruik te maken van de ISO-proces over dreigingsinformatie. Hij gaf aan per kwartaal met collega's op een gestructureerde manier te kijken naar het binnengekomen incident. Hoewel het nu nog een informeel proces is, ligt er een plan om dit te formaliseren.

Hoeveelheid en typen meldingen naar het NCSC

In de interviews is de deelnemers gevraagd hoe vaak zij incidenten hebben gemeld bij het NCSC en welke typen incidenten zij melden bij het NCSC. Het aantal meldingen gedaan onder de WBNI door de respondenten is opvallend laag. Geen van de geïnterviewde organisaties heeft een incident gehad die de WBNI-drempelwaarde heeft overschreden waardoor een WBNI-melding aan

[32] Luuk Bakkers, R. L. (2020). *Verkenning Best Practices Cybersecurity Informatiedeling.* Den Haag: Haagse Hogeschool.

[33] Scott Ainsli, D. T. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security*, 1-16.

de toezichthouder en het NCSC verplicht was. Drie van de respondenten gaven aan meldingen bij het NCSC te hebben gemaakt van incidenten.

In totaal hebben van de zeven ondervraagde organisaties, twee organisaties een vrijwillige melding bij het NCSC gemaakt. Een van de twee organisaties heeft meerdere malen een vrijwillige melding gemaakt. Beide organisaties hebben onder de WBNI een DDoS aanval op de organisatie bij het NCSC gemeld.

Een van de respondenten gaf aan regelmatig informatie met het NCSC te delen maar dan niet via het meldformulier, maar via het Mattermost kanaal gefaciliteerd door het NCSC. De organisatie was tevreden over de snelle respons en interactie die het kanaal leverde in het delen van informatie. De organisatie had nog geen melding via het meldformulier bij het NCSC gedaan.

Wat uit de interviews naar voren komt op het gebied van melden richting het NCSC is dat organisaties gebruik maken van verschillende kanalen om incidenten bij het NCSC te melden. Een respondent die een WBNI-melding heeft gemaakt gaf aan dat ze goed contact hebben met de relatiemanager en informatie op een snelle manier kunnen doorspelen aan de relatiemanager. Zoals boven beschreven maakt een andere organisatie veelvuldig gebruik van het Mattermost kanaal. Weer een ander gaf aan gebruik te maken van de CERT-mailbox om incidentinformatie te delen. Van de zeven geïnterviewde organisaties noemden zes organisaties verschillende manieren om incidentinformatie te delen met het NCSC.

Wat opvalt is dat organisaties uiteenlopende kanalen aanwijzen als de meest gebruikte manier. Slechts de helft van de organisaties was bekend met het WBNI-meldformulier op de website, een twee organisaties was bekend met het meldformulier op MijnNCSC. Geen van de organisaties heeft nog een melding via het meldformulier op MijnNCSC gemaakt. Het merendeel van de organisaties wist niet dat het ook mogelijk is om via hun account op MijnNCSC een incident vrijwillig te melden. Een respondent gaf aan dat hij het idee kreeg dat sommige functies van MijnNCSC nog in ontwikkeling zijn en hij niet altijd goed op de hoogte werd gehouden van ontwikkelingen op de website. Hij was wel bekend met de registratiemogelijkheid op MijnNCSC, maar was niet bekend met de mogelijkheid om ook incidenten te melden.

Respondenten geven aan dat zij goede ervaringen hebben met het delen van informatie richting het NCSC. Een van de organisaties gaf aan dat de reactie op gedeelde informatie sinds het log4j incident eind 2021 aanzienlijk was verbeterd. Interessant is hierbij om te vermelden dat deze organisatie meerdere (vrijwillige) WBNI-meldingen heeft gemaakt.

