# Samenwerken tegen Ransomware: Evaluatie Melissa

Bibi van den Berg, Daan Weggemans en Manon Nobbenhuis


Universiteit Leiden
Institute of Security and Global Affairs

Bij ons leer je de wereld kennen

# INHOUDSOPGAVE

# 1. AANLEIDING

Ransomware aanvallen zijn erop gericht economisch gewin te realiseren door individuen of organisaties af te persen.[1] Bij een ransomware aanval infiltreren cybercriminelen een systeem en versleutelen zij vaak kritieke data; de eigenaar of verwerker kan de toegang tot deze data alleen terugkrijgen na het betalen van een som aan losgeld – waarbij een losgeldbetaling overigens niet gegarandeerd leidt tot ontsleuteling van de data.[2] Regelmatig exfiltreren cybercriminelen ook belangrijke documenten en/of persoonsgegevens als onderdeel van een ransomware aanval, zodat ze deze data kunnen gebruiken als inzet in de onderhandelingen, bijvoorbeeld door (te dreigen met) het lekken van documenten of het verkopen of toegankelijk maken van persoonsgegevens.[3] Hoewel het eerste geval van ransomware al werd gemeld in 1989, heeft het sinds 2005 een vlucht genomen, waarbij in eerste instantie vooral individuen slachtoffer werden, maar aanvallen zich later steeds meer zijn gaan richten op (grote) publieke en private organisaties omdat de mogelijke buit daar vele malen groter is.[4] Sinds 2015 zijn ransomware aanvallen complexer en professioneler geworden[5], is het gevraagde losgeld exponentieel omhoog gegaan en is de economische en maatschappelijke impact van dit fenomeen sterk gestegen.[6]

In 2023 werden volgens de Auroriteit Persoonsgegevens 178 organisaties in Nederland slachtoffer van ransomware aanvallen.[7] Twee jaar eerder, in 2021, werden er nog 107 aangiftes van aanvallen met ransomware gedaan.[8] Er is dus sprake van een stijging van 66% in het aantal gemelde aanvallen in twee jaar tijd. Daarbij rijst de vraag of de getallen de volledige omvang van het fenomeen ransomware in Nederland laten zien. Volgens Blom *et al.* deed in 2021 slechts 2 tot 4% van de organisaties die slachtoffer werd aangifte bij de politie. In datzelfde jaar bleek uit hun onderzoek ook dat enquêtes van verzekeraars aantonen dat 26% van alle Nederlandse

1 Het Cybersecurity woordenboek (2021) omschrijft ransomware als kwaadaardige software waarbij "de aanvallers data [gijzelen] van het slachtoffer en drukmiddelen [gebruiken] om het slachtoffer over te halen te betalen. Die gijzeling bestaat vaak uit het versleutelen van de gegevens van het slachtoffer". Zie ook: Greenberg, Andy, 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *WIRED*, August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.; Schlette, Daniel, Marco Caselli, and Günther Pernul. "A comparative study on cyber threat intelligence: The security incident response perspective." *IEEE Communications Surveys & Tutorials* 23, no. 4 (2021): 2525-2556.

2 Opderbeck, David W. "Cybersecurity and Data Breach Harms: Theory and Reality." *Md. L. Rev.* 82 (2022): 1001.

3 Er zijn ook voorbeelden van aanvallen waarbij data niet meer wordt versleuteld en dat de criminelen zich beperken tot afpersen, zo geeft een van de respondenten (10) van dit onderzoek aan. Ook dit kan tot de scope van het nader te beschrijven project Melissa worden gerekend. Zie ook Blom, Tessel. 2023. "Ransomware-aanvallen Op Instellingen En Bedrijven in Nederland." Dialogic. September 12, 2023. https://dialogic.nl/2023/09/12/ransomware-aanvallen-op-instellingen-en-bedrijven-in-nederland/.; Autoriteit Persoonsgegevens (AP), 'Rapportage ransomware: Gebrekkige beveiliging maakte twee op de drie getroffen organisaties kwetsbaar', 2024, https://www.autoriteitpersoonsgegevens.nl/system/files?file=2024-10/AP%20rapportage%20ransomware.pdf; Matthijsse, Sifra R., M. Susanne van 't Hoff-de Goede, and E. Rutger Leukfeldt. "Your files have been encrypted: A crime script analysis of ransomware attacks." *Trends in Organized Crime* (2023): 1-27.

4 Blom, Tessel. 2023. "Ransomware-aanvallen Op Instellingen En Bedrijven in Nederland." Dialogic. September 12, 2023. https://dialogic.nl/2023/09/12/ransomware-aanvallen-op-instellingen-en-bedrijven-in-nederland/.; Matthijsse, Sifra R., M. Susanne van 't Hoff-de Goede, and E. Rutger Leukfeldt. "Your files have been encrypted: A crime script analysis of ransomware attacks." *Trends in Organized Crime* (2023): 1-27.

5 Hyslip, Thomas S., and George W. Burruss. "Ransomware." In *Handbook on Crime and Technology*, pp. 86-104. Edward Elgar Publishing, 2023.; Matthijsse, Sifra R., M. Susanne van 't Hoff-de Goede, and E. Rutger Leukfeldt. "Your files have been encrypted: A crime script analysis of ransomware attacks." *Trends in Organized Crime* (2023): 1-27.

6 Hyslip, Thomas S., and George W. Burruss. "Ransomware." In *Handbook on Crime and Technology*, pp. 86-104. Edward Elgar Publishing, 2023.

7 Autoriteit Persoonsgegevens (AP), 'Rapportage ransomware: Gebrekkige beveiliging maakte twee op de drie getroffen organisaties kwetsbaar', 2024, https://www.autoriteitpersoonsgegevens.nl/system/files?file=2024-10/AP%20rapportage%20ransomware.pdf;

8 Tessel, Blom. 2023. "Ransomware-aanvallen Op Instellingen En Bedrijven in Nederland." Dialogic. September 12, 2023. https://dialogic.nl/2023/09/12/ransomware-aanvallen-op-instellingen-en-bedrijven-in-nederland/.

bedrijven in 2022 slachtoffer geworden zou zijn van ransomware.[9]

Slachtofferschap van ransomware aanvallen is een kostbare aangelegenheid, zelfs als een organisatie besluit geen losgeld te betalen. Onderzoek naar de oorzaak en aard van het incident, maar ook de afhandeling ervan en het herstellen van systemen en netwerken kosten veel geld, tijd en menskracht.[10] Wanneer ransomware aanvallen grote en/of kritieke organisaties raken, kan dit, naast directe impact voor de eigen organisatie, ook gevolgen hebben voor grotere ketens en voor burgers. Het Cybersecurity Beeld Nederland uit 2021 bestempelde ransomware om die reden als een potentiële bedreiging voor onze nationale veiligheid.[11]

In het licht van deze ontwikkelingen zijn vertegenwoordigers vanuit de Politie, het Openbaar Ministerie (OM), het Nationaal Cyber Security Center (NCSC), Cyberveilig Nederland en een deel van haar leden in 2022 gestart met een nieuwe samenwerking voor de bestrijding van ransomware en gerelateerde vormen van cybercrime. Deze publiek-private samenwerking kreeg de naam 'Melissa'.[12] Binnen Melissa streven partijen ernaar om structureel kennis en informatie uit te wisselen en incidenteel samen te werken in specifieke opsporingsonderzoeken om zo gezamenlijk bij te dragen aan het minder aantrekkelijk maken van Nederlandse publieke en private organisaties voor ransomware aanvallen. Melissa bestaat uit een kerngroep, bestaande uit een elftal representanten van de hierboven genoemde organisaties. Zij vormen het 'kloppende hart' van de samenwerking. Zij bereiden onder andere de sessies en bijeenkomsten voor en bepalen welke (nieuwe) deelnemers betrokken worden bij Melissa. Om deze kerngroep heen bestaat een schil van vertegenwoordigers uit 3 publieke en 12 private organisaties.

In het najaar van 2023 is de samenwerking binnen Melissa geformaliseerd in een convenant dat door de genoemde partijen ondertekend is. In het convenant zijn de juridische, organisatorische en technische overeenkomsten voor deze samenwerking vastgelegd. Ook werd hierin afgesproken dat de samenwerking zou worden geëvalueerd. In de zomer van 2024 hebben de samenwerkende partners in Melissa een verzoek uitgezet bij de Universiteit Leiden voor het uitvoeren van deze evaluatie. De werkwijze, bevindingen en aanbevelingen van de evaluatie zijn opgetekend in dit rapport.

## Onderzoeksvragen

In dit evaluatieonderzoek staan de volgende vragen centraal:

a. Is de logica achter Melissa sluitend en in hoeverre worden de geformuleerde doelstellingen in de praktijk gerealiseerd?
b. Welke activiteiten hebben in de afgelopen jaren plaatsgevonden onder de banier van Melissa en tot welke resultaten heeft dit geleid?
c. Welke succes- en faalfactoren zien deelnemers aan Melissa wanneer ze terugkijken op de afgelopen periode, en wat betekent dit voor

9 Deze alinea laat zien dat er een groot gebrek is aan betrouwbare cijfers over de aard en omvang van het fenomeen ransomware in Nederland. De variëteit in cijfers kan erop wijzen dat partijen verschillende maatstaven of rekenmodellen gebruiken om een aanval wel of niet mee te tellen. Ze kan ook duiden op een groot 'dark number'. Dit betekent dat een fenomeen niet goed kwantificeerbaar is omdat er, bijvoorbeeld door gebrekkige informatie-uitwisseling, onvoldoende zicht is op de totaliteit van dat fenomeen. Partijen nemen dan elk slechts een deel van het fenomeen waar. Zie verder Blom, Tessel, 2023. "Ransomware-aanvallen Op Instellingen En Bedrijven in Nederland." Dialogic. September 12, 2023. https://dialogic.nl/2023/09/12/ransomware-aanvallen-op-instellingen-en-bedrijven-in-nederland/.

10 Akyazi, Ugur, M. J. G. van Eeten, and C. Hernandez Ganan. "Measuring cybercrime as a service (caas) offerings in a cybercrime forum." In *Workshop on the Economics of Information Security*. 2021.

11 Nationaal Cyber Security Centrum and Nationaal Coördinator Terrorismebestrijding en Veiligheid. 2021. "Cybersecuritybeeld Nederland 2021." https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021#:~:text=Het%20Cybersecuritybeeld%20Nederland%202021%20(CSBN,daarbij%20op%20de%20nationale%20veiligheid.

12 De naam Melissa kent haar oorsprong in een bijeenkomst in het voorjaar van 2022. Hier werd door een incident respons partij een geluidsfragment van een onderhandeling met een ransomware groepering gedeeld. Het bleek dat de onderhandelaar, die zich voorstelde als Melissa, op eerdere momenten had onderhandeld met enkele andere aanwezigen. Wat opvallen d was dat dit allemaal andere ransomware groeperingen waren. Zo leerde men dat onderhandelaars blijkbaar kunnen worden ingehuurd door verschillende groeperingen.

(de organisatie van) de samenwerking voor de komende jaren, zowel binnen Melissa zelf, als ook met publieke, private en wetenschappelijke stakeholders, zowel binnen als buiten Nederland?

## Aanpak

Het nog relatief jonge veld van evaluatieonderzoek, is de afgelopen jaren sterk gegroeid en er zijn in relatief korte tijd veel nieuwe methoden ontwikkeld.[13] Voor deze studie is gekozen voor een zogeheten *realistische* benadering waarmee we verder willen gaan dan de vraag '*of* Melissa werkt' maar in eerste instantie inzicht willen verkrijgen in *hoe* en *waarom* Melissa werkt in deze context. Hiervoor zullen we ons zowel richten op de logica van de onderliggende mechanismen van het project als ook op hun praktisch functioneren (zie hoofdstuk 2). Om deze inzichten te verkrijgen is derhalve gebruik gemaakt van verschillende bronnen en kwalitatieve onderzoeksmethoden.

### *Documentenstudie*

Voor deze studie zijn de beschikbare documenten van project Melissa bestudeerd. Dit betreft officiële stukken zoals het convenant, het projectplan, actiepunten vanuit de meetings van de kerngroep en presentaties en verslagen van georganiseerde bijeenkomsten met alle betrokkenen. Daarnaast zijn ook enkele publicaties vanuit het project (whitepapers over data-exfiltratie bij een cyberaanval en ransomware inzichten) en mediaberichten geanalyseerd. Deze documenten hebben we bestudeerd om inzicht te krijgen in zowel de onderliggende theorie als de samenwerkings- en informatieuitwisselingspraktijk. Een overzicht van de geraadpleegde documenten is te vinden in bijlage 2.

### *Interviews*

Voor dit project zijn in totaal 13 interviews afgenomen met verschillende betrokkenen binnen het project. Ten eerste betrof dit gesprekken met leden van de kerngroep over onder meer de veronderstellingen achter het project Melissa. Deze gesprekken zijn van belang geweest bij het uitwerken van de theoretische veronderstellingen die in het tweede deel van dit rapport centraal staat. Ten tweede zijn er gesprekken gevoerd met professionals die allen werkzaam zijn bij een van de samenwerkende partijen en gedurende de afgelopen tijd actief betrokken waren bij Melissa. Zo waren zij bijvoorbeeld aanwezig bij de georganiseerde (tweedaagse) bijeenkomsten en diverse sessies. Ook deelden zij online inzichten met het netwerk over relevante ontwikkelingen en trends. Het doel was hierbij om inzicht te krijgen in de belangrijkste resultaten, ervaringen en belangrijkste lessen binnen deze samenwerking.

Alle interviews waren semigestructureerd van aard. Binnen dit format worden op voorhand bepaalde gespreksonderwerpen vastgelegd maar is er ook ruimte om door te vragen of tot interessante aanvullende gespreksonderwerpen te komen.[14] De interviews vonden online plaats via MS Teams in de periode juni – september 2024 en duurden gemiddeld een uur. Er was sprake van een hoge mate van consistentie tussen de gesprekken: de respondenten deelde onafhankelijk van elkaar veel dezelfde observaties. Voor de afronding van de interviewfase - individueel en in zijn geheel - gold verzadiging als belangrijkste criterium: na verloop van tijd levert een (nieuw) gesprek weinig nieuwe inzichten meer op. Van alle deze gespreken zijn (niet-verbatim) transcripten opgesteld. De gehanteerde topiclijst en een overzicht van de gesprekspartners is opgenomen in bijlage 3.

