Defensie & Veiligheid
Oude Waalsdorperweg 63
2597 AK Den Haag
Postbus 96864
2509 JG Den Haag

www.tno.nl

T +31 88 866 10 00

TNO-rapport

TNO 2022 R10535

Kwantificering cyberrisico's: rapportage 2021 (P2108)

Datum	April 2022
Auteur(s)	Willem Verdaasdonk Marieke Klaver Peter Langenkamp
Rubricering rapport	TNO Publiek | ONGERUBRICEERD Releasable to the public
Vastgesteld door	Rik van Dijk
Vastgesteld d.d.	4 april 2022
Oplage	1 hard copy & 1 cd
Aantal pagina's	29 (excl. distributielijst)
Aantal bijlagen	0
Vraagstuurder	Nationaal Cyber Security Centrum
Projectnaam	Kwantificering cyberrisico's
Projectnummer	060.46708/01.04

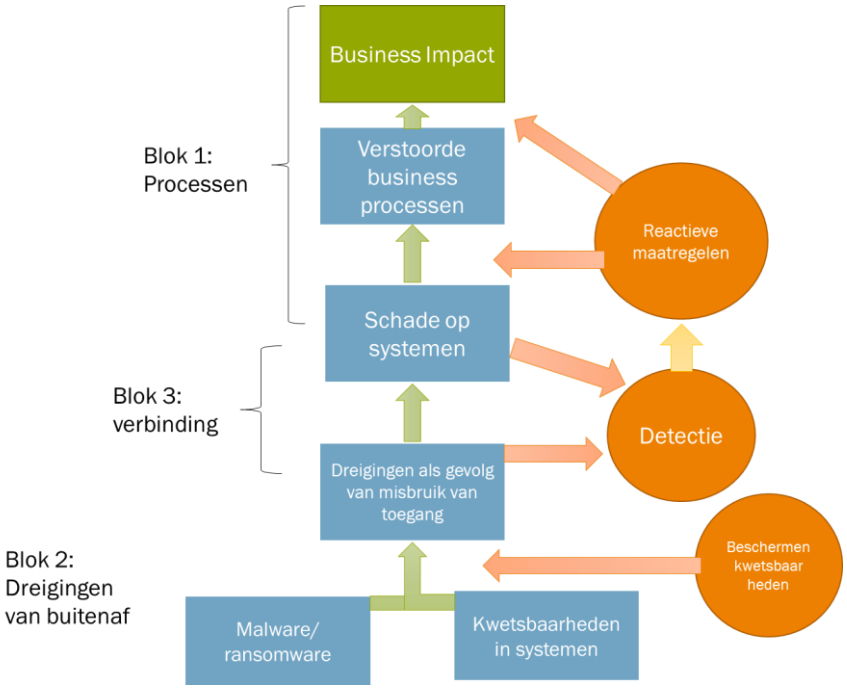
Management samenvatting

Titel	:	Kwantificering cyberrisico's: rapportage 2021 (P2108)
Auteur(s)	:	Willem Verdaasdonk, Marieke Klaver, Peter Langenkamp
Datum	:	April 2022
Rapportnr.	:	TNO 2022 R10535

Aanleiding en werkwijze
Risicoanalyses met betrekking tot cybersecurity zijn over het algemeen kwalitatief van aard. Kwantitatieve inschattingen van de mogelijke risico's en de daarbij behorende schade zijn zeer beperkt voor handen. Dit werkt belemmerend om de voor cybersecurity benodigde investeringen te agenderen in organisaties waar het investeren in digitale beveiliging lage prioriteit heeft.
Een aanknopingspunt om cyberrisico's beter te integreren in afwegingen is het integreren van cyberrisico's met bestaand risicomanagement. Dit onderzoek richt zich op methoden om cyberrisico's kwantitatief in kaart te brengen en af te wegen hoe deze zich verhouden tot andere bedrijfsrisico's. Om maximaal te kunnen aansluiten op de bestaande praktijk rond cyber risicoanalyses zijn deze mogelijke methoden getoetst en verder ontwikkeld in case studies met organisaties uit de vitale infrastructuur.
In 2020 is een methode voor het kwantificeren van een cyberrisico ontwikkeld. De methode is getoetst in een case studie. De deliverables hiervan zijn de methode en bijbehorende werkwijze.
In 2021 zijn twee aanvullende case studies uitgevoerd om de methodiek en werkwijze te toetsen en aan te scherpen. De beide case studies gingen in op een actuele dreiging, namelijk ransomware. Ter voorbereiding op de case studies is voor dit onderwerp een inventarisatie uitgevoerd van de hiervoor benodigde en beschikbare ondersteunende data.

Bereikte resultaten
Het onderzoek heeft de volgende resultaten opgeleverd.

Herkenbaarheid van het basismodel en de werkwijze
Het basismodel (2020) is gebruikt tijdens de case studies die in 2021 zijn uitgevoerd. Het uitvoeren van meerdere workshops, gebaseerd op de drie onderdelen in het basismodel bleek van toegevoegde waarde (één workshop over de impact aan de hand van incidenten, één over de frequentie en aard van dreigingen en één over bedrijfsspecifieke maatregelen en inschattingen).



Figuur 1 Gelaagde opzet van het basismodel.