Overwegingen om te melden bij het NCSC

Verplichte meldingen

Tijdens de interviews is respondenten gevraagd wat hun overwegingen zijn om incidenten of mogelijke incidenten te melden bij het NCSC. Zoals beschreven in het hoofdstuk *Nederlandse initiatieven voor delen van incidenten* leeft er bij veel organisaties een behoefte om meer

informatie over incidenten te delen. Het rapport Cyclotron uit 2022 geeft daarnaast aan dat er een behoefte is dat organisaties ook dreigende incidenten gaan delen en analyseren.[34]

Uit de interviews ontstaat een tweeledig beeld als het gaat om het melden van incidenten bij het NCSC. Organisaties die onder de WBNI vallen geven aan dat zij een heel duidelijk beeld hebben van wanneer zij verplicht zijn een incident bij het NCSC te melden. Van de zeven geïnterviewden organisaties vallen er vier onder de WBNI-wetgeving. Deze vier organisaties gaven aan goed op de hoogte te zijn van de wettelijke drempelwaarden. Alle vier de organisaties hebben incidentmanagementprocessen ingericht rondom incidenten die de WBNI-drempelwaarden overschrijden.

Een respondent gaf aan dat de organisaties guidelines heeft opgesteld om vast te stellen of de grootte van incident voldoende is om te melden aan het NCSC of de toezichthouder. De informatie die wordt gedeeld is wat wordt gevraagd in het formulier. Een andere respondent gaf aan een heel proces te hebben opgesteld voor collega's om hen helpen welke meldgrond zij voor de melding moeten kiezen, artikel 10a, 10b of artikel 16. Voor elke meldgrond is er een andere workflow.

Daarnaast hebben deze organisaties ook kunnen oefenen met het doen van meldingen tijdens de tweejaarlijkse ISIDOOR oefeningen. Al gaf een respondent eerlijk toe dat zijn organisatie vergeten was een meldingen te doen tijdens de laatste oefening, wat hij betreurde. Dit lijkt een breder probleem te zijn tijdens de ISIDOOR oefeningen, omdat uit de laatste evaluatie naar voren kwam dat maar 24% van de organisaties een WBNI-melding tijdens de oefening heeft gedaan.[35]

Voor het doen van verplichte meldingen gaan de geïnterviewde organisaties af op wat wettelijk verplicht is en delen de informatie die wettelijk verplicht is. Organisaties geven aan dat er geen andere afwegingen worden gemaakt voor dit type meldingen.

Vrijwillige meldingen

Wat betreft het delen van incidenten die niet onder de wettelijke verplichting vallen, ontstaat een ander beeld. Als het incidenten betreft die niet onder de meldplicht vallen, is het voor organisaties veel minder duidelijk wat het NCSC aan informatie zou willen ontvangen. We hebben de respondenten gevraagd of zij een beeld hebben van wat het NCSC graag aan informatie wil ontvangen met betrekking tot incidentinformatie. De reacties op de vraag lopen uiteen.

Ten opzichte van verplichte meldingen, spelen bij vrijwillige meldingen drijfveren een veel grotere rol. Beslissingen om te delen worden vaak tijdens of vlak na het incident genomen. Ook gaan organisaties, zoals een respondent beschreef, veel losser om met vrijwillige meldingen omdat er geen consequenties aan verbonden zijn. Vaak wordt tijdens de afhandeling van een incident ad

[34] Oldegarm, Mooy, CYCLOTRON: Gezamenlijk sneller en gerichter delen van informatie rondom (dreigende) cyberincidenten in publiek-privaat verband, 2022

[35] COT, Evaluatie ISIDOOR IV, April 2024

hoc besloten dat de informatie uit het incident mogelijk ook interessant is voor het NCSC. Dit gebeurt vaak op de persoonlijke inschatting van de betrokken expert.

Respondenten gaven aan reciprociteit een belangrijke drijfveer is om incidentinformatie te delen met het NCSC. Een respondent gaf aan dat wanneer er geen antwoord of een summier antwoord komt op de gedeelde informatie, dat de motivatie om de volgende keer iets te delen lager is. Een andere respondent gaf aan dat voor hen de interactie tussen de organisatie en het NCSC meespeelt. Zo hebben zij meer informatie over waar de organisatie een concrete bijdrage aan levert. Dit motiveert organisaties om actiever informatie met het NCSC te delen.

Een andere drijfveer is dat respondenten graag willen bijdragen aan een beter beeld van een incident. Zo noemde een respondent een afweging om informatie te delen zodat het ook bij andere organisaties in de sector terecht zou komen. Een respondent beschreef een poging tot het maken van een vrijwillige melding over een incident zonder cybercomponent. De respondent maakte de inschatting dat het toch goed was het NCSC proactief op de hoogte te stellen. Echter de respondent werd na initieel contact niet meer teruggebeld en beschreef het als een leermoment voor het doen van een melding.