### *Focusgroep*

Ter voorbereiding van de individuele interviews is er bij aanvang van het project een explorerende focusgroep georganiseerd met 12 deelnemers. Het doel was om relevante thema's te identificeren voor de topiclijst en eerste gedeelde inzichten te verzamelen. De focusgroep richtte zich daarnaast ook op de verwachtingen wat betreft het evaluatieonderzoek zelf. Er is door de onderzoekers een verslag opgesteld van deze sessie, die ongeveer een uur duurde.

### *Veldwerk: Op bezoek tijdens een van de tweedaagse bijeenkomsten*

Bij de start van het onderzoek hebben de onderzoekers een bezoek van enkele uren gebracht aan een van de tweedaagse bijeenkomsten van Melissa. Tijdens dat

13 Zoals elders eerder al treffend beschreven "There can be no doubt about it – evaluation is a vast, lumbering, overgrown adolescent" (Pawson, Ray, and Nick Tilley. "An introduction to scientific realist evaluation." *Evaluation for the 21st century: A handbook* 1997 (1997): 405-18.)

14 Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Sage.

bezoek kregen de onderzoekers een eerste beeld van de aard en omvang van de praktijk van samenwerken en informatiedelen binnen Melissa. Met behulp van participatieve observatie is in kaart gebracht in wat voor type sessies deelnemers kennis delen, over welke onderwerpen zij zoal met elkaar van gedachten wisselen en welke kennisdelingsformats hiervoor worden gebruikt. Ook het waarnemen van de interpersoonlijke en sociale dynamiek was onderdeel van deze observatie.

### *Wetenschappelijke literatuur*

Wetenschappelijke literatuur en bronnen zijn gebruikt om de verzamelde gegevens uit bovenstaande documenten en interviews te beoordelen en in een breder kader te plaatsen. Bestaande wetenschappelijke inzichten helpen bij het gericht reflecteren op ideeën over de werking, nut en noodzaak van de samenwerking.

### *Peer review*

Het volledige rapport is aan twee collega-wetenschappers uit eigen kring voorgelegd die hebben gefungeerd als kritische tegenlezers. Wij zijn Dr. Tommy van Steen en dr. Cristina del Real dankbaar dat zij, op grond van hun expertise op het gebied van cybersecurity en cybercrime, dit rapport hebben voorzien van relevante feedback.

### Leeswijzer

Deze evaluatie bestaat uit drie delen. Het eerste deel gaat in op de theoretische fundamenten van het project. We concentreren ons daarbij op de doelen en ontwikkelde aanpak (hoofdstuk 2). In hoeverre zijn de veronderstellingen over de werking van mechanismen achter Melissa logisch en *evidence based*? Het tweede deel richt zich vervolgens op de praktijkopbrengsten (hoofdstuk 3), en op de succesfactoren en huidige risico's (hoofdstuk 4). Wat is er in de praktijk gedaan en sluit dit aan bij de gestelde doelen? En wat heeft de samenwerking uiteindelijk opgeleverd? Het derde deel kijkt daarna vooruit en gaat in op de voornaamste kansen en uitdagingen voor dit samenwerkingsverband (hoofdstuk 5). Ten slotte worden de belangrijkste conclusies van deze evaluatie besproken (hoofdstuk 6).

# 2. ACHTERGROND EN VERONDERSTELDE WERKING

In het eerste deel van deze evaluatie staan we stil bij de verwachtingen ten aanzien van het samenwerkingsverband Melissa: wat waren de doelstellingen van deze samenwerking en welke veronderstellingen gingen erachter schuil? We gaan hiervoor eerst nader in op de bredere ontwikkelingen op het gebied van ransomware en de maatschappelijke context waarin het initiatief voor Melissa is ontstaan. Vervolgens bespreken we de algemene opzet en inrichting van Melissa. Daarna wordt het analysekader beschreven op basis waarvan de evaluatie is uitgevoerd.

## Context en ontwikkelingen

Ransomware of gijzelsoftware (*ransom* soft*ware*) is de meest voorkomende vorm van cybercrime wereldwijd.[15] Bij een ransomware-aanval gijzelen aanvallers data van personen of organisaties om hen vervolgens af te persen. Hiervoor wordt malware gebruikt die de data of systeembestanden van slachtoffers versleutelt; deze zaken worden pas vrijgegeven als het slachtoffer losgeld heeft betaald.[16] Ook bestaat een ransomware-aanval tegenwoordig vaak uit het exfiltreren van (belangrijke) data door de dader, die deze als extra dwangmiddel voor betaling kan gebruiken, bijvoorbeeld door persoonlijke data publiek te maken of door te verkopen, of gevoelige informatie te lekken naar de media.[17][18] In de literatuur wordt daarbij gesproken over "double" of zelfs "triple extortion".[19]

Ransomware-aanvallen kunnen zorgen voor serieuze schade. Georganiseerde netwerken van cybercriminelen maken dagelijks vele slachtoffers met het verstoren van bedrijfsprocessen en stelen van data om vervolgens grote losgeldbedragen te eisen.[20] Bij een gerichte, zorgvuldig voorbereidde aanval, kan dit een bedrag van miljoenen euro's voor het slachtoffer betekenen.[21] Zo zorgde bijvoorbeeld Wannacry ransomware in 2017 voor de besmetting van 230.000 apparaten en veroorzaakte voor 4 miljard dollar aan schade over de hele wereld.[22] Inmiddels wordt geschat dat de totale kosten voor ransomware-aanvallen tot in de tientallen[23] en zelfs honderden miljarden zullen oplopen.[24] Maar de impact van ransomware-aanvallen gaat verder dan de negatieve financiële gevolgen voor slachtoffers. Zoals elders gesteld: "Ransomware's effects are not just monetary, as the loss of the files themselves (or the costs of ransom) may be eclipsed by the loss of

15 O'Kane, Philip, Sakir Sezer and Domhnall Carlin. "Evolution of ransomware". *Iet Networks* 7, no. 5 (2018): 321-327.; Oz, Harun, Ahment Aris, Albert Levi, and A. Selcuk Uluagac. "A survey on ransomware: Evolution, taxonomy, and defense solutions."ACM Computing Surveys *(CSUR)*54, no. 11s (2022): 1-37.; Brewer, Ross. "Ransomware attacks: detection, prevention and cure." *Network security* 2016, no.9 (2016): 5-9.

16 Nationaal Cyber Security Centrum. 2024. "Ransomware." Wat Kun Je Zelf Doen? | Nationaal Cyber Security Centrum. Juni 14, 2024. https://www.ncsc.nl/wat-kun-je-zelf-doen/dreiging/ransomware.; Richardson, Ronny, and Max M. North. "Ransomware: Evolution, mitigation and prevention." *International Management Review* 13, no. 1 (2017): 10.

17 Hyslip, Thomas S., and George W. Burruss. "Ransomware." In *Handbook on Crime and Technology*, pp. 86-104. Edward Elgar Publishing, 2023.

18 Cyberveilig Nederland. 2023, Whitepaper Ransomware. https://cyberveilignederland.nl/upload/userfiles/files/CVNL_Ransomware_def.pdf.

19 Matthijsse, Sifra R., M. Susanne van 't Hoff-de Goede, and E. Rutger Leukfeldt. "Your files have been encrypted: A crime script analysis of ransomware attacks." *Trends in Organized Crime* (2023): 1-27.

20 Staatscourant 2023, Officiele bekendmakingen 29185. November 1, 2023 https://zoek.officielebekendmakingen.nl/stcrt-2023-29185.html

21 Nationaal Cyber Security Centrum. 2022. "Factsheet Ransomware." Factsheet | Nationaal Cyber Security Centrum. October 28, 2022. https://www.ncsc.nl/wat-kun-je-zelf-doen/documenten/factsheets/2020/juni/30/factsheet-ransomware.

22 Kumar, P. Ravi, and Hj Rudy Erwan Bin Hj Ramlie. 2021. "Anatomy of Ransomware: Attack Stages, Patterns and Handling Techniques." In *Advances in Intelligent Systems and Computing*, 205–14. https://doi.org/10.1007/978-3-030-68133-3_20.

23 Kumar, P. Ravi, and Hj Rudy Erwan Bin Hj Ramlie. 2021. "Anatomy of Ransomware: Attack Stages, Patterns and Handling Techniques." In *Advances in Intelligent Systems and Computing*, 205–14. https://doi.org/10.1007/978-3-030-68133-3_20

24 Freeze, Di. 2023. "Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031." Cybercrime Magazine. July 10, 2023. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

"client trust, relationships, and reputation"".[25] Daarnaast kunnen er potentieel onveilige situaties ontstaan, zoals wanneer ziekenhuizen of energiecentrales slachtoffer worden van een ransomware-aanval en vitale maatschappelijke processen stil worden gelegd.[26] Zo kan een ransomware-aanval op een organisatie ook een bredere impact op de maatschappij en de nationale veiligheid hebben.[27] Cybercriminelen willen doorgaans dat de ervaren impact van ransomware zo groot mogelijk is en kunnen ook dreigen gegevens definitief te wissen of juist openbaar te maken.[28] Dit overkwam bijvoorbeeld de KNVB in 2023 toen een ransomwaregroep dreigde de persoonsgegevens van trainers en spelers van de voetbalbond te lekken.[29] Ten slotte kunnen actoren die primair geïnteresseerd zijn in het verkrijgen van gevoelige informatie en persoonsgegevens of intellectueel eigendom hebben gestolen ransomware gebruiken om hun sporen te wissen.[30]

Ransomware is 'big business' en de dreiging is de afgelopen jaren overal ter wereld flink gegroeid. Het aantal aanvallen en de gemiddelde downtime zijn net als de losgeldbedragen en totale schade flink toegenomen. Geschat wordt dat het gemiddeld tussen de 16 en 23 dagen duurt voordat organisaties hun activiteiten hervatten.[31] Het merendeel van de geregistreerde cyberincidenten in Nederland betreft ransomware. Enkele voorbeelden van ransomware aanvallen die in Nederland het nieuws haalden zijn die van containerterminals in de Rotterdamse haven (juni 2017), de Universiteit van Maastricht (december 2019), de gemeente Hof van Twente (december 2020), de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO, februari 2021), het ROC Mondriaan (augustus 2021), de Mediamarkt (november 2021), ID-Ware (september 2022) en de al eerder genoemde aanval op de KNVB (september 2023). Eerder stelde Cyberveilig Nederland al dat 90% van de incident respons capaciteiten binnen de Nederlandse informatiebeveiligingssector in 2021 werd ingezet bij organisaties die het slachtoffer waren van een ransomware-aanval.[32]

Deze en andere aanvallen van het afgelopen decennium maken duidelijk dat ransomware zowel in omvang als complexiteit een flinke ontwikkeling heeft doorgemaakt. In een gezamenlijk whitepaper verwijzen Cyberveilig Nederland, de Politie en het Nationaal Cyber Security Centrum (NCSC) naar zogenaamde politie-ransomware uit 2011.[33] Hierbij werden computers geblokkeerd en verscheen er een politielogo op het beeldscherm met het bericht dat er kinderporno was gevonden. Om overal weer

25 Sherer, James, Melinda McLellan, Emily Fedeles, and Nichole Sterling. 2017. "Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web." *Richmond Journal of Law & Technology* 23 (3). https://jolt.richmond.edu/files/2017/05/Sherer-Final-clean-.pdf. (22).

26 Sherer, James, Melinda McLellan, Emily Fedeles, and Nichole Sterling. 2017. "Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web." *Richmond Journal of Law & Technology* 23 (3).

27 Tessel, Blom Wazir Sahebali, Kimberly Deppe, Peter Romijn, Floris Donath, and Reg Brennenraedts. 2023. "Ransomeware-aanvallen op instellingen en bedrijven in Nederland." 2022.173-2319. Dialogic. https://repository.wodc.nl/bitstream/handle/20.500.12832/3292/3375-ransomware-aanvallen-op-instelllingen-en-bedrijven-volledige-tekst.pdf?sequence=7&isAllowed=y. (21)

28 Nationaal Cyber Security Centrum. 2022. "Factsheet Ransomware." Factsheet | Nationaal Cyber Security Centrum. October 28, 2022. https://www.ncsc.nl/wat-kun-je-zelf-doen/documenten/factsheets/2020/juni/30/factsheet-ransomware.

29 NOS. 2023. "'Ransomwaregroep Dreigt KNVB Contracten Van Trainers En Spelers Te Lekken.'" April 17, 2023. https://nos.nl/artikel/2471789-ransomwaregroep-dreigt-knvb-contracten-van-trainers-en-spelers-te-lekken.

30 Nationaal Cyber Security Centrum. 2022. "Factsheet Ransomware." Factsheet | Nationaal Cyber Security Centrum. October 28, 2022. https://www.ncsc.nl/wat-kun-je-zelf-doen/documenten/factsheets/2020/juni/30/factsheet-ransomware.

31 August, Terrence, Duy Dao, and Marius Florin Niculescu. 2022. "Economics of Ransomware: Risk Interdependence and Large-Scale Attacks." *Management Science* 68 (12): 8979–9002. https://doi.org/10.1287/mnsc.2022.4300. (p. 8980) ; Cyberveilig Nederland. 2023. "Ransomware." https://cyberveilignederland.nl/upload/userfiles/files/CVNL_Ransomware_def.pdf.