Inventarisatie beschikbaarheid gegevens

In de case studie van 2020 bleek dat niet beschikbare gegevens een belangrijk aandachtspunt waren. Daarom is in 2021 onderzocht welke vrijelijk beschikbare gegevens gebruikt konden worden als ondersteuning. In de nationale context bleek er voor cyberrisico's geen integrale gegevensset voorhanden. Wel is een deel van het gewenste soort gegevens beschikbaar, verdeeld over diverse (grotendeels internationale) bronnen. De inventarisatie leidde tot de volgende observaties:

- *De mogelijke impact van aanvallen:* gegevens over de impact bleken slecht toegankelijk en deels onbetrouwbaar. De gegevens die beschikbaar zijn leggen de nadruk op de financiële implicaties en minder op aspecten die ook van belang zijn in de context van vitale sectoren. Voor de vitale infrastructuur is primair de eventuele verstoring van de vitale processen van belang (duur en grootte). Als mogelijke typen bronnen voor deze gegevens zijn onderkend:
  - gegevens uit openbare bronnen, waaronder databases met vitale infrastructuur incidenten en academische databases rond ransomware incidenten (t.b.v. inzicht in de effecten van verstoringen),
  - statistieken en data van het CBS of gegevens van verzekeringsmaatschappijen (t.b.v. duiden financiële impact) hebben het meeste potentie.
- *De dreiging*: over de aard en trends van de dreiging is relatief veel informatie beschikbaar. Het betreft bijvoorbeeld informatie over veelvoorkomende aanvalsvectoren en trends in de aantallen en soorten aanvallen.
  Deze informatie is deels beschikbaar in rapportages van het NCSC en in Amerikaanse bronnen.
- *Gegevens over de weerbaarheid van de systemen:* dit betreft gegevens die zowel vanwege de systemen zelf als de gekozen beveiligingsmaatregelen sterk organisatie-specifiek zijn. Hiervoor kan wel gebruik gemaakt worden van algemeen gehanteerde metrics, maar de inschatting dient in sterke mate op de organisatie te worden afgestemd.

Kwantificering bleek ten dele mogelijk
Bij de eerste case studie in 2020 bleek het erg lastig om kwantitatieve inschattingen te maken door een gebrek aan gegevens. In vergelijking met de eerste case studie beschikten beide case organisaties in 2021 over meer basisgegevens voor de te maken inschattingen. Zo waren bijvoorbeeld gegevens over de effectiviteit van phishing aanvallen goed in beeld, en was ook meer informatie beschikbaar over de maatregelen en de mogelijke impact.
Daarnaast was het door de uitgevoerde inventarisatie van gegevens over ransomware ook mogelijk om ervaringen uit het buitenland te gebruiken. Deze zijn als vergelijkingsmateriaal gebruikt voor de te maken inschattingen over de kans en de mogelijke impact. Hierdoor konden tijdens de workshops de juiste discussies worden gevoerd.
Wel bleek ook voor deze organisaties het maken van een volledige inschatting van kansen en impact nog een brug te ver.

Vervolgstappen
De werkzaamheden voor dit onderzoek in 2022 zijn erop gericht om de ontwikkelde methode te ontsluiten voor het NCSC en haar doelgroepen. Dit wordt gedaan door het ontwikkelen van 1) een factsheet waarin de methode op toegankelijke wijze wordt beschreven en 2) een toolkit waarin het onderliggende rekenmodel, aansprekende voorbeelden en ondersteunende databronnen bij elkaar worden gebracht.
Om dit te bereiken worden de volgende stappen ondernomen:

- het aanscherpen en vastleggen van de methode op basis van de use cases ten behoeve van de factsheet,
- het verzamelen en ontwikkelen van databronnen, voorbeelden en archetypes om de doelgroepen te ondersteunen bij het organisatie-specifiek maken en vullen van het rekenmodel (Archetypes zijn vooraf gestructureerde en ingevulde onderdelen van het hoofdmodel. Organisaties kunnen deze archetypes gebruiken om mee te beginnen, om vervolgens zelf het model aan te passen naar behoefte. Hierdoor hoeft men niet vanaf scratch te beginnen en wordt de drempel verlaagd om met kwantificering aan de slag te gaan.),
- het bij elkaar brengen van alle informatie in een overzichtelijk geheel in de vorm van een toolkit.

Inhoudsopgave

1 Inleiding

1.1 Achtergrond en probleemstelling

Het kunnen kwantificeren van mogelijke risico's en de daarbij behorende schade is een middel om cybersecurity te agenderen bij organisaties waar niet altijd draagvlak is voor het investeren in digitale beveiliging. Veel van de momenteel voor cybersecurity uitgevoerde risicoanalyses zijn kwalitatief van aard. Er wordt nog niet systematisch data verzameld om kwantitatieve inschattingen te kunnen maken. Historische data van financiële instellingen en verzekeraars en bijvoorbeeld de jaarlijkse incidentenoverzichten van ENISA kunnen een potentieel startpunt vormen voor een breed te gebruiken ondersteunende dataset.
Daarnaast ligt er ook een behoefte om de complexiteit en onderlinge verbanden tussen processen en systemen op een begrijpelijke manier te verwerken en mee te nemen in de analyses en modellen, om zo de besluitvorming in organisaties te verbeteren. Een mogelijk aanknopingspunt hiervoor is het integreren van cyberrisico's met bestaande risicomanagement praktijken binnen organisaties. De uitdaging ligt in het in kaart brengen van cyberrisico's en hoe deze zich verhouden tot andere bedrijfsrisico's. Om maximaal te kunnen aansluiten op de bestaande praktijk rond cyberrisicoanalyses zal het onderzoek zich richten op casestudies uit de vitale processen. Hierbij wordt voortgebouwd op kennis opgedaan uit andere domeinen.