Een drempel die meerdere keren naar voren kwam tijdens de interviews is dat organisaties niet precies weten wat het NCSC aan incidentinformatie zou willen ontvangen. Respondenten zijn van mening dat het NCSC niet geïnteresseerd is in phishingmails of kleine incidenten. Wat het NCSC wel graag zou willen ontvangen is bij de ondervraagde organisaties vaak niet bekend. Concrete omschrijvingen van welke incidentinformatie het NCSC wil ontvangen ontbreken volgens meerdere organisaties. Een respondent gaf aan dat heldere criteria van het NCSC het gemakkelijk zouden maken medewerkers binnen de organisatie duidelijk te maken wat vrijwillig gemeld kan worden.

Een andere drempel om informatie met het NCSC te delen is dat organisaties zelf ook niet de incidentinformatie hebben. Van de geïnterviewde organisaties nemen drie organisaties diensten af van een externe SOC-dienst die de triage doet. Een organisatie heeft een SOC die is geplaatst bij een ander onderdeel van de organisatie, die zeer omvangrijk is. Dit houdt in dat veel van de kleinschaligere cyberincidenten al worden behandeld voordat de respondent het incident onder ogen krijgt en kan beslissen over het delen van informatie. Deze strategie is logisch aangezien de vele kleinschalige incidenten veel capaciteit vragen als deze allemaal met het NCSC of een andere autoriteit gedeeld moeten worden. Het NCSC zou concreet advies kunnen geven over manieren om ook kleinschalige incidenten te delen.

Een drempel die in de literatuur wel vaak genoemd wordt maar in de interviews niet naar voren komt is terughoudend om incidentinformatie te delen uit angst voor boetes of schaamte. De geïnterviewde organisaties, zowel de partijen met langdurige contacten als de organisaties met weinig contact met het NCSC waren allen bereid om zeer open te spreken over hun incidentmanagementproces en incidenten die bij de organisaties hebben plaatsgevonden. Organisaties zijn bereid om desgevraagd meer informatie over incidenten te delen buiten de meldplicht en zijn ook bereid hier capaciteit van de organisatie aan te wijden. Dit komt overeen met de analyse van de WBNI-meldingen waaruit blijkt dat het grootste deel, 74% van de meldingen, vrijwillig bij het NCSC wordt gemaakt.

Relevant om te melden is dat drie organisaties zelf ook incidentinformatie voor hun achterban en/of sector analyseren. Een organisatie heeft een lopend initiatief waarbij zij een dreigingsbeeld voor hun sector opstellen met daarin relevante incidenten, ook incidenten die bij hen hebben

plaatsgevonden. Twee andere organisaties werken ook actief mee aan dreigingsbeelden voor hun sector. Een respondent gaf aan dat het voor hen belangrijk is tijdig incidentinformatie in hun netwerk te delen om nieuwe incidenten te voorkomen. Hij benadrukte dat transparantie op dit gebied voor de organisatie zeer belangrijk is.

Verwachtingen richting het NCSC

In de interviews is doelgroepen ook gevraagd welke verwachtingen richting het NCSC de organisaties hebben aangaande het thema van incidentmeldingen. Concrete vragen richting het NCSC lopen uiteen van meer informatie over de definities van incidenten onder de aankomende CBW tot statistieken over het aantal incidentmeldingen, criteria over typen incidenten en meer gerichte adviesgesprekken tussen de organisatie en het NCSC.

Van de ondervraagde respondenten gaven organisaties aan dat ze niet meer verwachten van het NCSC op het gebied van incidentmeldingen. Wel gaven verschillende respondenten aan dat zij wel meer duidelijkheid van het NCSC over welke incidentinformatie het NCSC wil ontvangen. Een andere respondent gaf aan dat hij graag meer informatie zou willen over wanneer hij na het doen van een melding aanspraak kan maken op technische ondersteuning vanuit het NCSC, zoals forensische analyses.