32 Cyberveilig Nederland. 2023, ibid.

33 Cyberveilig Nederland. 2023, ibid (p.7); Dergelijke politie-ransomware werd in meerdere landen gebruikt. Zie voor een korte internationale bespreking: O'Gorman, Gavin, and Geoff McDonald, 2012.. "Ransomware: A Growing Menace." Symantec.

bij te kunnen moest een "boete" worden betaald via anonieme online betaalmiddelen. Het doel was hier ook om slachtoffers zo bang mogelijk te maken zodat ze zouden betalen. In de beginjaren waren ransomware-aanvallen vaak vooral opportunistisch en simplistisch van aard: bestanden werden niet altijd daadwerkelijk versleuteld en de computer bleek vaak relatief eenvoudig weer te herstellen.[34] Maar sindsdien is er veel veranderd en is er sprake van een sterke mate van specialisering en professionalisering van cybercriminelen.[35] Op wetenschappelijk gebied is de afgelopen jaren bijvoorbeeld veel gepubliceerd over de ontwikkeling van *Ransomware-as-a-Service* (RaaS) waarbij individuen of groepen verschillende diensten kunnen afnemen binnen een goed georganiseerde criminele keten.[36] Ook het NCSC (2020) schreef over hoe groepen zich hebben gespecialiseerd in het verkrijgen van toegang tot netwerken of juist het exploiteren van deze toegang en deze verkopen aan geïnteresseerde partijen.[37] Op deze manier kunnen ook criminelen met begrensde programmeervaardigheden deelnemen en geld verdienen aan ransomware.[38]

De verwachting is dat de complexiteit van ransomware-aanvallen zal blijven toenemen en dat cybercriminelen nieuwe methoden zullen blijven ontwikkelen om opbrengsten te maximaliseren en risico's te minimaliseren.[39] Ransomware, met andere woorden, betreft een dynamisch fenomeen met grote aantallen gerichte en ongerichte aanvallen door een netwerk van verschillende partijen.[40] In de literatuur wordt daarom geregeld benadrukt dat het voor politie en justitie vaak ingewikkeld is om een volledig beeld te krijgen van ransomware-operaties. Actoren zijn vaak technisch moeilijk te traceren en er is doorgaans sprake van een hoge mate van anonimiteit, bijvoorbeeld doordat slachtoffers gevraagd worden om losgeld in bitcoins of andere cryptocurrencies te betalen.

Bovendien spelen zaken als "under-reporting" vanuit slachtoffers, terughoudendheid in het uitwisselen van informatie over ransomware, en de capaciteit bij justitie en politiediensten een rol waardoor onderzoeken soms blijven liggen.[41] Hierdoor blijft de kwaliteit en het volume van informatie beperkt verspreid waardoor het ontwikkelen van een passende en effectieve respons geen sinecure is.[42] In de literatuur

34 Ibid.

35 O'Kane, Philip, Sakir Sezer, and Domhnall Carlin. 2018. "Evolution of Ransomware." *IET Networks* 7 (5): 321–27. https://doi.org/10.1049/iet-net.2017.0207.

36 Akyazi, Ugur, M. J. G. van Eeten, and C. Hernandez Ganan. "Measuring cybercrime as a service (caas) offerings in a cybercrime forum." In *Workshop on the Economics of Information Security*. 2021.; Hyslip, Thomas S., and George W. Burruss. "Ransomware." In *Handbook on Crime and Technology*, pp. 86-104. Edward Elgar Publishing, 2023.; Blom, Tessa, Wazir Sahebali, Kimberly Deppe, Peter Romijn, Floris Donath, and Reg Brennenraedts. 2023. "Ransomeware-aanvallen op instellingen en bedrijven in Nederland." 2022.173-2319. Dialogic. https://repository.wodc.nl/bitstream/handle/20.500.12832/3292/3375-ransomware-aanvallen-op-instelllingen-en-bedrijven-volledige-tekst.pdf?sequence=7&isAllowed=y. Meland, Per Håkon, Yara Fareed Fahmy Bayoumy, and Guttorm Sindre. 2020. "The Ransomware-as-a-Service Economy Within the Darknet." *Computers & Security* 92 (May): 101762. https://doi.org/10.1016/j.cose.2020.101762.

37 Nationaal Cyber Security Centrum. 2022. "Factsheet Ransomware." Factsheet | Nationaal Cyber Security Centrum. October 28, 2022. https://www.ncsc.nl/wat-kun-je-zelf-doen/documenten/factsheets/2020/juni/30/factsheet-ransomware.

38 Meland, Per Håkon, Yara Fareed Fahmy Bayoumy, and Guttorm Sindre. 2020. "The Ransomware-as-a-Service Economy Within the Darknet." *Computers & Security* 92 (May): 101762. https://doi.org/10.1016/j.cose.2020.101762.

39 Cyberveilig Nederland. 2023. "Ransomware." https://cyberveilignederland.nl/upload/userfiles/files/CVNL_Ransomware_def.pdf ; 2018b. "Evolution of Ransomware." IET Networks 7 (5): 321–27. https://doi.org/10.1049/iet-net.2017.0207.

40 Meland, Per Håkon, Yara Fareed Fahmy Bayoumy, and Guttorm Sindre. 2020. "The Ransomware-as-a-Service Economy Within the Darknet." *Computers & Security* 92 (May): 101762. https://doi.org/10.1016/j.cose.2020.101762.

41 Ministerie van Justitie en Veiligheid. 2024. "Cyberrechercheurs Voor Één Dag." Reportage | Opportuun. February 9, 2024. https://magazines.openbaarministerie.nl/opportuun/2024/01/politiehackathon.; Robles-Carrillo, M., and P. García-Teodoro. 2022. "Ransomware: An Interdisciplinary Technical and Legal Approach." *Security and Communication Networks* 2022 (August): 1–17. https://doi.org/10.1155/2022/2806605; Institute for Security and Technology, 2021. "Combating Ransomware." https://www.in.gr/wp-content/uploads/2021/05/RTF.pdf.

42 NCTV, "Nederlandse Cybersecuritystrategie 2022-2028." Nationaal Coördinator Terrorismebestrijding En Veiligheid. https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022-2028.

wordt dan ook gewezen op het belang van een brede aanpak waarbij publieke en private partijen vanuit verschillende achtergronden samenwerken om ransomware-aanvallen te voorkomen en te bestrijden.[43] Zo wordt onder meer geconcludeerd dat voor een goede analyse van het fenomeen en een passende aanpak zowel technische als juridische kennis en kunde over ransomware samen moeten worden gebracht.[44] Maar hierbij wordt soms ook direct de kanttekening gemaakt dat de ontwikkeling van een dergelijke aanpak in de praktijk niet eenvoudig blijkt, bijvoorbeeld door bestaande juridische barrières of als gevolg van botsende belangen en concurrentie tussen de betrokken partijen.[45]

## Melissa: een public-private partnership tegen ransomware

Project Melissa is een public-private partnership (PPP), ofwel een samenwerkingsverband tussen publieke- en private partijen. Bij dergelijke samenwerkingen is er vrijwel altijd sprake van een overeenkomst tussen de partijen om te werken aan een gemeenschappelijk doel, waarbij het delen van informatie in de regel een essentieel onderdeel is. Vanwege de complexiteit en verstrekkende gevolgen van cyberaanvallen worden PPP's overal ter wereld, zowel binnen als buiten de wetenschap, als aangewezen oplossing gezien.[46] Dergelijke samenwerkingsverbanden zouden onder meer een remedie vormen tegen versnippering van informatie verspreid over verschillende partijen. Ook in de Nederlandse Cybersecuritystrategie 2022-2028 (NLCS) staat expliciet benoemd dat informatie-uitwisseling gefragmenteerd is, waardoor organisaties dreigingsinformatie mogelijk niet tijdig ontvangen, wat hen kan beletten de juiste maatregelen te treffen.[47]

Het versterken van de informatiepositie van partijen die zich bezighouden met (bescherming tegen aanvallen met) ransomware vormde ook een belangrijk uitgangspunt voor Melissa. Zo valt in het convenant te lezen:

> "Er is op het moment (..) nog te weinig zicht op de omvang van de dreiging van ransomware en gerelateerde vormen van cyber criminaliteit voor Nederland, onder andere door gebrek aan informatie(deling) tussen en gezamenlijke analyse door de partijen die een rol vervullen in het domein van bestrijden van dit type cybercriminaliteit. Partijen hebben 'stukjes van de puzzel', maar deze worden onvoldoende bij elkaar gelegd. Dit staat effectieve bestrijding in de weg".[48]

Verschillende wetenschappelijke studies geven aan dat er vaak een bepaalde spanning is binnen PPP's, gekarakteriseerd door organisatorische grenzen en verschillende belangen en bevoegdheden enerzijds

43 Robles-Carrillo, M., and P. García-Teodoro. 2022. "Ransomware: An Interdisciplinary Technical and Legal Approach." *Security and Communication Networks* 2022 (August): 1–17. https://doi.org/10.1155/2022/2806605.

44 Robles-Carrillo, M., and P. García-Teodoro. 2022. "Ransomware: An Interdisciplinary Technical and Legal Approach." *Security and Communication Networks* 2022 (August): 1–17. https://doi.org/10.1155/2022/2806605.

45 Robles-Carrillo, M., and P. García-Teodoro. 2022. "Ransomware: An Interdisciplinary Technical and Legal Approach." *Security and Communication Networks* 2022 (August): 1–17. https://doi.org/10.1155/2022/2806605; Benmalek, Mourad. 2024. "Ransomware on Cyber-physical Systems: Taxonomies, Case Studies, Security Gaps, and Open Challenges." *Internet of Things and Cyber-Physical Systems*, January. https://doi.org/10.1016/j.iotcps.2023.12.001.

46 Carr, Madeline. "Public–private partnerships in national cyber-security strategies." *International Affairs* 92, no. 1 (2016): 43-62.; Boeke, Sergei. "National cyber crisis management: Different European approaches." *Governance* 31, no. 3 (2018): 449-464.; Weiss, Moritz, and Vytautas Jankauskas. "Securing cyberspace: How states design governance arrangements." *Governance* 32, no. 2 (2019): 259-275.; Luiijf, Eric, Kim Besseling, and Patrick De Graaf. "Nineteen national cyber security strategies." *International Journal of Critical Infrastructures 6* 9, no. 1-2 (2013): 3-31.; Shackelford, Scott J., Anjanette Raymond, Danuvasin Charoen, Rakshana Balakrishnan, Prakhar Dixit, Julianna Gjonaj, and Rachith Kavi. "When toasters attack: A polycentric approach to enhancing the security of things." *U. Ill. L. Rev.* (2017): 415.; Van den Berg, Bibi, and Sanneke Kuipers. "Vulnerabilities and cyberspace: A new kind of crises." *Oxford Research Encyclopedia of Politics* (2022); Christensen, Kristoffer Kjærgaard, and Karen Lund Petersen. "Public–private partnerships on cyber security: a practice of loyalty." *International Affairs* 93, no. 6 (2017): 1435-1452.

47 NCTV. "Nederlandse Cybersecuritystrategie 2022-2028." Nationaal Coördinator Terrorismebestrijding En Veiligheid. https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022-2028.

48 Convenant Melissa (2022).

en het gedeelde gevoel van urgentie anderzijds.[49] Dit maakt dat samenwerking tussen publieke en private partijen vaak complex, kostbaar en kwetsbaar. Desondanks zien we op steeds meer gebieden pogingen tot dergelijke samenwerking.

## Een realistisch analysekader

Er liggen diverse veronderstellingen, impliciet of expliciet, ten grondslag aan de inrichting en het functioneren van Melissa. De realistische benadering beschrijft deze veronderstellingen en hoe een programma of project rust op een bepaalde logica die beschrijft hoe een zekere inspanning zal leiden tot een gewenste uitkomst. Deze logica heeft de vorm van een serie 'als - dan' premisen van de initiatiefnemers. Voor de onderstaande analyse staan we daarom eerst stil bij de causale mechanismen van Melissa en de wijze waarop ondernomen acties *in theorie* zouden moeten bijdragen aan het bereiken van het gestelde doel. Deze mechanismen vormen, als het ware, de motor van het project en bieden een verklaring voor een bepaalde uitkomst of resultaat.

Deze analyse is in eerste plaats gebaseerd op de beschikbare formele stukken vanuit het project zelf – zoals het convenant en projectplan. In aanvulling hierop hebben we verdiepende gesprekken gevoerd met leden van de kerngroep die zowel betrokken waren bij de totstandkoming van het samenwerkingsverband als een rol spelen in de huidige uitvoering hiervan. Door deze gesprekken hebben we meer inzicht gekregen in de ontwikkeling en totstandkoming van Melissa en konden eventuele impliciete veronderstellingen worden blootgelegd. De onderstaande weergave volgt dus nadrukkelijk niet uit eigen (normatieve) interpretaties maar juist uit de projectbronnen en betrokken deskundigen zelf. Later in dit hoofdstuk staan we vervolgens verder stil bij de onderbouwing van deze veronderstelde causale mechanismen: in hoeverre is het project *theoretisch-* en *evidence based*? We beoordelen volgens het realistische kader de gevonden theoretische uitgangspunten door deze te spiegelen aan (wetenschappelijke) literatuur en bredere maatschappelijke inzichten.

## Beschrijving: wat is het idee achter Melissa?

Het doel van Melissa is om Nederland een onaantrekkelijker doelwit te maken voor ransomware-aanvallen.[50] Dit overkoepelende doel wordt consistent genoemd in de bestudeerde stukken alsook in de interviews en focusgroep. In het eerdergenoemde convenant wordt vervolgens gesteld dat dit doel bestaat uit het verbeteren van de efficiëntie en effectiviteit van:

- De pakkans en mogelijkheden voor verstoring van criminele activiteiten;
- Het bieden van handelingsperspectief voor de samenleving;
- De ondersteuning van (potentiële) slachtoffers van activiteiten binnen de ransomware aanvalsketen.

Op basis van onder andere het projectplan en aanvullende gesprekken onderscheiden de onderzoekers twee dimensies aan het hoofddoel:

- *Het vergroten van de risico's en kosten* voor daders van cyberaanvallen: het vergroten van de pakkans en mogelijkheden van verstoring van criminele activiteiten.
- *Het verhogen van de weerbaarheid* van slachtoffers en de samenleving: het bieden van handelingsperspectief voor de samenleving en ondersteuning van (potentiële) slachtoffers van activiteiten binnen de ransomware aanvalsketen.[51]

In de documenten wordt niet gesproken over een hiërarchie tussen deze beide dimensies – zij staan gezamenlijk centraal binnen het samenwerkingsproject.

49 Christensen, Kristoffer Kjærgaard, and Karen Lund Petersen. "Public–private partnerships on cyber security: a practice of loyalty." *International Affairs* 93, no. 6 (2017): 1435-1452. Carr, Madeline. "Public–private partnerships in national cyber-security strategies." *International Affairs* 92, no. 1 (2016): 43-62. Dunn-Cavelty, Myriam, and Manuel Suter. "Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection." *International Journal of Critical Infrastructure Protection* 2, no. 4 (2009): 179-187.

50 Convenant Melissa (2022), p.4

51 Convenant Melissa (2022), p. 6; interne stukken.


Figuur 1: Het analysekader voor Melissa

Voor het bereiken van deze doelstelling wordt een tweetal middelen ingezet:

- Gestructureerde kennis en informatiedeling over ransomware dreigingen en incidenten.
- Verbeteren samenwerking tussen de overheid en het cybersecurity bedrijfsleven op dit terrein.