1.2 Doelstelling van het onderzoek

Het onderzoek kent de volgende doelstellingen:

- Het ontwikkelen van een methode voor het kwantificeren van mogelijke cyberrisico's en daarbij behorende schade;
- Het inventariseren van mogelijk geschikte ondersteunende datasets[1];
- Het integreren van de ontwikkelde methode met bestaande risicomanagement-methodieken.

In 2020 is gewerkt aan het ontwikkelen van een methode voor het kwantificeren van het cyberrisico en het toetsen van deze methode. Het resultaat hiervan is een basismodel en werkwijze (die in 2020 is getoetst in een case studie).
In 2021 zijn twee aanvullende case studies uitgevoerd om de methodiek en werkwijze te toetsen en aan te vullen. Daarnaast is een inventarisatie uitgevoerd van de benodigde en beschikbare ondersteunende data. Hiervan is gebruik gemaakt bij het vormgeven van de case studies. De derde doelstelling, het integreren van de ontwikkelde methode in bestaande risicomanagement-methodieken, wordt in 2022 opgepakt.

[1] Het ontwikkelen van een integrale dataset is niet mogelijk gebleken. Op basis van de inventarisatie is wel duidelijk geworden welke elementen nodig zijn, en hoe delen daarvan te ontwikkelen zijn (zie voor meer informatie hoofdstuk 3).

1.3 Leeswijzer

Dit document beschrijft achtereenvolgens de werkwijze tijdens het project gedurende 2021, het resultaat van de literatuurstudie naar de beschikbaarheid van databronnen en de opzet en resultaten van de case studies.
Het laatste hoofdstuk bevat een reflectie op de resultaten en de gekozen richting voor vervolgwerkzaamheden.

2 Werkwijze

2.1 Werkwijze

De werkwijze in 2021 bouwde voort op de in 2020 ontwikkelde producten en bevindingen (Langenkamp, Van Egmond, & Klaver, 2020). In 2020 bleek één van de belangrijkste uitdagingen van de werkzaamheden de beschikbaarheid van ondersteunende databronnen te zijn. Daarom is in het eerste kwartaal van 2021 een inventarisatie van mogelijke databronnen uitgevoerd. Op basis van deze inventarisatie is het eerder ontwikkelde basismodel verrijkt met relevante gegevens voor de case studies.

Vervolgens is het basismodel aangepast voor de specifieke eigenschappen van de case organisaties in twee aanvullende case studies.
Na afloop van de case studies heeft een evaluatie plaatsgevonden en zijn aanpassingen aan het model en de werkwijze doorgevoerd.

2.2 Inventarisatie mogelijke databronnen

Als extra ondersteuning voor de uitwerking van de case studies is een inventarisatie uitgevoerd van mogelijke databronnen. Voor deze inventarisatie is allereerst een literatuurstudie gedaan naar mogelijke databronnen voor de in de case studies centraal staande dreiging ransomware, en data voor de specifieke sector van de case studies.
Vervolgens is een vergadering opgezet met een lid van de klankbordgroep om na te gaan of het overzicht van geïnventariseerde bronnen volledig was of dat er nog aanvullende bronnen bekend en beschikbaar waren.
De op basis hiervan geïdentificeerde bronnen en informatie zijn gebruikt ter verrijking van het basismodel en benut in de voorbereiding van de case studies.