Respondenten gaven aan dat het contact met het NCSC over het algemeen goed verloopt en dat zij geen probleem hebben het NCSC te vinden wanneer zij een melding willen maken. Opvallende uitzondering was de organisatie die nu nog buiten de doelgroep van het NCSC valt. Deze organisatie had nog weinig ervaring in de communicatie met het NCSC en zou graag meer informatie ontvangen van het NCSC op dit onderwerp. Een respondent gaf aan dat zijn opvatting tweeledig is. De richtlijnen van het doen van een melding onder de WBNI zijn zeer duidelijk maar voor meldingen buiten de wettelijke plicht zijn de richtlijnen minder helder. Verschillende organisaties geven wel aan dat het geen kwaad kan als het NCSC meer communiceert over het doen van incidentmeldingen of concrete criteria en handvatten biedt voor het doen van (vrijwillige) meldingen aangezien de wensen van het NCSC op dit onderwerp niet duidelijk zijn.

Conclusies

We hebben met dit onderzoek gepoogd om inzichten te verschaffen in het systeem van incidentmeldingen richting het NCSC door doelgroeporganisaties. Hiervoor hebben we verschillende aspecten van dit systeem geanalyseerd. We hebben gekeken naar de kanalen van het NCSC waar incidentinformatie ontvangen kan worden, de systemen waar de informatie wordt verzameld en verrijkt en naar de kanalen om incidentinformatie te delen met de doelgroepen en Nederlandse organisaties. Hierbij hebben we ook gekeken naar de gebruikte taxonomieën binnen het NCSC.

Vervolgens hebben we semigestructureerde interviews gehouden met zes doelgroeporganisaties van het NCSC en een organisatie buiten de huidige doelgroep van het NCSC. We hebben de organisaties gevraagd hoe zij incidenten identificeren, afhandelen en hoe zij leren van incidenten. Ook hebben wij hen gevraagd hoe zij incidentinformatie doorgeven aan het NCSC, of zij incidentmeldingen bij het NCSC hebben gedaan en welke aanbevelingen zij voor het NCSC hebben op het onderwerp incidentmeldingen.

Uit de zeven gevoerde interviews gaven de organisaties aan tevreden te zijn over de mogelijkheden om incidentinformatie met het NCSC te delen. Daarnaast zijn doelgroepen over het algemeen tevreden over de respons vanuit het NCSC op de incidentinformatie die organisaties delen. Doelgroeporganisaties die meldingen onder de WBNI hebben gedaan waren tevreden over het proces. Een doelgroeporganisaties gaf aan dat een poging tot melding niet gelukt is en classificeerde dat tot leermoment.

Organisaties die al onder de WBNI vallen zijn goed op de hoogte van de sectorale drempelwaarden die verplichte meldingen vereisen bij incidenten. Verschillende organisaties hebben tot op zekere hoogte de WBNI-drempelwaarden opgenomen in hun incidentmanagementproces door de drempelwaarden intern te communiceren binnen de securityteams. Drie organisaties hebben processen opgesteld waarbij incidenten die binnen de organisaties worden geclassificeerd als PRIO1 van het ITIL-incidentmanagement framework ook onder de WBNI bij het NCSC worden gemeld. Hierbij moet worden vermeld dat dit type incidenten bij geen van de organisaties heeft plaatsgevonden. De hoogste incidentclassificatie die in de interviews werd genoemd was PRIO2.

Hoewel doelgroeporganisaties tevreden zijn over de communicatie vanuit het NCSC wanneer een melding is gemaakt, zijn organisaties niet goed op de hoogte wat het NCSC aan informatie wil ontvangen over incidenten. Doelgroeporganisaties die onder de WBNI vallen zijn goed op de hoogte over de meldplicht. Echter, voor incidenten die niet onder de meldplicht vallen is het voor doelgroeporganisaties veel onduidelijker wanneer en wat zij kunnen delen met het NCSC. Uit de interviews kwam naar voren dat doelgroeporganisaties ad hoc beslissen om een vrijwillige melding te maken, maar ook dat zij niet terughoudend zijn om informatie met het NCSC te delen. Duidelijke richtlijnen en criteria voor vrijwillige meldingen kunnen helpen informatiedelen te promoten.