Het veronderstelde werkzame mechanisme is dat samenwerking bij de bestrijding van ransomware zal verbeteren wanneer partijen elkaar beter leren kennen en vinden. Hiervoor dienen processen en werkwijzen te worden ontwikkeld die dit faciliteren. Om uiteindelijk effectief samen te kunnen werken is er een drietal sporen geïdentificeerd waar binnen Melissa in wordt geïnvesteerd:

1. Een technisch/inhoudelijk spoor, waarbinnen onder andere een communicatiekanaal en een MISP-omgeving zijn ingericht;
2. Een juridisch spoor, waarbinnen de non-disclosure agreement (NDA) en het samenwerkingsconvenant ontwikkeld zijn en juridische uitdagingen worden gemonitord; en
3. Een praktisch/organisatorisch spoor, dat zorg draagt voor het opzetten van meetings, het vastleggen van processen en gedragsregels en het gezamenlijk communiceren van/over resultaten.

Wat betreft de uitwisseling van informatie tussen betrokken partijen draait het onder andere om het verkrijgen van een completer beeld van de aanvalsketen. Dit kan door middel van (statistisch) onderzoek en het structureel onderling delen van relevante operationele en tactische inzichten alsook door het maken van gezamenlijke (fenomeen of incident) analyses. Het samenwerkingsverband hecht veel waarde aan vertrouwen, vertrouwelijkheid, rechtmatigheid en de bescherming van (gevoelige) gegevens. Om die reden gelden bij de uitwisseling van informatie allerhande waarborgen die moeten zorgen voor de "bescherming van persoonsgegevens en het tegengaan van oneigenlijke toegang daartoe".[52]

De doelen en veronderstelde mechanismen van Melissa zijn weergegeven in figuur 1. We zullen gedurende dit rapport telkens terugverwijzen naar dit analysekader bij de bespreking van de opbrengsten, succesfactoren, de risico's en vragen voor de toekomst.

## Beoordeling: Melissa in theorie

De toegenomen dreiging van ransomware-aanvallen vormde de belangrijkste aanleiding voor de totstandkoming en de samenwerking binnen Melissa. Dit zou zogezegd het gedeelde zicht moeten verbeteren op de aard en omvang van de dreiging van ransomware in Nederland.[53] Vanuit de (wetenschappelijke) literatuur wordt de groeiende complexiteit van ransomware-aanvallen en het belang van nieuwe initiatieven ruimschoots onderschreven.

52 Convenan Melissa, 2.2

53 Convenant Melissa, p. 2.

Een belangrijk thema binnen de huidige *state-of-the-art* betreft vervolgens de intensivering van publiek-private samenwerking op dit gebied. Ondanks de nog vele openstaande vragen lijkt er sprake van consensus dat samenwerking tussen overheid (politie, openbaar ministerie, etc.) en private partijen essentieel is voor een effectieve bestrijding van ransomware-aanvallen.[54] Zo schreef het *Institute for Security and Technology* in een recent rapport: "stopping the flow of ransomware attacks requires a whole-of-society approach. Governments and the private sector alike have highlighted the need to enhance collaboration between government, law enforcement, and the private sector in order to effectively combat ransomware".[55]

Hoe dergelijke samenwerkingen tot stand zouden moeten komen, welke vorm zij zouden moeten hebben, en hoe ze duurzaam gemaakt kunnen worden blijft in de literatuur echter onderbelicht. Er wordt vaak slechts in abstracte termen gesteld dat publiek-private samenwerking een belangrijke bijdrage kan leveren aan het terugdringen van de dreiging van ransomware zonder nadere invulling.[56] Wel wordt het delen van informatie geregeld als fundamentele pijler genoemd van een dergelijke samenwerking.[57] In Nederland betoogde ook de Cyber Security Raad (CSR) al in 2020 dat het cybersecurity landschap sterk versplinterd is en dat er meer samenhang, slagkracht en snelheid nodig is.[58] De gecoördineerde uitwisseling van informatie wordt daarbij als essentieel gezien om Nederland digitaal weerbaarder te maken tegen ransomware en andere dreigingen.[59] Ook in wetenschappelijke publicaties worden publieke en private partijen geadviseerd om overeenkomsten af te sluiten om snel en in gestandaardiseerde vorm informatie te kunnen delen.[60] Door het structureel delen van inzichten tussen publieke en private organisaties kan fragmentatie van informatie(deling) worden tegengegaan en uiteindelijk een beter dreigingsbeeld ontstaan waardoor passende(re) maatregelen kunnen worden genomen. De bestaande literatuur schetst een beeld van private en publieke partijen die in relatieve isolatie ransomware-aanvallen bestuderen, terwijl juist het belang van een collectieve analyse van technische, organisationele en praktische aspecten van ransomware wordt aanbevolen om beter te kunnen anticiperen op nieuwe methoden en ontwikkelingen.[61]

54 Laitinen, Marja, and Sarah Armstrong-Smith. "Tackling cybercrime and ransomware head-on: Disrupting criminal networks and protecting organisations." *Cyber Security: A Peer-Reviewed Journal* 5, no. 3 (2022): 190-205; Vish, Elizabeth, and Georgeanela Flores Bustamante. "Public Private Partnerships to Combat Ransomware: An inquiry into three case studies and best practices." https://securityandtechnology.org/virtual-library/reports/public-private-partnerships-to-combat-ransomware/.

55 Vish, Elizabeth, and Georgeanela Flores Bustamante. "Public Private Partnerships to Combat Ransomware: An inquiry into three case studies and best practices." https://securityandtechnology.org/virtual-library/reports/public-private-partnerships-to-combat-ransomware/ p.4.

56 Overigens is er daarnaast een tekort aan gedegen kennis van, en zicht op, de empirische werkelijkheid van publiek-private samenwerking op het gebied van digitale veiligheid, alsook op de validatie van dergelijke samenwerkingen.

57 Christensen, Kristoffer Kjærgaard, and Karen Lund Petersen. "Public–private partnerships on cyber security: a practice of loyalty." *International Affairs* 93, no. 6 (2017): 1435-1452; Carr, Madeline. "Public–private partnerships in national cyber-security strategies." *International Affairs* 92, no. 1 (2016): 43-62.

58 Cyber Security Raad, 2020. "CSR Jaaroverzicht 2020", p. 17.

59 Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2022. "Nationale Cybersecuritystrategie 2022-2028". 13 -24.

60 Institute for Security and Technology, 2021. "Combating Ransomware." https://www.in.gr/wp-content/uploads/2021/05/RTF.pdf.

61 Benmalek, Mourad. 2024. "Ransomware on Cyber-physical Systems: Taxonomies, Case Studies, Security Gaps, and Open Challenges." *Internet of Things and Cyber-Physical Systems*, January. https://doi.org/10.1016/j.iotcps.2023.12.001:

Hiermee bieden de huidige maatschappelijke en wetenschappelijke inzichten een passende basis en een degelijke legitimatie voor een samenwerkingsinitiatief als Melissa. De veronderstelling dat om ransomware effectief te bestrijden, betere samenwerking en informatiedeling tussen verschillende partijen vereist is, kent derhalve voldoende theoretische grondslag.[62]

De veronderstellingen over de werking van Melissa als instrument tegen ransomware blijken bovendien niet alleen theoretisch maar ook, tot op zekere hoogte, empirisch gegrond te zijn. Zo blijkt uit de documenten en de interviews dat al voor het bestaan van deze samenwerking door de betrokken partijen relevante ervaringen opgedaan werd met onderlinge samenwerking. Verschillende gesprekpartners verwijzen bijvoorbeeld naar een bijeenkomst in 2021 waar vertegenwoordigers van de politie, OM, NSCS, Cyberveilig Nederland en verschillende cybersecuritybedrijven samenkwamen om te bespreken hoe zij elkaar in de praktijk zouden kunnen aanvullen. Hier bleek meteen dat het delen van relevante kennis tussen verschillende professionals relevante inzichten opleverde: niet alleen over wat technisch kan en juridisch mag, maar ook over concrete casuïstiek. Zo kon het gebeuren dat informatie van een private onderzoeker over een server die werd gebruikt door cybercriminelen terecht kwam bij de aanwezige vertegenwoordigers van politie en justitie en werd een paar dagen later de inhoud van de server onderdeel van het dossier. Bovendien leidden uitwisselingen tussen de verschillende partijen tot relevante nieuwe inzichten over de organisatie van ransomwaregroeperingen. Het convenant, zo werd ook al eerder geconcludeerd, vormde een bevestiging en bestendiging van eerdere ervaringen en afspraken die reeds op operationeel niveau al leken te werken.[63]

Pas toen er voldoende aanwijzingen waren die de waarde van verdere samenwerking in deze context bevestigden, besloot men deze verder te bestendigen. De formalisatie van dit initiatief ontwikkelde zich in gezamenlijkheid en is het resultaat van de actieve betrokkenheid van relevante experts en organisaties. Daarmee volgt dat Melissa zowel een theoretische- als een evidence based logica.

> More proactive insights into adversary tactics, techniques and procedures require continued malware reverse engineering and intelligence sharing between public and private organizations. (..) Sectors tend to examine attacks in isolation rather than collectively identifying cross-vertical ransomware innovations. In-depth collaborative analysis of (..) ransomware code evolution, attack infrastructure, adversarial telemetries and victim profiling is essential for anticipating - and getting ahead of - emerging techniques (..).

62 Andersom is Melissa in wetenschappelijke zin een relevante en interessante empirische casus omdat het een uitwerking is van wat in de literatuur in abstracte zin wordt aanbevolen. Daarbij wordt in het convenant en de overige documenten zichtbaar met welke mechanismen het samenwerkingsverband in concrete zin invulling geeft aan informatieuitwisseling rondom dit gekaderde thema. Voor de wetenschap is Melissa een interessante bron voor het bestuderen van bijvoorbeeld succesfactoren voor PPP's, maar ook het in de praktijk bijeenkomen van publieke en private belangen, mandaten en kaders.

63 Holterman, Liesbeth, 2024. "Over 'Melissa.'" In *Opportuun*. https://cyberveilignederland.nl/actueel/liesbeth-holterman-in-oppertuun-over-melissa, .

# 3. PRAKTIJK: OPBRENGSTEN

In dit deel van de evaluatie zoomen we in op de praktijk: wat is er tot nu toe gedaan binnen het project en wat zijn de opbrengsten en ervaringen? Eerst lichten we toe wat voor activiteiten er binnen Melissa plaatsvinden om vervolgens stil te staan bij concrete resultaten die behaald zijn (mede) dankzij deze samenwerking. Deze worden vervolgens samen met aanvullende opbrengsten weergegeven in een schema en gespiegeld met de doelen zoals beschreven in het convenant.

## Wat is er gedaan in de praktijk?

Centraal binnen Melissa staat het informatiedelen en het structureren en standaardiseren van onderlinge communicatie en informatie. Informatiedeling kent een aantal verschillende vormen met een eigen ritme en dynamiek. Zo delen deelnemers bijvoorbeeld statistieken en inzichten tijdens techsessies. Deze vonden in eerste instantie maandelijks plaats en wisselden af tussen on- en offline, maar inmiddels vinden deze eens in de zes weken fysiek plaats omdat dit beter bleek te werken. Tijdens deze sessies wordt ook een TLP-RED ronde over specifieke voorvallen besproken waarbij de gebruikte tactieken, technieken en procedures (TTP›s) worden gedeeld en geanalyseerd.[64] Daarnaast is er een gezamenlijke MISP-omgeving ingericht om informatie actueel te kunnen houden.[65] Vervolgens zijn er online communicatiekanalen (Signal en Mattermost) voor de betrokken partijen waarin ontwikkelingen en trends met elkaar worden gedeeld. Ook worden er regelmatig gezamenlijke kennissessies gehouden in verschillende formats, zoals bijvoorbeeld technische informatieuitwisselingen, maar ook "tweedaagses" met alle betrokken partijen. Bij dit laatste type event wisselen plenaire en track sessies elkaar af en worden de onderlinge banden aangehaald. Tijdens tweedaagses is er ruimte voor technische, juridische en praktische sessies, en wordt bijvoorbeeld ook over ethische en maatschappelijke dilemma's gesproken.

Al deze activiteiten van informatiedeling passen bij het subdoel om gezamenlijk een bijdrage aan de bestrijding van cybercrime.

Daarnaast zijn vanuit het samenwerkingsverband meerdere whitepapers en andersoortige kennisdocumenten gepubliceerd. Deze whitepapers bieden een toegankelijk inzicht en initieel handelingsperspectief voor organisaties op het gebied van ransomware. Zij dragen zo bij aan het andere subdoel, namelijk het verhogen van de weerbaarheid tegen cybercriminaliteit.[66]

Voor de komende periode wordt gewerkt aan de verdere ontwikkeling van MISP voor informatiedeling rondom cyberincidenten. Deze taak zal vanuit Cyberveilig Nederland worden overgedragen aan het NCSC. Ook is er aandacht voor het verbeteren van het aangifteproces voor slachtoffers van ransomware en de realisatie van een cyberloket waar incident respons partijen een incident snel bij de politie kunnen melden zodat er effectiever kan worden gehandeld.

In Figuur 2 worden de opbrengsten van Melissa samengevat. Hieronder worden de uitkomsten nader toegelicht.

## Concrete resultaten

Het samenwerkingsverband heeft een aantal in het oog springende opbrengsten gerealiseerd. Hieronder staat een opsomming van enkele publiek gedeelde resultaten waar Melissa een bijdrage aan heeft geleverd:

- De politie heeft meer dan 150 decryptiesleutels van ransomware-groep Deadbolt weten te bemachtigen tijdens een gerichte actie dankzij een tip van cybersecuritybedrijf Responders.NU.[67]

64 TLP staat voor *Traffic Light Protocol* en betreft een methode om data of informatie te classificeren en geeft richting aan het informatiedelingsproces. De verschillende categorieën zijn *Red*, *Amber*, *Green* en *White*. Bij een TLP Red mogen de ontvanger(s) de informatie uitsluitend delen met de informatieverstrekker en de medeontvangers. Ter vergelijking: bij een TLP White zit er geen beperking aan de verspreiding van de informatie en mag alles publiekelijk worden gedeeld. Een volledige bespreking is te vinden in het Cybersecurity woordenboek (2021),https://cyberveilignederland.nl/woordenboek#:~:text=Met%20het%20woordenboek%20kunnen%20gebruikers,druk%20met%20een%20nieuwe%20look.