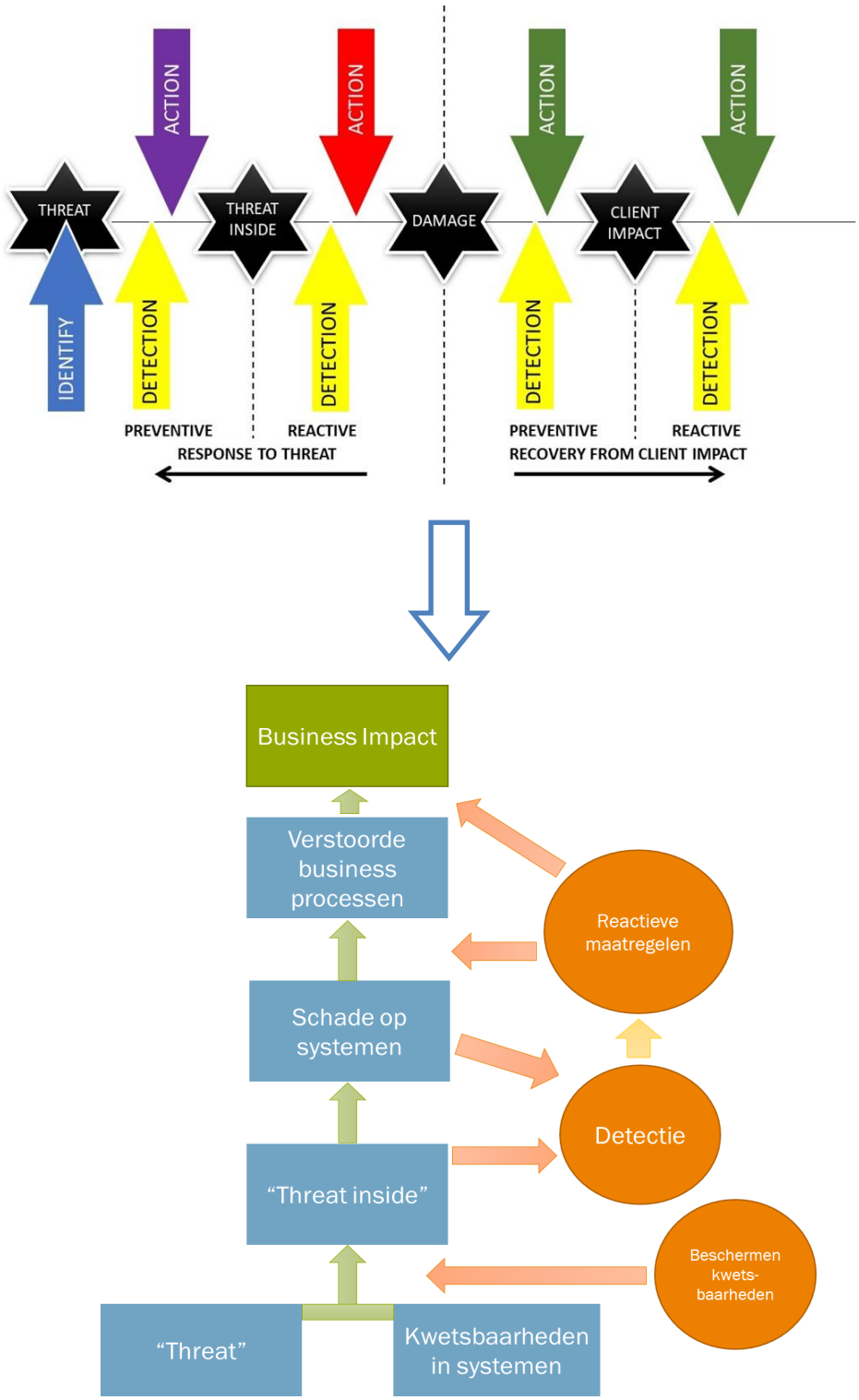
2.3 Gebruikt basismodel

Als basis voor de werkzaamheden in 2021 is gebruikgemaakt van het basismodel en de werkwijze zoals ontwikkeld in 2020. Op basis van de geïnventariseerde databronnen is dit model verrijkt met enkele gegevens en elementen die specifiek voor ransomware gelden.
Het ontwikkelde basismodel voor dreiging vanuit ransomware is weergegeven in Figuur 2. Dit basismodel is gebruikt als uitgangspunt voor de case studies.

Case studies
Voor de toetsing van het model en de werkwijze is een tweetal case studies uitgevoerd. Het betrof twee case studies binnen dezelfde vitale sector.
Voor beide case studies is de eerder ontwikkelde werkwijze gevolgd (Langenkamp, Van Egmond, & Klaver, 2020). Hierbij is een drietal workshops georganiseerd waarbij het basismodel specifiek werd aangepast aan de deelnemende organisaties. In de laatste workshop zijn gezamenlijk kans inschattingen van de mogelijke risico’s gemaakt.

2.4 Evaluatie case studies voor werkwijze

Op basis van de ervaringen van de case studies uit 2021 is onderzocht welke aanpassingen en aanvullingen voor het basismodel en de werkwijze nodig zijn. Deze aanpassingen en aanvullingen worden in 2022 verder uitgewerkt.



Figuur 2 Basismodel kwantificeren van cyberrisico's vertaald naar het basismodel voor deze case studies.

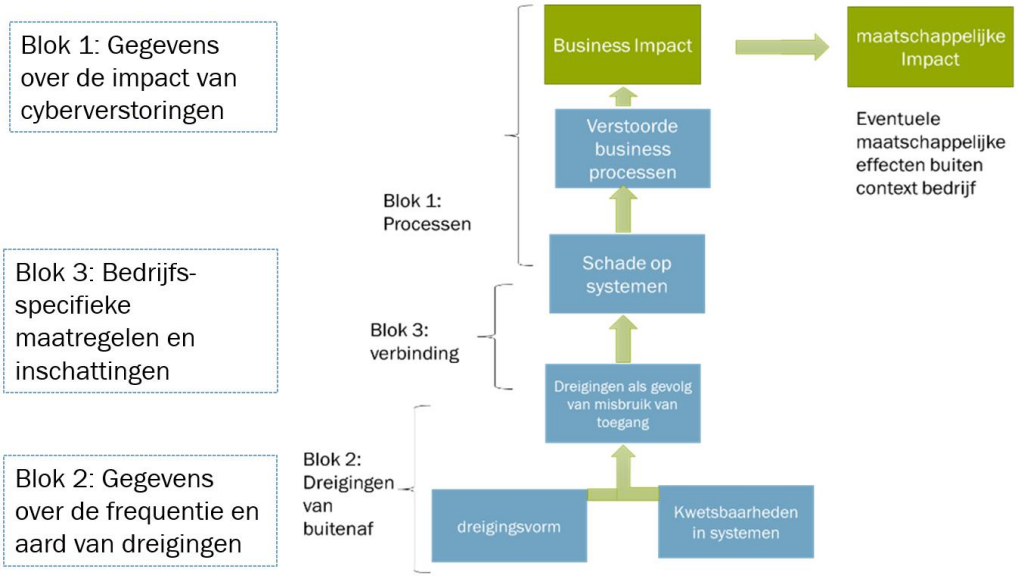
3 Analyse data ten behoeve van risicoanalyses

3.1 Inleiding

Voor de case studies in 2021 is gekozen voor het thema ransomware. Om de case studies voor te bereiden is een analyse uitgevoerd van de verschillende soorten gegevens die ondersteunend kunnen zijn aan risicoanalyses. Hiervoor is allereerst een literatuurstudie uitgevoerd. Dit hoofdstuk betreft een overzicht van de verschillende datatypen die een rol spelen binnen risicoanalyses en de mogelijke bronnen die zijn geïdentificeerd.