Ook blijkt uit de interviews naar voren dat bijna alle organisaties gebruik maken van een intern of extern SOC. Een van de diensten van het SOC is de eerste triage van incidenten die vervolgens met de securityteam(s) van de organisatie worden gedeeld. De relatie tussen de SOCs en de organisatie is verschillend. Sommige interne SOCs zijn sterk ingebed in de organisatie, terwijl externe SOC-dienstelverleners meer op afstand staan en alleen incidenten met een hogere classificatie delen met de organisatie. Daardoor heeft de organisatie ook geen compleet beeld van alle incidenten. De triage is een belangrijke strategie om de schaarse capaciteit van het securityteam behapbaar te houden. Echter, voor de aggregatie van incidenten zou de verzameling van kleine incidenten ook een zeer relevante informatiebron zijn. Hiervan kan geleerd worden van rapportagesystemen van veiligheidsincidenten waar een grote hoeveelheid van incidenten wordt verzameld en geanalyseerd.

Aanbevelingen

Aan de hand van het bovenstaande onderzoek doen wij de volgende aanbevelingen aan het NCSC om de stroom van incidentinformatie te verbeteren.

1. *Zorg voor een product waar kwantitatieve incidentinformatie gedeeld kan worden*

Het NCSC mist op dit moment een product waar kwantitatieve overzichten van incidenten met doelgroeporganisaties kunnen worden gedeeld. Sinds het verdwijnen van het kwantitatieve overzicht van incidenten in het jaarlijkse CSBN is er geen product binnen het NCSC waar periodieke kwantitatieve overzichten gedeeld kunnen worden. Een logische plek voor dit type overzichten is een jaarlijks rapport waar dieper in kan worden gegaan op het type incidenten, de impact en ontwikkelingen in incidenten binnen Nederland.

2. *Zorg voor producten met informatie over wensen NCSC voor incidentinformatie*

Ten tijde van schrijven zijn doelgroeporganisaties niet goed op de hoogte van de informatie die het NCSC wil ontvangen over incidenten buiten de WBNI-meldplicht. Uit de analyse van de WBNI-meldingen komt naar voren dat de gedeelde informatie niet bruikbaar is voor analyses of het delen van relevante dreigingsinformatie met de doelgroepen. Er zijn op dit vlak kleine stappen gezet met de *Infosheet Vrijwillig Melden* en de *Situationeel Rapporten NAVO-top.* Gezien het belang van tijdige en gedetailleerde informatiedeling voor de programma's CWN en Cyclotron adviseren wij duidelijke en concrete adviesproducten op te stellen voor organisaties over hoe zij bij het NCSC kunnen melden en welke incidentinformatie het NCSC wil ontvangen.

3. *Zorg voor een periodieke communicatiestrategie voor incidentinformatie*

Uit de literatuur voor het rapporteren van veiligheidsincidenten blijkt dat organisaties prikkels nodig hebben om incidenten te melden bij instanties of toezichthouders. Het communiceren van

herinneringen om incidenten te melden ondersteunt de stroom van incidentinformatie. Wij adviseren om een communicatiestrategie op te zetten rondom een periodieke herinnering aan doelgroeporganisaties om informatie te delen en duidelijk te communiceren welke informatie het NCSC zou willen ontvangen op dit onderwerp. De herinnering kan bijvoorbeeld halfjaarlijks of jaarlijks worden opgenomen in producten of communicatie uitingen van het NCSC.

4. Zorg voor eenvoudige meldsystemen van kleinere incidenten bij SOCs

Doelgroeporganisaties zijn goed op de hoogte wanneer zij verplicht een melding moeten maken. Echter, kleine incidenten, bijvoorbeeld ingeschaald onder PRIO 3 of 4, gevallen van spearphishing, of mislukte pogingen tot initiële toegang worden veel minder met het NCSC gedeeld terwijl ook incidenten zonder grote impact relevante informatie kunnen bevatten. Alle incidenten bij het NCSC melden zou een onoverkomelijk capaciteitsvraagstuk bij de organisaties neerleggen. Echter, kunnen de SOCs van organisaties wel geaggregeerde overzichten van incidenten met het NCSC delen. Wij adviseren om de mogelijkheid te verkennen om geaggregeerde incidentgegevens vanuit SOCs met het NCSC om zo een completer beeld te krijgen over de cyberincidenten in Nederland.