65 MISP staat voor *Malware Information Sharing Platform* en wordt gebruikt door organisaties om informatie over cybersecurity dreigingen tussen partijen te delen. Verschillende partijen kunnen hier hun informatie invoeren/delen zodat uiteindelijk een beter beeld ontstaat van het dreigingslandschap.

66 Zie bijvoorbeeld: Nederland, 2023. "Data-exfiltratie bij een ransomware-aanval." Online via https://cyberveilignederland.nl/upload/userfiles/files/VCNL_Whitepaper_Exfiltratie_v3_0_Web.pdf.

67 "Nederlandse Gedupeerden  Geholpen in Unieke Ransomware-actie." n.d. Politie.Nl. https://www.politie.nl/nieuws/2022/


Figuur 2: opbrengsten van Melissa

- Eén van de grootste wereldwijde botnets, Qakbot, is ontmanteld tijdens een gecoördineerde, internationale operatie van opsporingsautoriteiten. Hieraan leverden ook verschillende private deelnemers van Melissa op de achtergrond een actieve bijdrage. In Nederland wisten het OM en de politie 22 servers offline te halen.[68]
- De Nederlandse Politie heeft een bijdrage geleverd aan Operation Cookiemonster. De criminele handelswebsite Genesis market is daarmee door de FBI offline gehaald. Op de handelswebsite werden onder andere social mediaprofielen verkocht en bankrekeningen geplunderd. [69]
- In maart 2024 zijn Nederlandse slachtoffers van ransomwaregroep Cactus geïdentificeerd. Dit was mogelijk doordat ransomwarestatistieken onderling gedeeld werden tussen partijen binnen Melissa. Minimaal tien Nederlandse organisaties waren doelwit van Cactus. Deze organisaties konden, door ze tijdig te informeren, passende tegenmaatregelen nemen.[70]
- Dankzij een tip vanuit een private partij binnen Melissa kon team High Tech Crime van de Nederlandse Politie onderzoek doen naar ransomware-groep Lockbit. Met dit onderzoek heeft dit team bijgedragen aan een internationale verstoringsactie. [71]

oktober/14/09-nederlandse-gedupeerde-geholpen-in-unieke-ransomware-actie.html.

68 Ministerie van Justitie en Veiligheid. 2023. "Grootste Wereldwijde Botnet Qakbot Onschadelijk Gemaakt." Nieuwsbericht | Openbaar Ministerie. September 4, 2023. https://www.om.nl/actueel/nieuws/2023/08/29/grootste-wereldwijde-botnet-qakbot-onschadelijk-gemaakt.

69 "Wereldwijd Aanhoudingen Voor Online Identiteitsdiefstal Miljoenen Mensen." 2023. Politie.Nl. April 5, 2023. https://www.politie.nl/nieuws/2023/april/5/operation-cookiemonster-nl.html.

70 "Samenwerkingsverband Melissa Vindt Diverse Nederlandse Slachtoffers Van Ransomwaregroepering Cactus." n.d. Digital Trust Center (Min. Van EZ). https://www.digitaltrustcenter.nl/nieuws/samenwerkingsverband-melissa-vindt-diverse-nederlandse-slachtoffers-van-ransomwaregroepering.

71 "Servers Neergehaald Van 'S Werelds Grootste Ransomware Groepering." 2024. Politie.Nl. February 20, 2024. https://www.politie.nl/nieuws/2024/februari/20/09-servers-neergehaald-van-s-werelds-grootste-ransomware-groepering.html.

- Met het whitepaper "Ransomware", dat uitgebracht is door Cyberveilig Nederland en tot stand gekomen is met de samenwerkingspartners in Melissa, geeft het consortium organisaties inzicht in ransomware om zo bij te dragen aan hun weerbaarheid. Zo worden er onder andere maatregelen omschreven om ransomware-aanvallen te voorkomen. [72]
- Melissa bracht ook de whitepaper "Data-exfilitratie bij een ransomware-aanval" voort. Het doel van dit document is om inzicht te geven in het proces van exfiltratie door cybercriminelen. Met kennis van dit proces kunnen organisaties zich beter wapenen tegen dit fenomeen.

## Overstijgende opbrengsten

In aanvulling op bovenstaande concrete resultaten worden er in de interviews diverse algemene – of overstijgende – opbrengsten geïdentificeerd. Deze resultaten van Melissa staan schematisch weergegeven in figuur 2 hierboven.

### *Ethisch vermogen*

De samenwerking binnen Melissa heeft ethische grenzen bij het bestrijden van ransomware zichtbaarder gemaakt. Verschillende respondenten geven aan dat door intensieve gesprekken, onder andere gevoerd in kennissessies en tweedaagses, binnen het consortium helderder is geworden welke ethische kaders publieke en private partijen gezamenlijk willen volgen in hun drive om ransomware aanvallen te bestrijden. De uitwisselingen binnen Melissa laten zien dat het waarborgen van een gedeeld moreel kompas cruciaal is, niet alleen voor de samenwerking, maar ook voor de samenleving die profijt heeft van deze samenwerking. Tijdens de gevoerde gesprekken zijn ook de negatieve consequenties van mogelijke overtredingen door betrokken partijen benoemd. De juridische en ethische kaders zijn daarmee duidelijker geëxpliciteerd voor alle deelnemers aan het consortium. Ook wordt er gewerkt aan een klachtenreglement voor deelnemers.

### *Elkaar weten te vinden*

Naast de gestandaardiseerde momenten waarop de partijen binnen Melissa contact met elkaar hebben, spreken zij elkaar ook regelmatig buiten deze momenten om, bijvoorbeeld bij een conferentie of tijdens hun dagelijkse werk. Respondenten geven aan dat de lijntjes tussen de betrokken publieke en private partijen veel korter zijn geworden. Zowel in formele als informele verbanden weet men elkaar nu beter te vinden. Deze korte lijnen dragen bij aan een weerbaarder ecosysteem, omdat actuele relevante informatie snel en effectief gedeeld wordt tussen betrokkenen. De hierboven genoemde concrete successen zijn een direct resultaat van het feit dat partijen elkaar beter en gemakkelijker weten te vinden.

### *Inzicht in elkaars werkwijze*

Doordat de partijen binnen Melissa nadrukkelijker met elkaar in contact staan is ook het bewustzijn over de verschillende posities, de (soms op gespannen voet verkerende) belangen, en de verschillende werkwijzen gegroeid. Men geeft aan beter te weten hoe elkaar te benaderen en welke informatie mogelijk relevant is voor de ander. Ook is men bekender geworden met de eventuele problemen waar partijen tegenaan lopen door deze gezamenlijk te bespreken. Door een dieper besef van de belangen en werkwijzen van de ander kan beter geanticipeerd worden op mogelijke obstakels en slagen partijen er beter in om daar omheen te werken.[73]

### *Verbeterde communicatie*

Door de formalisering van Melissa en de afspraken die binnen dit samenwerkingsverband gemaakt zijn is er een zekere volwassenheid in de samenwerking ontstaan. Hierdoor is de onderlinge communicatie sterk verbeterd en is volgens respondenten bovendien een nieuw soort openhartige gesprekken ontstaan. Doordat dezelfde groep mensen regelmatig bij elkaar komen groeit het vertrouwen in de groep, waardoor "je makkelijker met elkaar praat en informatie met elkaar deelt", zo stelt een van de betrokkenen.[74]

72 Cyberveilig Nederland, 2023. Whitepaper Ransomware. https://cyberveilignederland.nl/upload/userfiles/files/CVNL_Ransomware_def.pdf.

73 Respondent 2, Interview

74 Respondent 3, Interview

# 4. ERVAREN SUCCES- EN RISICOFACTOREN

De resultaten van de samenwerking zoals besproken in het vorige hoofdstuk, maar ook de samenwerking als zodanig, zijn te verklaren vanuit een combinatie van factoren die bijdragen aan de behaalde positieve resultaten. In dit hoofdstuk staan we nader stil bij de verklaringen voor succes als ook de ervaren risico's voor Melissa. Welke succesfactoren en risico's voor Melissa kunnen er worden geïdentificeerd? Deze succesfactoren, risico's en drempels zijn door respondenten gedeeld tijdens de interviews en de bijeenkomst met de focusgroep. Daarnaast hebben we ze waargenomen tijdens de participatieve observatie bij de tweedaagse bijeenkomst.

## Succesfactoren

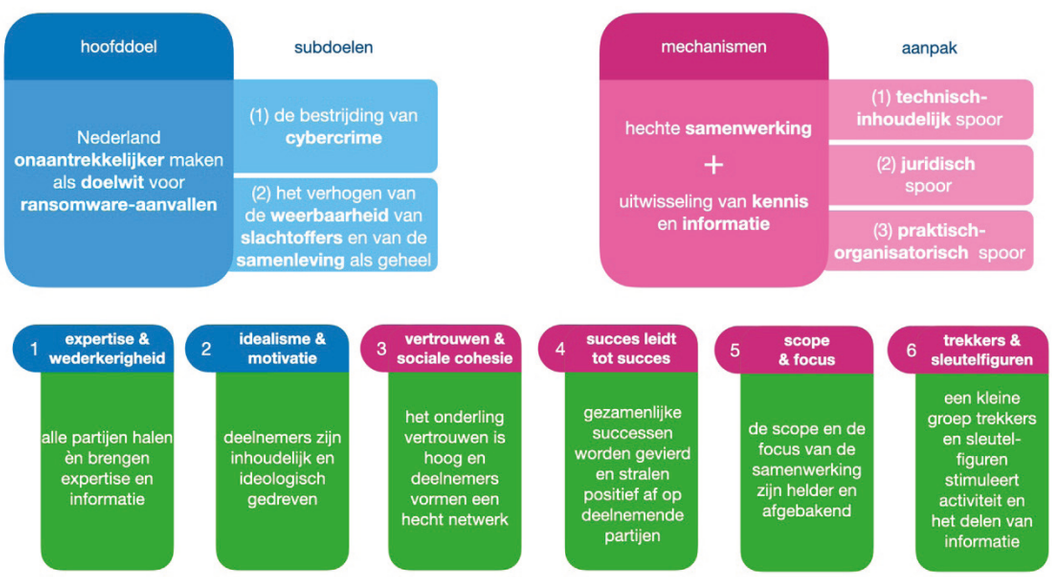
We richten ons eerst op de diverse succesfactoren die uit het bronnenmateriaal naar voren komen. Deze raken een breed aantal thema's die zijn samengevat in figuur 3.

### *Expertise en wederkerigheid*

De expertise en positie van de aangesloten stakeholders vormt een eerste relevante succesfactor. Volgens de respondenten zijn onder andere het juiste aantal partijen aangesloten (niet te veel en niet te weinig), waardoor informatieuitwisseling snel en makkelijk plaatsvindt. Daarnaast beschikken de betrokken professionals over de juiste kennis en vaardigheden om een waardevolle bijdrage te kunnen leveren aan het project. Van alle betrokkenen wordt verwacht dat zij relevante inzichten delen, en niet deelnemen om alleen maar informatie op te halen. De uitwisseling binnen Melissa is georganiseerd op basis van *quid pro quo*. Uiteraard kan het voorkomen dat een stakeholder tijdens een of enkele bijeenkomsten geen bijdrage kan leveren. Maar alle respondenten zijn het erover eens dat wanneer dit structureel het geval is, betrokkenheid binnen Melissa dient te worden heroverwogen. Volgens de respondenten is dit principe van wederkerigheid één van de voorwaarden voor een effectieve samenwerking.

### *Intrinsieke motivatie en doelen*

Aanvullend wordt meermaals aangegeven in de interviews dat er sprake is van een sterke intrinsieke motivatie van de deelnemers. De meesten delen een haast idealistische kijk op het bestrijden van ransomware. Voor hen staat het veiliger maken van Nederland en het beschermen van (potentiële) slachtoffers voorop. Daarnaast geldt dat voor individuele betrokkenheid in de regel sprake is van een sterke inhoudelijke drijfveer. Melissa biedt een interessante omgeving waar men veel over alle aspecten van ransomware en haar manifestaties kan leren. In meerdere interviews




Figuur 3: Succesfactoren van Melissa

werden de betrokken professionals binnen Melissa bestempeld als "vakidioten" die gegrepen zijn door de materie.[75] Dit is belangrijk want betrokkenheid bij dit samenwerkingsverband verloopt vaak langs de lijn van vrijwilligheid. Met andere woorden, er is doorgaans geen budget of uren gekoppeld aan de inspanningen die stakeholders leveren binnen Melissa.

### *Vertrouwen en sociaal klimaat*

In veel interviews kwam ook het positieve sociale klimaat binnen Melissa naar voren. Eén van de respondenten sprak zelfs over een "geïnstitutionaliseerde vrijdagmiddagborrel".[76] De gedeelde motivatie en het feit dat er samengewerkt wordt in een vaste groep draagt bij aan een positieve sfeer binnen het project. De professionals geven aan graag aanwezig te zijn bij de georganiseerde sessies waar ook voldoende ruimte wordt geboden voor informele gesprekken. Juist deze informele interacties worden als zeer belangrijk gezien. Dit vertaalt zich ook naar momenten buiten Melissa waar de betrokken professionals elkaar geregeld tegenkomen; het Nederlandse cybersecurity landschap is immers niet heel groot.[77] Het formeel en informeel kunnen samenwerken met een relatief vaste groep stimuleert het vertrouwen onderling.

### *Succes leidt tot succes*

Ook het behalen van concrete resultaten, zoals het offline halen van Genesis Market, zorgt voor een aanhoudende positieve sfeer en hoge motivatie binnen de groep. Respondenten noemen het ook wel een "hier wil je bij zijn"-gevoel.[78] Resultaten worden gezien en gevierd als gezamenlijk succes, maar partijen geven aan ook individueel erkenning te krijgen voor hun bijdrage. Dat is voor het vertrouwen van deze organisaties, gezien vanuit het oogpunt van hun klanten, ook goed. Door de successen van Melissa te communiceren naar de klanten groeit het vertrouwen in de diensten die de organisaties leveren.