3.2 Indeling benodigde typen gegevens

Voor de indeling van de typen gegevens wordt gebruik gemaakt van het binnen de case studies gehanteerde basismodel zoals weergegeven in Figuur 3.



Figuur 3 Indeling gegevens voor het basismodel.

Binnen het model worden drie typen gegevens onderscheiden:

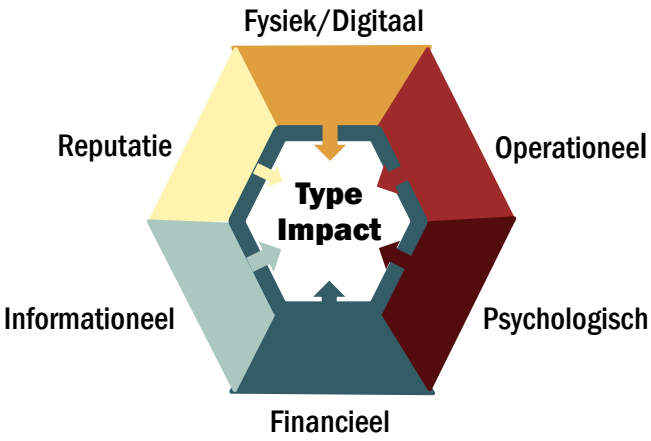
- gegevens over de impact aan de hand van incidenten;
- gegevens over de frequentie en aard van dreigingen;
- bedrijfsspecifieke maatregelen en inschattingen.

In de komende drie secties worden deze typen gegevens kort toegelicht.

3.3 Gegevens omtrent impact

In blok 1 van het basismodel wordt gekeken naar de business impact op een bedrijf of organisatie uit de vitale sectoren en naar de mogelijke maatschappelijke impact. Om een breed beeld te krijgen van zowel de business impact als de maatschappelijke impact van ransomware in blok 1, is een analyse uitgevoerd van de verschillende typen impact die in de literatuur worden onderkend.
Op basis van literatuuronderzoek zijn zes verschillende typen impact gespecificeerd en geïdentificeerd (Boot, 2021): reputatie, fysiek/digitaal, operationeel, informationeel, financieel, en psychologisch (zie Figuur 4). Vijf van de zes

impactfactoren worden gebruikt om impact te duiden. De psychologische impact is niet meegenomen, omdat deze meer op individueel niveau wordt gehanteerd en voor de vitale infrastructuur minder relevant lijkt.



Figuur 4 Type impact geïdentificeerd op basis van literatuuronderzoek.

In blok 1 (zie **Fout! Verwijzingsbron niet gevonden.**) wordt gekeken naar de b usiness processen en hoe deze verstoord kunnen worden door ransomware. Zodra dit in kaart is gebracht, kan worden gekeken naar de impact hiervan onderverdeeld in de verschillende categorieën die benoemd zijn in de vorige alinea. Dit is belangrijk om een compleet beeld te krijgen van de consequenties van een ransomware aanval voor de vitale infrastructuur.

Om een overzicht te creëren van bestaande datasets over de impact van ransomware is verkend welke gegevens beschikbaar zijn op basis van ransomware case studies. Hierbij heeft TNO een aantal vragenlijsten en onderzoeken geanalyseerd uit de volgende categorieën:

1 *Statistische rapportages*, bijvoorbeeld van het CBS. Het CBS brengt jaarlijks de cybersecurity monitor uit (CBS, 2021). Hierin vallen ransomware aanvallen onder de categorie ‘ICT-veiligheidsincidenten door een aanval van buitenaf’. Er zijn geen aparte gegevens opgenomen over ransomware.
2 *Formele incidentrapportages:* hieronder vallen de rapportages van de NIS Directive. Onder de NIS Directive dienen vitale organisaties grootschalige cyberincidenten te melden. Het gaat momenteel nog slechts om een klein aantal incidenten (NIS CG, 2020).
3 *Gebruik van openbare bronnen en datasets*: er bestaan een aantal (academische) datasets van ransomware (zie bijvoorbeeld de dataset van Temple University). Hierin staan vaak gegevens over het getroffen bedrijf, de datum, de duur van de impact, en soms gegevens over de kosten. Voor de maatschappelijke impact van verstoringen is gekeken in hoeverre de ‘lessons learned’ van de TNO Critical Infrastructure Incident Database (CIID) gebruikt kunnen worden (Luiijf & Klaver, 2021).
4 *Rapportages van security bedrijven*: veel security bedrijven brengen rapportages uit over de incidenten die zij hebben waargenomen. Bij veel van deze rapportages ligt de nadruk op Amerikaanse gegevens. De rapportage van de Amerikaanse Ransomware Task Force (2021) combineert gegevens uit deze rapportages om een beeld te schetsen van de trends en impact van ransomware.

5 *Rapportages van verzekeringsmaatschappijen*: in toenemende mate brengen verzekeringsmaatschappijen rapportages uit over de incidenten die bij hen zijn gerapporteerd. Ook hier lijken de bronnen uit de Verenigde Staten te overheersen (NetDiligence, 2021), maar er komen in toenemende mate ook gegevens over Europa beschikbaar (Marsh, 2021).

Voor deze verschillende typen bronnen is nagegaan in hoeverre gegevens over de impact beschikbaar waren. Op basis van de indeling van de impact in het basismodel is hiervoor gekeken naar de volgende impactfactoren:
- effect op de vitale processen van de organisatie;
- financiële impact;
- reputatie;
- veiligheid van mensen;
- materieel;
- omgeving.