Bronnen

Adam Zibak, A. S. (2019). Cyber Threat Information Sharing: Perceived Benefits and Barriers. *ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security*.

Annika Andreasson, H. A. (2024). Cybersecurity work at Swedish administrative authorities: taking action or waiting for approval. *Cognition, Technology & Work*, 709-731.

Article 23 - Reporting obligations - NIS2 Directive (nis2-info.eu). (sd).

Bibi van den Berg, D. W. (2025). *Samenwerken tegen ransomware: Inzichten uit het Melissa-onderzoek.* Leiden: Universiteit Leiden.

BSI. (2024, 12 31). *After global IT outages - BSI develops follow-up measures*. Opgehaald van bsi.bund.de: https://www.bsi.bund.de/EN/Service-Navi/Presse/Pressemitteilungen/Presse2024/240729_Folgemassnahmen_Crowdstrike.html

BSI. (2024). *Crowdstrike – Auswirkungen auf die deutsche Wirtschaft.* Berlin: BSI.

Buildahelpdesk.com. (2022, 4 4). *ITIL Incident Management Priority Matrix*. Opgehaald van Buildahelpdesk.com: https://buildahelpdesk.com/itil-incident-management-priority-matrix/

CBS. (2022). *Cybersecurity Monitor 2022.* CBS.

Clare M. Patterson, J. R. (2024). "I don't think we're there yet": The practices and challenges of organisational learning from cyber security incidents. *Computers & Security*.

COT. (2024). *Evaluatie ISIDOOR IV .* COT.

Eerste Kamer der Staten Generaal. (sd). *Wet beveiliging netwerk- en informatiesystemen (34.883); Memorie van toelichting (TK, 3) - Eerste Kamer der Staten-Generaal*. Opgehaald van eerstekamer.nl: https://www.eerstekamer.nl/behandeling/20180214/memorie_van_toelichting_2/info

ENISA. (2016). *Security incidents indicators - measuring the impact of incidents affecting electronic communications.* ENISA.

ENISA. (2018). *Reference Incident Classification Taxonomy Task Force Status and Way Forward.* ENISA.

Kasteleijn, N. (2024, 07 19). *Wat is Crowdstrike en hoe kon het zo misgaan? Dit is wat we nu weten*. Opgehaald van NOS: https://nos.nl/artikel/2529477-wat-is-crowdstrike-en-hoe-kon-het-zo-misgaan-dit-is-wat-we-nu-weten

Kooij, E. (2025). *Verslag opzet incidentenregister Unit Operatie .* NCSC.

Luuk Bakkers, R. L. (2020). *Verkenning Best Practices Cybersecurity Informatiedeling.* Den Haag: Haagse Hogeschool.

NCSC UK. (2023). *Cyber Security Breaches Survey 2023.* NCSC UK.

NCSC. (sd). *Zorgplicht*. Opgehaald van ncsc.nl: https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/hoe-kan-uw-organiseren-zich-voorbereiden-op-de-nis2-richtlijn#:~:text=De%20Cyberbeveiligingswet%20schrijft%20tien%20zorgplichtmaatregelen%20voor%20waar%

NCTV. (2024). *Cybersecuritybeeld Nederland 2024.* NCTV.

NCTV. (2024). *Het Cyberweerbaarheidsnetwerk: Toekomstvisie voor het verbeteren van publiek-private samenwerking t.b.v. het verhogen van de cyberweerbaarheid van organisaties, .* Den Haag: Ministerie van Justitie en Veiligheid.

NIST. (sd). *Incident*. Opgehaald van nist.gov: https://csrc.nist.gov/glossary/term/incident

Petra Olegarm, L. M. (2022). *CYCLOTRON: Gezamenlijk sneller en gerichter delen van informatie rondom (dreigende) cyberincidenten in publiek-privaat verband.* Den Haag: NCTV.

RDI. (2022). *Samenhangend Inspectiebeeld cybersecurity vitale processen.* RDI.

Scott Ainsli, D. T. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security*, 1-16.

Simone Busetti, F. M. (2025). Evaluating incident reporting in cybersecurity. From threat detection to policy learning. *Government Information Quarterly*, 1-17.