### *Scope en focus*

Het samenwerkingsverband Melissa kent een duidelijke afbakening, waardoor de focus optimaal blijft. Die afbakening is aan de ene kant inhoudelijk: de samenwerking richt zich op een ingekaderd onderwerp, namelijk ransomware. Hoewel ransomware zich doorheen de tijd gemuteerd heeft in termen van gebruikte technieken, de professionaliteit van daders, de gekozen slachtoffers, de omvang en de impact, blijft de kern van het fenomeen en het oogmerk erachter gelijkluidend. Daardoor is er een stabiele focus en een heldere scope. Tegelijkertijd is er door de ontwikkelingen rondom ransomware voldoende dynamiek voor het consortium om de meest recente inzichten met elkaar te blijven delen en zo gezamenlijk in te kunnen spelen op de genoemde ontwikkelingen.

Het (er)kennen van en omgaan met ethische en juridische kaders zorgt eveneens voor focus en heeft een positief effect op de scope van de samenwerking. Die kaders bieden handvatten waardoor het consortium koersvast blijft ten aanzien van de gedeelde doelstellingen.

### *Voortrekkers en sleutelfiguren*

Tot slot erkennen de partijen ook de rol van de trekkers van het samenwerkingsverband. Zij organiseren bijeenkomsten en stimuleren de partijen om actief informatie te delen met elkaar. Ook zorgen zij ervoor dat de verwachtingen helder blijven. Volgens de respondenten zou het succes van een PPP niet af moeten hangen van individuen, maar zoals een van de respondenten aangeeft: "Elk project kent voortrekkers, die zul je altijd nodig blijven hebben. Dit is niet anders in andere sectoren".[79]

## Bestaande risico's en drempels

Ondanks een goede samenwerking en de aanzienlijke successen die al behaald zijn met Melissa gaf de evaluatie ook inzicht in een aantal risico›s en drempels waar de partijen tot heden mee te maken hebben gekregen. Figuur 4 vat deze risico's samen. Opvallend is dat deze risico›s en drempels nauw verbonden zijn met de succesfactoren.

75 Respondent 5, interview

76 Respondent 4, interview

77 Respondent 3, interview

78 Respondent 1, interview

79 Respondent 2, interview


Figuur 4: Risico›s van Melissa

### *Investeringen*

Partijen die betrokken zijn bij het samenwerkingsverband Melissa nemen deel op vrijwillige basis. Dit houdt in dat er geen uren of financiële middelen gekoppeld zijn aan de investering en bijdragen die de partijen leveren. Aan de ene kant benoemen de partijen dat dit een voordeel is – zo blijft deelname laagdrempelig en behoudt de samenwerking een informeel karakter. Aan de andere kant wordt het ook als een drempel gezien. Het lukt de partijen bijvoorbeeld niet altijd om op tijd informatie aan te leveren, bijvoorbeeld doordat er drukke periodes zijn binnen de eigen organisatie.

### *Spanning met waarborgen en grenzen*

Aansluitend op het gesprek over ethiek geven respondenten aan dat het delen van (gevoelige) informatie soms ingewikkeld blijft. Een risico is dat informatie soms niet met partijen gedeeld mag of kan worden en dat er dus beperkingen bestaan ten aanzien van informatiedeling. Dit kan een belemmering vormen voor het maximaal benutten van de samenwerking en, belangrijker nog, voor het zo effectief mogelijk bestrijden van ransomware aanvallen. Een respondent geeft aan dat er behoefte bestaat aan wettelijke kaders die iets meer handelingsruimte zouden bieden.[80] Tegelijk is een verruiming van wettelijke kaders gemakkelijker gezegd dan gedaan, en moet een dergelijke verruiming altijd worden afgewogen tegen potentiële risico's enerzijds en de vrijheden en belangen van individuen en groepen anderzijds. Het is bovendien de vraag of verruiming van de wettelijke kaders de enige oplossing is of dat een herinterpretatie van bestaande wetgeving, of het maken van aanvullende vastgelegde afspraken tussen politie, justitie en cybersecurity bedrijven, voldoende ruimte zouden kunnen bieden voor het effectiever bestrijden van ransomware.[81] Op dit moment loopt een verkenning naar deze laatste mogelijkheid.

Daarnaast werd binnen Melissa duidelijk dat samenwerken soms ook ethische dilemma's met zich meebrengt. Met name voor politie en justitie kan het ingewikkeld zijn wanneer informatie wordt gedeeld waar zij niets mee kunnen vanuit hun taakstelling of die hier zelfs mee in strijd lijkt.[82] Een dergelijke latente

80 Respondent 6, interview

81 Respondent 2, interview

82 Respondent 1, Interview

spanning is wellicht inherent aan samenwerking tussen publieke en private partijen met eigen waardestructuren en soms botsende belangen. Tegelijk houden partijen elkaar door het bespreekbaar houden van die spanning juist ook scherp, nodigen zij elkaar uit om na te denken over het verleggen van bestaande grenzen en zoeken zij gezamenlijk naar de maximale speelruimte die recht doet aan het morele kompas en een gedreven optreden faciliteert.

### *Het wegvallen van sleutelfiguren*

In het deel over de opbrengsten van Melissa werd al gemeld dat één van de succesfactoren van deze PPP is dat een beperkte groep sleutelfiguren een trekkersrol vervuld binnen Melissa, en zo de samenwerking aanjaagt en inspireert. Tijdens de interviews, de focusgroep en de participatieve observatie bij de tweedaagse bijeenkomst werd telkens bevestigd wat het belang is van deze sleutelfiguren. Een risico is dat deze sleutelfiguren moeilijk te vervangen zijn wanneer zij wegvallen, zeker als er meerdere personen tegelijk vertrekken. In dat geval bestaat de kans dat het de resultaten van de samenwerking negatief beïnvloed worden, en kan zelfs de continuïteit van Melissa onder druk komen te staan.[83]

### *Implementatie van informatiedelingssysteem*

Het gebruik van het systeem waarmee technische informatie wordt uitgewisseld, MISP, verliep soms stroef. Dit zorgde bij meerdere partijen voor frustratie omdat het, wegens andere verplichtingen, voor hen niet altijd haalbaar was om de data in het systeem aan te vullen. Het gevolg hiervan is dat het informatiedelingsproces vertraagd wordt, omdat deze data gedeeld en verrijkt wordt tijdens de technische sessies. Bij afwezigheid van deze informatie kan deze verrijking niet naar behoren plaatsvinden.

83 Respondent 5, interview

# 5. TOEKOMST: KANSEN EN UITDAGINGEN

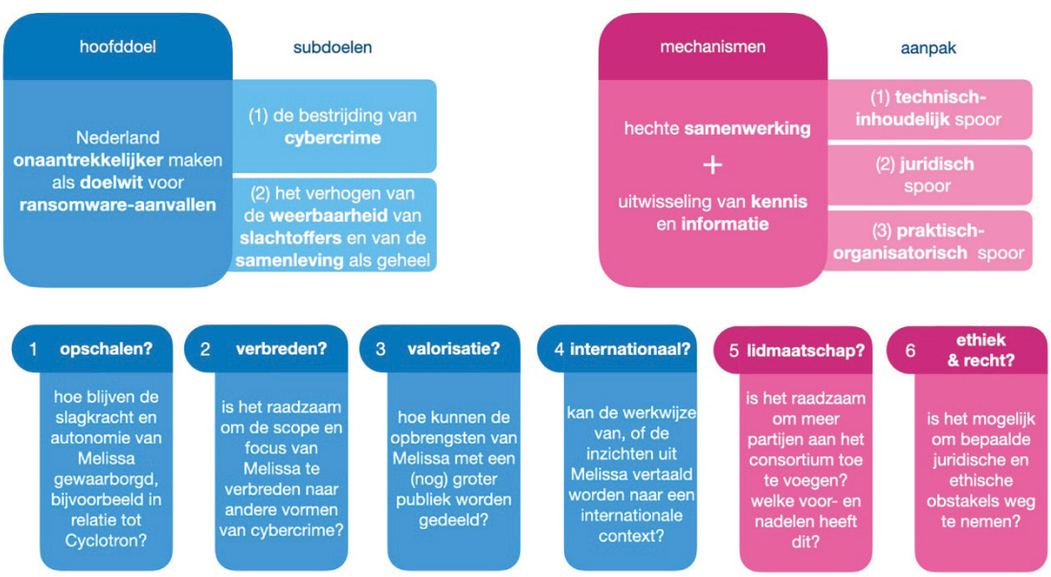
De afgelopen jaren zijn mede dankzij de samenwerking binnen Melissa de nodige successen geboekt in de bestrijding van ransomware in Nederland. In het vorige hoofdstuk zijn de mogelijke succesfactoren en risico's reeds uitgelicht. De onderstaande paragrafen richten zich op de toekomst van project Melissa. Welke kansen en ontwikkelingsvragen dienen zich aan? En voor welke (mogelijke) uitdagingen staat het samenwerkingsverband? Figuur 5 geeft de belangrijkste vragen schematisch weer.

## Van start-up naar scale-up?

De periode vanaf de start van de informele samenwerking, via de consolidatie daarvan in het ondertekende convenant en eindigend met dit evaluatiemoment markeert de eerste fase van Melissa. In deze periode stond onder meer de inrichting van de sporen en organisatorische aspecten ter bevordering van de samenwerking centraal. Op deze manier kregen de diverse betrokkenen meer inzicht in elkaars informatiepositie en werkzaamheden. Het faciliteerde dat professionals van elkaar konden leren en versterkte netwerken tussen de partijen.

De komende periode zal meer draaien om de ontwikkeling van start-up naar scale-up. Streeft men bijvoorbeeld naar een duurzame inbedding van Melissa in het bredere Nederlandse cybersecurity landschap? En zo ja, hoe geef je dit organisatorisch vorm? Met name de toekomstige verhouding tot andere initiatieven op het gebied van publiek-private samenwerking – zoals het programma Cyclotron van de Rijksoverheid – is in de interviews meer dan eens benoemd. Belangrijk lijkt uiteindelijk dat voor een structureel succes de energie, de slagkracht en de gevoelde autonomie binnen Melissa behouden blijft in dit proces van doorgroeien. Ook het belang van de vertrouwensband en het beleefde gedeelde idealisme zijn randvoorwaardelijk voor een succesvolle toekomst. Daarbij lijkt integratie in een rijksbreed programma geen verstandige richting, maar er zijn zeker waardevolle lessen te leren vanuit Melissa voor Cyclotron en andere PPP's.

Bij alle keuzes die voor de toekomst van Melissa gemaakt worden zal zorgvuldig afgewogen moeten worden wat de impact op de genoemde vijf factoren (energie, slagkracht, autonomie, vertrouwen en gedeeld idealisme) is, en op welke wijze zij gewaarborgd worden. De doorontwikkeling van Melissa raakt een aantal kwesties die we hieronder verder zullen bespreken.




Figuur 5: de belangrijkste vragen voor (de toekomst van) Melissa

### Thematiek verbreden?

De heldere scope en focus van project Melissa wordt, zoals eerder benoemd, als één van de succesfactoren van het project gezien. Sommige partijen binnen het consortium stellen de vraag of het waardevol zou zijn om de scope van het project toch te verbreden en ook informatie te delen over andere, aanpalende, cybersecurity thema's. Als reden voor deze verbreding wordt genoemd dat diverse organisaties ook andere ontwikkelingen zien die waarschijnlijk relevant zijn voor de partijen die actief zijn binnen Melissa. Hoewel zij deze inzichten graag willen delen voelen zij dat hier niet altijd ruimte is binnen de huidige kaders. De duidelijke afbakening zoals die nu bestaat zorgt ook voor kwaliteit, structuur, houvast en normatieve en juridische kaders; eventuele verbreding kan die zaken onder druk zetten.

### Nieuwe en huidige leden?

Melissa heeft een goede reputatie opgebouwd. Ondanks dat betrokkenheid bij Melissa een substantiële investering vergt, geven organisaties en professionals aan graag een rol te spelen binnen het project. Niet alleen geven ze aan veel van elkaar te kunnen leren en relevante netwerken (verder) te vormen, maar lijkt betrokkenheid hen ook een zekere professionele legitimiteit te bieden. In verschillende gesprekken komt naar voren dat organisaties graag met Melissa, haar successen en de andere partners worden geassocieerd. Dit is onder meer het resultaat van het structureel breed erkennen van inspanningen van partners voor behaalde resultaten. Dergelijke positieve opbrengsten wekken de interesse van nieuwe geïnteresseerde partijen. Dit betekent dat het samenwerkingsverband in de toekomst verder kan groeien.

Een wijziging in het aantal betrokken stakeholders binnen Melissa brengt niet alleen nieuwe kansen maar ook punten van aandacht met zich mee. Ten eerste blijft het van belang om toe te zien op de inbreng van huidige en nieuwe leden. Zijn alle partijen in staat om structureel relevante kennis en informatie te delen en zo bij te dragen aan effectieve samenwerking? Ten tweede geldt dat te veel wijzigingen in het deelnemersbestand - toetreding of vertrek van leden – sociale cohesie en vertrouwen kunnen beïnvloeden. Tegelijkertijd geven verschillende respondenten aan dat er altijd ruimte is voor nieuwe gezichten binnen Melissa die een beduidende bijdrage kunnen leveren. Over toetreding, lidmaatschap en de betrokkenheid van overige stakeholders zijn in het volgende hoofdstuk een aantal aanbevelingen opgenomen.

### Over grenzen heen?

Ook in deze evaluatie is meermaals benoemd dat ransomware-criminelen zich niet aan landsgrenzen houden en dat zij georganiseerd samenwerken binnen internationale netwerken. Tijdens de interviews gaven diverse betrokkenen aan dat ook voor de bestrijding van ransomware goed contact met organisaties in andere landen waardevol is. Zo gaven respondenten van private partijen met vestigingen in andere landen bijvoorbeeld aan dat zij geregeld nieuwe kennis en inzichten verkrijgen via hun buitenlandse partners. Bovendien kwam in de interviews en tijdens de focusgroep een gevoel van trots en eigenaarschap over de successen van Melissa ter sprake, waaruit de vraag voortvloeit of, en in welke mate, een samenwerking als Melissa ook zou kunnen worden ingericht in en tussen Europese landen. Kort gezegd: zou Melissa een exportproduct kunnen zijn? Een van de respondenten zei daarover dat dit in theorie mooi klinkt, maar dat er wel degelijk "flinke haken en ogen" aan zitten.[84] De grote wettelijke en bestuurlijke verschillen tussen landen vormen een fundamentele barrière voor de eenvoudige oprichting van een internationale equivalent van Melissa waarbij informatie tussen relevante partijen uitwisseling centraal staat. Bovendien zijn er grote culturele verschillen, waardoor een samenwerking zoals die tussen de betrokken publieke en private partijen in Nederland wellicht in andere landen niet , of niet zo eenvoudig, tot stand zou kunnen komen. Desondanks blijft het de moeite waard om de verbinding met partners uit andere landen te blijven zoeken en liggen er vragen over hoe die samenwerking dan het beste gestalte kan krijgen, met welke landen en met welke internationale stakeholders.