Met name de eerste twee factoren komen in de onderzochte bronnen naar voren.

Verstoring vitale processen
Voor vitale organisaties wordt de mogelijke verstoring van de vitale processen als belangrijkste impactfactor gezien. Deze impact is opgenomen in de formele incidentrapportages en in een deel van de openbare bronnen.
In de incidentrapportages onder de NIS Directive zijn de volgende elementen onderscheiden met betrekking tot de verstoring van vitale processen (NIS CG, 2018):
- het aantal betrokken gebruikers dat wordt geraakt door de verstoring;
- de duur van het incident;
- het geografische gebied van de verstoring.

Ervaringen uit bijvoorbeeld Zweden (Franke, 2021) laten zien dat in de rapportages de impact van incidenten vaak summier is beschreven.
In de CIID zijn voor de impact van de verstoring van vitale processen vergelijkbare factoren opgenomen als in de rapportages voor de NIS Directive (Luiijf & Klaver, 2021). Gezien de impact van grootschalige verstoringen van de vitale infrastructuur bleek dergelijke informatie vaak via berichten in de media en aanvullende incidentrapportages beschikbaar.

Financiële impact
Gegevens over de financiële impact zijn bijvoorbeeld beschikbaar in een deel van de statistische rapportages (CBS, 2021) en rapportages van verzekeringsbedrijven. Hierbij wordt in een deel van de rapportages onderscheid gemaakt tussen een aantal categorieën van financiële impact (NetDiligence, 2021):
- kosten voor crisisservices;
- kosten gerelateerd aan de verstoring van de bedrijfsprocessen;
- kosten ransomware;
- herstelkosten.

Algemeen beeld
Op basis van het literatuuronderzoek is het beeld ontstaan dat het merendeel van de bronnen zich richt op algemene informatie van ransomware incidenten, bijvoorbeeld over wanneer een incident heeft plaatsgevonden, welke sector het

heeft beïnvloed, in welk land het incident heeft plaatsgevonden, en wat de financiële effecten waren voor een bedrijf of organisatie. De andere elementen van de impact van een aanval worden vaak niet meegenomen. Het blijft vooral bij de financiële impact waar een bedrijf of organisatie mee te maken krijgt. Er zijn dus geen bronnen die een ideale set presenteren van impacts, of modellen over hoe impact is gemeten.

Daarnaast liet de inventarisatie ook zien dat de data die we hebben gevonden voornamelijk uit de VS afkomstig is en dat er in Nederland niet of nauwelijks systematisch data wordt verzameld over ransomware aanvallen.

3.4 Gegevens omtrent dreiging

Voor de dreiging is gekeken naar gegevens over trends in de frequentie, aangetaste sectoren, aanvalsvectoren en type aanvallers omtrent ransomware om een breed beeld te schetsen over de huidige situatie en een overzicht te creëren van de relevante dreigingen.

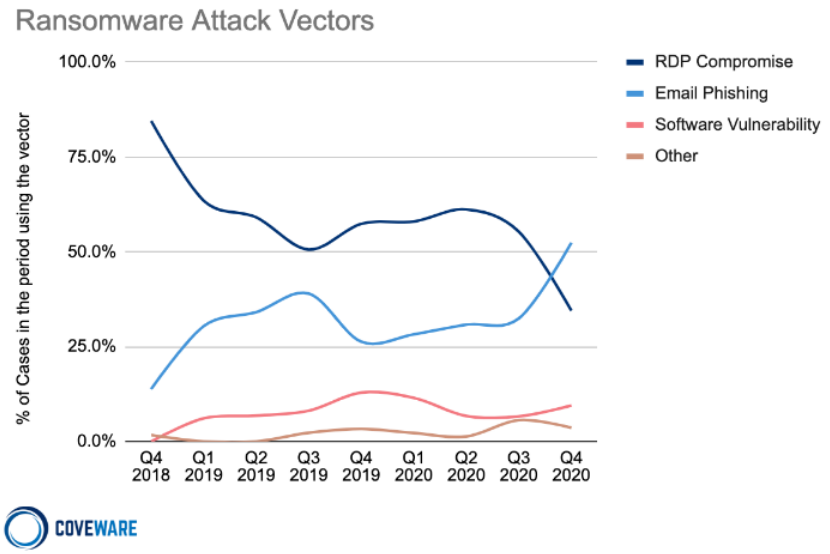
Trends binnen het ransomware domein
Op het moment is ransomware volgens het CBS de voornaamste oorzaak van het uitvallen of anderszins onbruikbaar worden van systemen (CBS, 2020). In overeenstemming met deze bevindingen categoriseert ook de NCTV ransomware als één van de top vier risico's voor de nationale veiligheid binnen het thema cybersecurity (NCTV, 2021). Begrijpelijk, niet alleen vanwege de huidige getallen, maar zeker ook gezien de exponentiële toename die heeft plaatsgevonden in het gebruik van ransomware. Zo is geconstateerd dat ransomware aanvallen van 2019 tot 2020 in aantal verdubbelden, gebruikt werden bij 10% van alle data breaches, en het de derde meest populaire vorm van malware was (Verizon, 2020). Verzekeringsmaatschappij Allianz komt eveneens tot hoge cijfers en geeft aan dat ransomware aanvallen samen met DDOS-aanvallen verantwoordelijk waren voor 81% van cyberverzekeringsclaims in 2020 (Allianz Global Corporate & Specialty, 2021). Marsh, een andere verzekeringsmaatschappij, toont lagere cijfers voor Europa en komt uit op 32% van alle cyberclaims in 2020 (Marsh, 2021). Desalniettemin zien beide bedrijven een sterke groei van claims gerelateerd aan ransomware aanvallen ten opzichte van eerdere jaren. Allianz geeft aan dat het totaal aantal claims op ransomware tot juli 2021 al hetzelfde was als het totaal aantal claims in heel 2019, en Marsh constateert eenzelfde soort verdubbeling (Allianz Global Corporate & Specialty, 2021; Marsh, 2021).