Srinath Perera, X. J.-G. (2022). Factors Affecting Reputational Damage to Organisations Due to Cyberattacks. *Informatics*, 8-28.

Thomas D. Wagner, K. M. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*.

Wet beveiliging netwerk- en informatiesystemen. (2019). Opgehaald van Overheid.nl: https://wetten.overheid.nl/BWBR0041515/2019-01-01

Appendix A: Interviewprotocol

Vragen incidentmeldingen doelgroepen

Introductie

- Wat is je naam?
- Wat is je functie?

Identificatie van incident

1. Wat verstaat de organisatie onder een cyber incident?
2. Wat is een significant incident?
3. Is er een prioritering in de incidenten?
4. Op welke systemen ontvangen jullie meldingen over incidenten? Bv SOC, mail, TIP
5. Heeft er het afgelopen jaar een cyberincident in de organisatie plaatsgevonden?
6. Zo ja, kan je het identificeren van het incident beschrijven?
7. Heeft de organisatie een proces voor de identificatie van een cyberincident? Bijvoorbeeld een afwegingskader om de ernst vast te stellen?
8. Zijn er mensen in de organisatie aangesteld om informatie over (mogelijke) cyberincidenten te ontvangen binnen de organisatie? Bijvoorbeeld een security officer?
9. Krijgen collega's training in het melden van incidenten bij de verantwoordelijke personen binnen de organisatie?

Afhandelen incident binnen de organisatie

1. Is er een incident response plan? Vanaf welke prioriteit geldt een incident response?
2. Wie is er betrokken bij de afhandeling van een incident binnen de organisatie?

3. Is er een incident response team die een incident kan afhandelen?
4. Wat voor informatie wordt verzameld voor een incident binnen de organisatie? Bijvoorbeeld inschatting van impact, indicators of compromise, type aanval, datum/tijd?
5. Hoe wordt een incident binnen de organisatie gecommuniceerd?
6. Wie is er betrokken bij het rapporteren van een incident bij autoriteiten?
7. Is er een collega aangewezen als verantwoordelijke voor het meldproces?
8. Is er een afwegingskader bij welke autoriteiten een incident moet worden gemeld?

Leren van incidenten

1. Is er een evaluatieproces na afloop van een incident?
2. Krijgt jij of een collega periodiek informatie over cyberincidenten bij andere organisaties?
3. Wat vind je de meest waardevolle informatie om te bestuderen uit andere incidenten? Denk bijvoorbeeld aan: type organisatie? Impact van het incident? Omschrijving van het incident? Omschrijving van de aanval?
4. Bespreek je incidenten binnen samenwerkingsverbanden zoals een ISAC of een branchevereniging?
5. Ervaar je het delen van incidenten binnen een samenwerkingsverband als waardevol?
6. Wat doe je met informatie over incidenten uit een samenwerkingsverband?

Melden richting het NCSC

1. Heeft de organisatie de afgelopen drie jaar een incident gemeld bij het NCSC?
2. Is er een interne afweging wanneer een incident met het NCSC wordt gedeeld? Bijvoorbeeld bij een bepaalde prioriteit?
3. Welke informatie wordt initieel gedeeld met het NCSC?
4. Welke informatie wordt in een later stadium met het NCSC gedeeld?
5. Heb je kennis van het incidentmeldformulier van het NCSC?
6. Heb je feedback op het formulier?
7. Zijn er andere manieren waarop je organisatie meldt bij het NCSC?

Communicatie vanuit NCSC

1. Is er binnen de organisatie duidelijkheid wat de wensen van het NCSC zijn voor het melden van incidenten?
2. Is er binnen de organisatie duidelijkheid wat de wensen van het NCSC zijn voor het melden van incidenten onder de NIS2?
3. Is er binnen de organisatie duidelijkheid over de drempelwaarden voor het melden onder de WBNI?
4. Is de communicatie vanuit het NCSC wanneer en hoe een incident gemeld moet worden voldoende?
5. Zou het NCSC meer moeten doen om het doen van incidentmeldingen te promoten?
6. Zou het NCSC meer moeten doen om informatie over incidenten met organisaties te delen?
7. Ervaar je dat het NCSC voldoende ondersteuning biedt om een incident te melden? Bijvoorbeeld door het geven van advies over welke informatie belangrijk is