### Ethische dilemma's

Zoals ook in het vorige hoofdstuk besproken zijn binnen Melissa ook de ethische grenzen en dilemma's bij het bestrijden van ransomware zichtbaar gemaakt. Daarmee is echter de discussie niet gesloten en blijft het noodzakelijk om gezamenlijk te blijven zoeken naar ethische methoden voor effectieve samenwerking.

84 Respondent 3, interview

Voor de politie blijft het bijvoorbeeld soms lastig om details te delen, terwijl dat volgens sommigen best nuttig zou kunnen zijn. Voor commerciële partijen kan delen soms lastig zijn vanwege het beschermen van hun bedrijfsbelang. Een gedeelde zorg is het gevaar dat gevoelige informatie op de één of andere manier op straat zou komen te liggen. Sommige respondenten geven aan soms meer te willen doen tegen ransomware criminaliteit dan de gedoogde kaders daadwerkelijk toelaten. Het gezamenlijk evalueren van de huidige kaders en het informeren van bestuur en maatschappij over bestaande ethische dilemma's blijft daarmee ook in de toekomst van belang.

### Valorisatie en publiekseducatie

Hoe kunnen de opgedane ervaringen en kennis binnen Melissa verder worden verspreid? In de voorgaande periode hebben whitepapers, interviews en persberichten over succesvolle operaties de dreiging van ransomware voor een breder publiek meer tastbaar gemaakt. Dergelijke initiatieven dragen bij aan het behalen van de overkoepelende doelstelling: het verhogen van de algehele weerbaarheid van samenleving en slachtoffers. Voor de toekomst blijft het dan van belang om de gezamenlijk verkregen inzichten binnen Melissa toegankelijk te maken voor de Nederlandse samenleving. De uitdaging ligt hem dan vooral in het zorgen voor diversiteit van publieke output en het vinden van een balans met alle andere werkzaamheden binnen het project.

# 6. CONCLUSIES EN AANBEVELINGEN

Ransomware vormt een serieuze bedreiging voor de Nederlandse overheid en het bedrijfsleven. De noodzaak van effectieve samenwerking wordt inmiddels breed onderschreven en vormde tevens de aanleiding voor de totstandkoming van het bijzondere samenwerkingsverband Melissa. In dit hoofdstuk staan we stil bij de inzichten van dit evaluatieonderzoek. We beginnen dit hoofdstuk met een bespreking van de belangrijkste conclusies en een aantal aanbevelingen. Tot slot staan we stil bij een aantal algemene lessen die volgen uit dit project die mogelijk van waarde zijn voor andere (bestaande of toekomstige) samenwerkingsverbanden.

## Conclusies

De samenwerking tussen publieke en private partijen binnen Melissa is zondermeer waardevol gebleken in de strijd tegen ransomware. Het initiatief vormde een reactie op een landschap gekenmerkt door fragmentatie van informatie en kennis, waardoor ransomwaredreigingen niet effectief konden worden geïdentificeerd en bestreden. In hoofdstuk 2 is stilgestaan bij de theoretische en empirische basis van Melissa. Zowel wetenschappelijke inzichten als praktische ontwikkelingen op het gebied van ransomware onderschrijven het belang van intensieve samenwerking tussen de overheid en het cybersecurity bedrijfsleven. Door informatiedeling, kennisontwikkeling en afstemming van werkwijzen en processen centraal te zetten, heeft Melissa deze ervaren noodzaak van meer samenwerking passend weten te concretiseren. Hierbij was sprake van een incrementeel proces en vormden eerder opgedane ervaringen een solide fundament voor het samenwerkingsconvenant dat in 2023 werd ondertekend.

De samenwerking binnen Melissa heeft zich vervolgens op diverse manieren gematerialiseerd. In het oog springend zijn natuurlijk de succesvolle acties tegen criminele ransomware groeperingen die het (inter-)nationale nieuws haalden. Ook zijn er interviews en whitepapers gepubliceerd bijdragen aan het bestrijden van cybercrime en het verhogen van de weerbaarheid van slachtoffers. Minder breed zichtbaar, maar cruciaal voor de samenwerking, zijn de georganiseerde bijeenkomsten, werksessies en online uitwisselingen. Deze vormden een belangrijke basis voor bovengenoemde successen als een stimulans voor professionele ontwikkeling en netwerkvorming. Professionals die langer en korter in het veld zitten, konden zo nieuwe kennis en ervaringen opdoen. Ze geven aan elkaar hierdoor nu makkelijker te kunnen vinden. Bovendien zijn tijdens de diverse bijeenkomsten de ethische kaders van de opsporing en bestrijding van ransomware binnen de gehele keten geëxpliciteerd waardoor het algemene bewustzijn van de juridische grenzen en mogelijkheden kon groeien. Deze evaluatie toont dat de brede opbrengsten van Melissa op sommige punten voorbijgaan aan de initieel geformuleerde verwachtingen van informatiedelen en samenwerking bevorderen. De gedeelde verwachting is dat Melissa, ongeacht haar toekomstige koers, een duurzame impact heeft gehad op de cybersecuritysector in Nederland.

Tenslotte zijn in het laatste deel de belangrijkste succesfactoren en toekomstvragen besproken. Sociale relaties, vertrouwen, heldere normen en een sterk gevoeld gedeeld belang vormen de belangrijkste drijvende krachten achter de behaalde resultaten van Melissa. Bepaalde leden vormden daarbij een onmisbare schakel binnen Melissa door een aanjagende rol te spelen bij de organisatie en het stellen (en bewaken) van normen. Daarnaast zorgden de successen en de gedeelde erkenning van eenieders rol hierin voor momentum en energie binnen het project.

Samenwerkingsverbanden tussen publieke en private partijen komen niet vanzelf tot stand en zijn geen sinecure. Dit geldt ook voor Melissa. Het is een intensief project en de organisatie en uitvoer vergt structurele inspanning van betrokken stakeholders. Hierin schuilt ook een zekere kwetsbaarheid. De komende periode zal de doorontwikkeling van Melissa centraal staan. Hiervoor ligt nu een mooi fundament.

## Aanbevelingen

Uit deze evaluatie volgen een aantal aanbevelingen ter overweging voor het vervolgtraject van Melissa:

### *Begrens het project en behoudt focus*

Het is verleidelijk om de grenzen van Melissa te verleggen. Zo bestaan er allerhande acute cybersecurity vraagstukken die vragen om meer en betere samenwerking tussen organisaties. Het verbreden van de thematische focus van Melissa biedt in theorie de mogelijkheid om ook kennis en informatie uit te

wisselen over dergelijke andere dreigingen. In de praktijk zal het risico zijn dat de aandacht te veel verdeeld zal raken waardoor gerichte betrokkenheid in het gedrang komt. Een bredere samenwerking vraagt om een grotere inzet van middelen en meer partijen met een diversiteit aan expertise. De complexiteit en uitdagingen van het project zal hierdoor waarschijnlijk enkel verder toenemen.

### *Behoud autonomie*

Eén van de vragen die voorligt is hoe Melissa zich in de toekomst wil verhouden tot andere PPP's in het cybersecurity domein en/of het Rijksbrede samenwerkingsprogramma Cyclotron. Vanuit dat programma, en vanuit andere gremia, wordt soms druk uitgeoefend om Melissa bijvoorbeeld te integreren, om lessons learnt te genereren die als voorbeeld kunnen dienen, of om in een adviserende rol op te treden voor Cyclotron of andere PPP's. Op basis van de succesfactoren van Melissa bevelen we aan de autonomie van Melissa zorgvuldig te waarborgen. De gedeelde ideologie, de korte lijnen, de inhoudelijke expertise en de sterke gevoelde vertrouwensbasis maken dit samenwerkingsverband tot een succes. Al deze succesfactoren komen onder druk te staan door integratie met andere initiatieven. Het delen van lessons learnt is zeker waardevol. Een adviserende rol kan interessant zijn, zeker ook om wederkerigheid met andere PPP's te bewerkstelligen. Gezien de beperkte menskracht en middelen moet goed worden afgewogen welke ruimte hiervoor beschikbaar is.

### *Evalueer toetreding en lidmaatschap*

Wat betreft het samenwerkingsverband zelf, is er een noodzaak om doorlopende aandacht te besteden aan de structuur van lidmaatschap en de processen van toetreding. Het landschap van ransomware en cybersecurity is dynamisch. Dit kan leiden tot een behoefte aan nieuwe expertise en leden maar er misschien ook voor zorgen dat bestaande leden na verloop van tijd een minder centrale rol zullen vervullen. Tegelijkertijd geldt dat continuïteit van individuele betrokkenheid van groot belang wordt geacht om vertrouwen en herkenbaarheid binnen de samenwerking van centraal belang te waarborgen. Dit maakt het evalueren van toetreding maar ook van duurzaam lidmaatschap een belangrijk proces. Zorg dat er passende (ballotage) procedures blijven bestaan die hierbij helpen.

### *Onderzoek mogelijkheden naar betrokkenheid breder veld*

De samenwerking binnen Melissa heeft geleid tot een solide netwerk van organisaties actief in de opsporing en bestrijding van ransomware. Hierboven is reeds aanbevolen de focus en de omvang van Melissa te begrenzen en de autonomie zorgvuldig te bewaken. Tegelijkertijd is het de moeite waard om te verkennen of andere gespecialiseerde cybersecurity partijen een perifere rol kunnen spelen binnen het project. Te denken valt aan die professionals die misschien niet aan alle voorwaarden van lidmaatschap voldoen – bijvoorbeeld omdat zij niet beschikken over relevante informatie die zij kunnen delen - maar wel over relevante vaardigheden en kennis beschikken. Zij zouden mogelijk een schil kunnen vormen om het project en vanuit deze rol een bijdrage kunnen leveren in bijvoorbeeld de ontwikkeling van nieuwe (kennis) producten zoals whitepapers en zo relaties binnen het Nederlandse cybersecurity domein versterken.

### *Blijf ethische dilemma's benoemen en onderzoeken*

Melissa heeft geleid tot een aantal succesvolle gezamenlijke operaties, maar ook tot gedeelde reflecties op een moreel kompas bij de bestrijding van ransomware. Door informatie en ervaringen uit te wisselen over de juridische context waarin de verschillende partijen zich bewegen kan het handelingsperspectief van alle betrokkenen concreter gemaakt worden en worden aangescherpt. Daarnaast kunnen ethische discussies soms ook zichtbaar maken waar de praktijk en het recht kunnen schuren. Dit kan een startpunt vormen voor discussies over nieuwe werkvormen of voor de ontwikkeling van nieuwe beleidskaders. Juridische kaders veranderen door de tijd heen, en hetzelfde geldt voor de aard, omvang en impact van ransomware aanvallen. Om die reden is het van belang om binnen Melissa structureel aandacht te besteden aan het bespreken van de juridische en ethische kaders, zodat die optimaal aansluiten bij de stand van zaken binnen het recht en de praktijk.

## Lessen voor andere samenwerkingsverbanden binnen het cyberdomein

Uit de opgedane ervaringen binnen Melissa worden een aantal eerste algemene lessen voor effectieve samenwerking op het gebied van cybersecurity zichtbaar. Deze lessen gaan over 1) de organisatie, 2) de uitvoering en 3) de resultaten van samenwerking.

### *Organisatie: wie zit er aan tafel? En onder welke voorwaarden?*

1. Betrek een select aantal partijen met relevante expertise. Groter is niet altijd beter. Sociale cohesie en vertrouwen, daarentegen, is onmisbaar. Expertise zorgt voor respect en inhoudelijke kennisuitwisseling is cruciaal voor zingeving, enthousiasme en duurzaam draagvlak.
2. Zorg voor diversiteit in participanten. Dit vormt de basis van leren en uitwisseling van kennis en inzichten.
3. Leiderschap en gestructureerde coördinatie is nodig voor de organisatie van effectieve samenwerking.
4. Voorkom onnodige roulatie van deelnemers, maar lidmaatschap is niet heilig. Wanneer structureel niet kan worden bijgedragen aan de doelstellingen kan betrokkenheid beter op een andere manier worden vormgegeven.
5. Start vanuit een gemeenschappelijke drijfveer en draag deze uit.
6. Schets vooraf duidelijke verwachtingen van de samenwerking en formuleer duidelijke en haalbare doelen.

### *Uitvoering: hoe krijgt samenwerking in de praktijk vorm?*

7. Stimuleer het actief en gelijkmatig delen van informatie en kennis tussen partijen op basis van quid pro quo.
8. Organiseer trainings- en kennisuitwisselingssessies. Hierbij is een goede voorbereiding en een actieve houding van de deelnemers van belang.
9. Succesvolle samenwerking en netwerkvorming gaat over sociale relaties en vertrouwen. Dit maakt fysieke bijeenkomsten en voldoende sociale elementen binnen projecten van significant belang.
10. Zorg binnen de samenwerking voor basisregels (bijvoorbeeld over vertrouwelijkheid/ geheimhouding), maak deze regelmatig tot onderwerp van gesprek, en houdt toezicht op de naleving hiervan.
11. Maak duidelijke werkafspraken en zorg dat deze door alle partijen worden nagekomen.
12. Erken dat partijen verschillende achtergronden en middelen hebben waardoor eenieders inbreng binnen de samenwerking soms kan verschillen.
13. Erken dat partijen verschillende belangen hebben en dat die belangen soms tegenstrijdig kunnen zijn. Maak het gedeelde belang zichtbaar en bespreek waar de grenzen ervan liggen, zodat in de samenwerking duidelijk is hoe ‘we’ de dingen samen doen.