De VS treasury Financial Crimes Enforcement Network heeft een diepgaand onderzoek verricht naar aanleiding van de Colonial Pipline hack. Het onderzoek keek naar "Suspicious Activity Reports" (SARs) in relatie tot ransomware en kwam tot de conclusie dat er sprake was van een 42% toename van SARs in de eerste helft van 2021 vergeleken met 2020. Als de trend zou doorzetten tot het einde van het jaar, zou het totale aantal transacties in 2021 meer zijn dan van de afgelopen 10 jaar gecombineerd (FinCEN, 2021)

Verder zien we een verandering in de methodiek waarmee ransomware aanvallen worden uitgevoerd. Zogenoemde "double extortion" aanvallen komen steeds vaker voor. Hierbij worden niet alleen de systemen van een organisatie versleuteld, maar wordt ook gedreigd om de gestolen data openbaar te maken (NCTV, 2021; FinCEN, 2021; Lella et al., 2021a). Zo zag Coveware dat in 70% van alle

ransomware aanvallen in het laatste kwartaal van 2020 de methode van double extortion werd toegepast. In toenemende mate komen nu ook zogenoemde “triple extortion” aanvallen voor waarmee, naast het versleutelen van systemen en het dreigen met het publiekelijk maken van gestolen data, klanten van de geraakte organisatie worden bedreigd om losgeld te betalen in ruil voor het niet publiceren van hun gegevens (Allianz Global Corporate & Specialty, 2021).
Er is ook een professionalisering gaande van de criminelen die zich bezighouden met ransomware. Ransomware wordt namelijk as-a-Service aangeboden (RaaS), waarbij tools verkocht en openbaar gemaakt worden voor anderen die niet over de technische kennis beschikken om systemen te infiltreren en te besmetten met ransomware (NCTV, 2021; NCSC, 2020).

Aanvalsvectoren van Ransomware
Hackers hebben een manier nodig om systemen binnen te dringen. Het Cybersecurity & Infrastructuur Security Agency (CISA) uit de VS schrijft dat ransomware het makkelijkst bij organisaties binnenkomt via email phishing, Remote Desktop Protocol (RDP) compromise, of via een kwetsbaarheid in de soft- of hardware van een bedrijf (CISA, 2020). ENISA voegt daaraan toe dat terwijl de RDP aanvalsvector in absolute zin aan het afnemen is, de aanvallen via phishing mail juist in opkomst zijn (Lella et al., 2021a). Het bedrijf Keeper constateert dat 42% van alle ransomware aanvallen te linken zijn aan phishing emails. Daarnaast heeft Coveware een trendanalyse uitgevoerd en een overzicht gecreëerd van de ransomware aanvalsvectoren (Figuur 5) die de onderzoeksresultaten van zowel ENISA als Keeper bevestigen (Siegel, 2020; Keeper, 2021).



Figuur 5 Aanvalsvectoren van ransomware.

Hoewel RDP, email phishing en het uitbuiten van kwetsbaarheden in software de populairste manieren zijn om ransomware aanvallen uit te voeren, zien we een toename in aanvallen die via de supply chain plaatsvinden. Hierbij worden externe leveranciers van systemen geraakt door een cyberaanval, waardoor klanten van dat bedrijf ook worden geraakt (NCTV, 2021). Denk hierbij bijvoorbeeld aan de SolarWinds hack in de VS of de Kaseya hack. ENISA voorspelt dat supply chain aanvallen in 2021 zullen verviervoudigen vergeleken met het jaar ervoor (Lella et al., 2021b). Daarnaast wijst ENISA er in hetzelfde onderzoek op dat 66% van de

leveranciers niet wisten hoe zij waren gecompromitteerd, waardoor niet met zekerheid valt te zeggen welke maatregelen getroffen moeten worden om supply chain aanvallen te voorkomen.