### *Resultaten: hoe om te gaan met de output?*

14. Zorg dat resultaten voldoende tastbaar worden voor de deelnemers. Zo wordt duidelijk waar men het voor doet.
15. Deel resultaten met elkaar en de buitenwereld waar dit kan en wees gul in het erkennen van elkaars rol en bijdrage.
16. Accepteer dat samenwerken met een groot aantal partijen vaak aanzienlijke investeringen vraagt (tijd, energie, geld).

# LITERATUUR


Akyazi, Ugur, M. J. G. van Eeten, and C. Hernandez Ganan. "Measuring cybercrime as a service (caas) offerings in a cybercrime forum." In *Workshop on the Economics of Information Security*. 2021.

August, Terrence, Duy Dao, and Marius Florin Niculescu. 2022. "Economics of Ransomware: Risk Interdependence and Large-Scale Attacks." *Management Science* 68 (12): 8979–9002. https://doi.org/10.1287/mnsc.2022.4300.

Autoriteit Persoonsgegevens (AP), 'Rapportage ransomware: Gebrekkige beveiliging maakte twee op de drie getroffen organisaties kwetsbaar', 2024, https://www.autoriteitpersoonsgegevens.nl/system/files?file=2024-10/AP%20rapportage%20ransomware.pdf;

Benmalek, Mourad. 2024. "Ransomware on Cyber-physical Systems: Taxonomies, Case Studies, Security Gaps, and Open Challenges." *Internet of Things and Cyber-Physical Systems*, January. https://doi.org/10.1016/j.iotcps.2023.12.001.

Blom, Tessel, Wazir Sahebali, Kimberly Deppe, Peter Romijn, Floris Donath, and Reg Brennenraedts. 2023. "Ransomeware-aanvallen op instellingen en bedrijven in Nederland." 2022.173-2319. Dialogic. https://repository.wodc.nl/bitstream/handle/20.500.12832/3292/3375-ransomware-aanvallen-op-instelllingen-en-bedrijven-volledige-tekst.pdf?sequence=7&isAllowed=y.

Boeke, Sergei. "National cyber crisis management: Different European approaches." *Governance* 31, no. 3 (2018): 449-464.

Brewer, Ross. "Ransomware attacks: detection, prevention and cure." *Network security* 2016, no. 9 (2016): 5-9.

Carr, Madeline. "Public–private partnerships in national cyber-security strategies." *International Affairs* 92, no. 1 (2016): 43-62.

Christensen, Kristoffer Kjærgaard, and Karen Lund Petersen. "Public–private partnerships on cyber security: a practice of loyalty." *International Affairs* 93, no. 6 (2017): 1435-1452.

Convenant Melissa (2023). https://zoek.officielebekendmakingen.nl/stcrt-2023-29185.pdf

Cyber Security Raad, 2020. "CSR Jaaroverzicht 2020".

Cyberveilig Nederland. 2021. "Cybersecurity Handboek 2021". https://cyberveilignederland.nl/woordenboek#:~:text=Van%20cybersecurity%20naar%20Nederlands&text=Het%20woordenboek%20blijft%20in%20ontwikkeling,via%20woordenboek%40cyberveilignederland.nl.

Cyberveilig Nederland. 2023. "Ransomware." https://cyberveilignederland.nl/upload/userfiles/files/CVNL_Ransomware_def.pdf.

Digital Trust Center, "Samenwerkingsverband Melissa Vindt Diverse Nederlandse Slachtoffers Van Ransomwaregroepering Cactus." https://www.digitaltrustcenter.nl/nieuws/samenwerkingsverband-melissa-vindt-diverse-nederlandse-slachtoffers-van-ransomwaregroepering.

Dunn-Cavelty, Myriam, and Manuel Suter. "Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection." *International Journal of Critical Infrastructure Protection* 2, no. 4 (2009): 179-187.

O'Gorman, Gavin, and Geoff McDonald, 2012.. "Ransomware: A Growing Menace." Symantec.

Greenberg, Andy, and Excerpt. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *WIRED*, 22 augustus, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Freeze, Di. 2023. "Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031." Cybercrime Magazine. July 10, 2023. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

Holterman, Liesbeth, 2024. "Over 'Melissa.'" In *Opportuun*. https://cyberveilignederland.nl/actueel/liesbeth-holterman-in-oppertuun-over-melissa, .

Hyslip, Thomas S., and George W. Burruss. "Ransomware." In *Handbook on Crime and Technology*, pp. 86-104. Edward Elgar Publishing, 2023.

Institute for Security and Technology. 2021. "Combating Ransomware." https://www.in.gr/wp-content/uploads/2021/05/RTF.pdf.

Kumar, P. Ravi, and Hj Rudy Erwan Bin Hj Ramlie. 2021. "Anatomy of Ransomware: Attack Stages, Patterns and Handling Techniques." In *Advances in Intelligent Systems and Computing*, 205–14. https://doi.org/10.1007/978-3-030-68133-3_20.

Laitinen, Marja, and Sarah Armstrong-Smith. "Tackling cybercrime and ransomware head-on: Disrupting criminal networks and protecting organisations." *Cyber Security: A Peer-Reviewed Journal* 5, no. 3 (2022): 190-205.

Luiijf, Eric, Kim Besseling, and Patrick De Graaf. "Nineteen national cyber security strategies." *International Journal of Critical Infrastructures 6* 9, no. 1-2 (2013): 3-31.

Matthijsse, Sifra R., M. Susanne van 't Hoff-de Goede, and E. Rutger Leukfeldt. "Your files have been encrypted: A crime script analysis of ransomware attacks." *Trends in Organized Crime* (2023): 1-27.

Meland, Per Håkon, Yara Fareed Fahmy Bayoumy, and Guttorm Sindre. 2020. "The Ransomware-as-a-Service Economy Within the Darknet." *Computers & Security* 92 (May): 101762. https://doi.org/10.1016/j.cose.2020.101762.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Sage.

Ministerie van Justitie en Veiligheid. 2023. "Grootste Wereldwijde Botnet Qakbot Onschadelijk Gemaakt." Nieuwsbericht | Openbaar Ministerie. September 4, 2023. https://www.om.nl/actueel/nieuws/2023/08/29/grootste-wereldwijde-botnet-qakbot-onschadelijk-gemaakt.

Ministerie van Justitie en Veiligheid. 2024. "CyberrechercheursVoorÉénDag."Reportage|Opportuun. February 9, 2024. https://magazines.openbaarministerie.nl/opportuun/2024/01/politiehackathon.

Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2022. "Nationale Cybersecuritystrategie 2022-2028".

Nationaal Cyber Security Centrum en Nationaal Coördinator Terrorismebestrijding en Veiligheid. 2021. "Cybersecuritybeeld Nederland 2021." https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021#:~:text=Het%20Cybersecuritybeeld%20Nederland%202021%20(CSBN,daarbij%20op%20de%20nationale%20veiligheid.

Nationaal Cyber Security Centrum. 2022. "Factsheet Ransomware." Factsheet | Nationaal Cyber Security Centrum. October 28, 2022. https://www.ncsc.nl/wat-kun-je-zelf-doen/documenten/factsheets/2020/juni/30/factsheet-ransomware.

Nationaal Cyber Security Centrum. 2024. "Ransomware." Wat Kun Je Zelf Doen? | Nationaal Cyber Security Centrum. June 14, 2024. https://www.ncsc.nl/wat-kun-je-zelf-doen/dreiging/ransomware.

"Nederlandse Cybersecuritystrategie 2022-2028." Nationaal Coördinator Terrorismebestrijding En Veiligheid. https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022-2028.

NOS. 2023. "'Ransomwaregroep Dreigt KNVB Contracten Van Trainers En Spelers Te Lekken.'" April 17, 2023. https://nos.nl/artikel/2471789-ransomwaregroep-dreigt-knvb-contracten-van-trainers-en-spelers-te-lekken.

O'Kane, Philip, Sakir Sezer, and Domhnall Carlin. "Evolution of ransomware." *Iet Networks* 7, no. 5 (2018): 321-327.

Opderbeck, David W. "Cybersecurity and Data Breach Harms: Theory and Reality." *Md. L. Rev.* 82 (2022): 1001.

Oz, Harun, Ahmet Aris, Albert Levi, and A. Selcuk Uluagac. "A survey on ransomware: Evolution, taxonomy, and defense solutions." *ACM Computing Surveys (CSUR)* 54, no. 11s (2022): 1-37.

Pawson, Ray, and Nick Tilley. "An introduction to scientific realist evaluation." *Evaluation for the 21st century: A handbook* 1997 (1997): 405-18.

Politie,"Servers Neergehaald Van 'S Werelds Grootste Ransomware Groepering." Politie.Nl. februari 20,

2024. Politie.nl. https://www.politie.nl/nieuws/2024/februari/20/09-servers-neergehaald-van-s-werelds-grootste-ransomware-groepering.html (2024).

Politie, "Nederlandse Gedupeerden geholpen in Unieke Ransomware-actie." Politie.nl. https://www.politie.nl/nieuws/2022/oktober/14/09-nederlandse-gedupeerde-geholpen-in-unieke-ransomware-actie.html (2023).

Richardson, Ronny, and Max M. North. "Ransomware: Evolution, mitigation and prevention." *International Management Review* 13, no. 1 (2017): 10.

Robles-Carrillo, M., and P. García-Teodoro. 2022. "Ransomware: An Interdisciplinary Technical and Legal Approach." *Security and Communication Networks* 2022 (August): 1–17. https://doi.org/10.1155/2022/2806605

Schlette, Daniel, Marco Caselli, and Günther Pernul. "A comparative study on cyber threat intelligence: The security incident response perspective." *IEEE Communications Surveys & Tutorials* 23, no. 4 (2021): 2525-2556.

Shackelford, Scott J., Anjanette Raymond, Danuvasin Charoen, Rakshana Balakrishnan, Prakhar Dixit, Julianna

Staatscourant 2023, Officiele bekendmakingen 29185. November 1, 2023. https://zoek.officielebekendmakingen.nl/stcrt-2023-29185.html.

Gjonaj, and Rachith Kavi. "When toasters attack: A polycentric approach to enhancing the security of things." *U. Ill. L. Rev.* (2017): 415.

Sherer, James, Melinda McLellan, Emily Fedeles, and Nichole Sterling. 2017. "Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web." *Richmond Journal of Law & Technology* 23 (3). https://jolt.richmond.edu/files/2017/05/Sherer-Final-clean-.pdf. (22).

Van den Berg, Bibi, and Sanneke Kuipers. "Vulnerabilities and cyberspace: A new kind of crises." *Oxford Research Encyclopedia of Politics* (2022).

Vish, Elizabeth, and Georgeanela Flores Bustamante. n.d. "Public Private Partnerships to Combat Ransomware: An inquiry into three case studies and best practices." https://securityandtechnology.org/virtual-library/reports/public-private-partnerships-to-combat-ransomware.

Weiss, Moritz, and Vytautas Jankauskas. "Securing cyberspace: How states design governance arrangements." *Governance* 32, no. 2 (2019): 259-275.

# BIJLAGEN

## Bijlage 1: Respondenten en affiliatie

| Naam | Organisatie |
|---|---|
| Baars, Esther | OM |
| Blokhuis, Joeri | Responders.Nu |
| Brand, Rosalie | Kennedy Van der Laan |
| Brouwer, Rayan | Deloitte |
| Fennis, Joey | Dataexpert |
| Hensen, Lodi | Eye Security |
| Jaspers, Matthijs | Politie |
| Keuper, Daan | Computest |
| Koopman, Gert | NFIR |
| Oldengarm, Petra | Cyberveilig Nederland |
| Takkenberg, Pim | Northwave |
| Van Amelsfort, Matthijs | Politie |
| Woutersen, Dave | NCSC |

## Bijlage 2: Geraadpleegde documenten (project-specifiek)

Convenant Melissa (2023). https://zoek.officielebekendmakingen.nl/stcrt-2023-29185.pdf

Cyberveilig Cyberveilig Nederland (2023), Whitepaper Ransomwaware. Online op 13 november 2024 via https://cyberveilignederland.nl/upload/userfiles/files/CVNL_Ransomware_def.pdf

Cyberveilig Nederland (2023) "Data-exfiltratie bij een ransomware-aanval." Online op 13 november 2024 via https://cyberveilignederland.nl/upload/userfiles/files/VCNL_Whitepaper_Exfiltratie_v3_0_Web.pdf

Melissa (2024), Presentatie Melissa tweedaagse 2024.

Melissa (2023), Presentatie Tweedaagse Ransomware, Programma Juridisch/Organisatorisch.

Melissa (2023), Presentatie Aanpak technische informatiedeling Melissa.

Melissa (2022), Presentatie Resultaten en Vervolgstappen Project Melissa.

Melissa (2022), Presentatie Melissa Bijeenkomst 30 november.

Melissa (2022), Presentatie Melissa captain's dinner. Samenvatting en conclusies.

Melissa (2022), Presentatie Projectplan Melissa 2022 – 2023.

Melissa (2022), Status actiepunten Melissa a.

Melissa (2022), Status Actiepunten Melissa b.

## Bijlage 3: Topiclijst interviews

**Introductie:**

*Hoe bent u betrokken geweest bij het project?*

*Wat was uw rol?*

**Exploratieve topics evaluatie:**

**Voor (Status quo, Verwachtingen en Doelen):**

*Hoe warende relaties voor het project?*

*Kan u het landschap/situatie rondom bestrijding ransomware in Nederland beschrijven voor Melissa?*

*Wat was uw belangrijkste verwachting van Melissa?*

*Wat was uw doel met dit samenwerkingsverband tussen private en publieke partijen?*

**Terugblik afgelopen periode (Behaalde resultaten, Werkwijze, Ervaringen en Obstakels):**

*Hoe heeft u de samenwerking vorm proberen te geven? Welke ideeën zaten hierachter?*

*Wat zijn voor u belangrijkste opbrengsten/prestaties geweest?*

*Zijn volgens u de gestelde doelen bereikt? (zo ja, wat heeft hier volgens u voor gezorgd?).*

*Wat is volgens u de belangrijkste meerwaarde van het samenwerkingsverband?*

*Zijn er ook obstakels en uitdagingen geweest?*

**Toekomst (Aanvullende wensen, Ambities lange termijn):**

*Wat is er nodig om in de toekomst als maatschappij succesvol te zijn tegen ransomware-aanvallen?*

*Hoe kijkt u naar Melissa op lange termijn?*

Universiteit
Leiden
Institute of Security
and Global Affairs

Bij ons leer je de wereld kennen