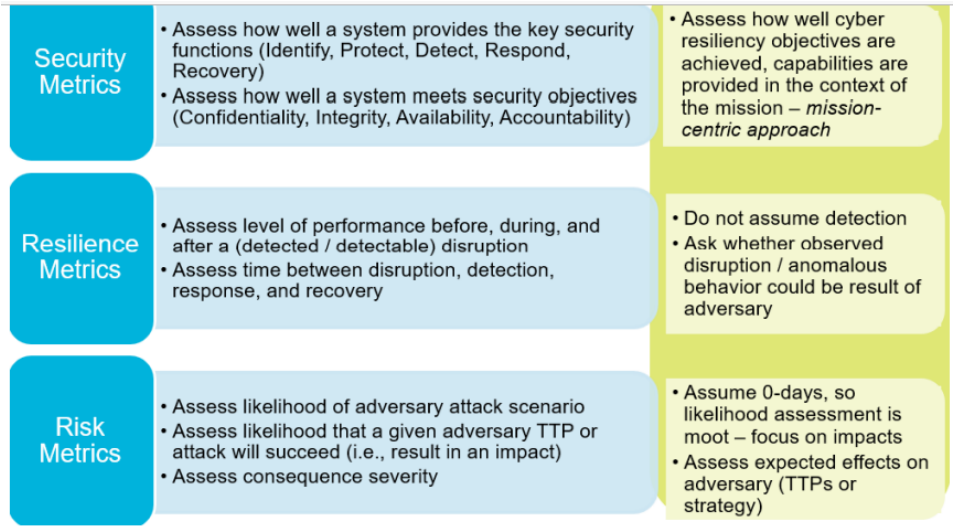
Ransomware actoren
Het type hackers dat gebruik maakt van ransomware is divers en complex. Binnen dit onderzoek richten we ons op vier soorten actoren die het meest relevant zijn. Hieronder vallen scriptgebruikers, insiders/medewerkers, cybercriminelen en statelijke actoren. Daarnaast zijn een aantal variaties op deze actoren geïdentificeerd die ook van belang zijn. De NCTV en Coveware benoemen bijvoorbeeld RaaS als actoren binnen het ransomware domein.[2] Het uitvoeren van een ransomware aanval door RaaS wordt makkelijker voor gebruikers met beperkte technische kennis (NCTV 2021; Siegel, 2021).
ENISA geeft naast statelijke actoren en cybercriminelen ook hacktivisten en hackers for hire aan als mogelijk actoren in de brede context van cybersecurity.

In het Verizon rapport (2021) staat beschreven wat de motivaties zijn van al deze actoren. Hierbij moet de kanttekening worden geplaatst dat dit rapport gaat over aanvallen in algemene zin en niet specifiek gericht is op ransomware. Uit dit rapport blijken financiële motieven en spionage de top twee populairste motieven te zijn voor respectievelijk criminele organisaties en statelijke actoren wanneer het gaat om aanvallen op de vitale sector. De NCTV sluit zich hierbij aan en concludeert dat actoren zich vooral richten op het verstoren van belangrijke digitale processen voor financieel gewin (NCTV, 2021).

3.5 Risico-inschattingen voor de eigen infrastructuur

De derde categorie gegevens betreft het organisatie-specifieke deel van de risico-inschattingen. Voor dit type gegevens geldt dat deze sterk afhankelijk zijn van de specifieke digitale architectuur van de betrokken organisatie, de genomen cybersecuritymaatregelen en hun effectiviteit.
Dit maakt dat het voor deze categorie gegevens niet voor de hand ligt om gebruik te maken van algemene data. Wel is zo veel mogelijk aansluiting gezocht met andere ontwikkelingen om deze gegevens beter meetbaar te maken. Hierbij bleken de gegevens rond metrics aanknopingspunten te bevatten. Metrics is één van de richtingen die wordt benut om cybersecurity afweging te ondersteunen. De inventarisatie van Waldron (2019) geeft aan dat er nog geen standaard systeem van cyber metrics beschikbaar is.
Er kunnen verschillende typen metrics worden onderkend, zoals weergegeven in Figuur 6.

[2] Aangezien groeperingen die tools creëren en aanbieden om ransomware aanvallen uit te voeren (en een deel van de inkomsten ontvangen die middels aanvallen wordt gegenereerd) de tools niet zelf gebruiken, staat het ter discussie of deze ook moeten worden meegenomen als actor.



Figuur 6 Overzicht categorieën metrics. (Mitre2018)

Voor de case studies bleek elk van deze categorieën metrics van belang. Hierbij is vastgesteld dat een deel van de metrics goed is in te schatten (bijvoorbeeld de kans op succes van een phishing mail), terwijl dat voor andere metrics een stuk moeilijker is (bijvoorbeeld de kans en tijdsduur voor detectie).

3.6 Samenvatting en conclusies

Ten behoeve van de risicoanalyses worden drie categorieën van gegevens onderscheiden. Voor elk van deze categorieën is ter voorbereiding van de case studies een literatuuronderzoek uitgevoerd naar relevante gegevens.
Op grond van het literatuuronderzoek zijn de volgende conclusies te trekken:

- *De mogelijke impact van aanvallen:* gegevens over de impact bleken slecht toegankelijk en deels onbetrouwbaar en waren onvoldoende van kwaliteit en kwantiteit om een eigen database van op te bouwen. De gegevens die beschikbaar zijn leggen de nadruk op de financiële aspecten en minder op de andere aspecten die ook relevant zijn in de context van vitale sectoren. Voor de vitale infrastructuur is vooral de eventuele verstoring van de vitale processen van belang (duur en grootte). Als mogelijke typen bronnen voor deze gegevens zijn onderkend:
  - gegevens uit openbare bronnen, waaronder databases met vitale infrastructuur incidenten en academische databases rond ransomware incidenten (t.b.v. inzicht in de effecten van verstoringen);
  - statistieken en data van het CBS of gegevens van verzekeringsmaatschappijen (t.b.v. duiden financiële impact) hebben het meeste potentie.
- *De dreiging*: over de aard en trends van de dreiging is relatief veel informatie beschikbaar. Het betreft hier bijvoorbeeld informatie over veelvoorkomende aanvalsvectoren en trends in de aantallen en soorten aanvallen.
- *Metrics over de weerbaarheid:* Dit onderdeel betreft gegevens die sterk organisatie-specifiek zijn en afhangen van de gekozen beveiligingsmaatregelen. Hiervoor kan wel gebruik gemaakt worden van algemeen gehanteerde metrics, maar dient de inschatting organisatie-specifiek te worden gemaakt.

4 Resultaten van de case studies

4.1 Inleiding

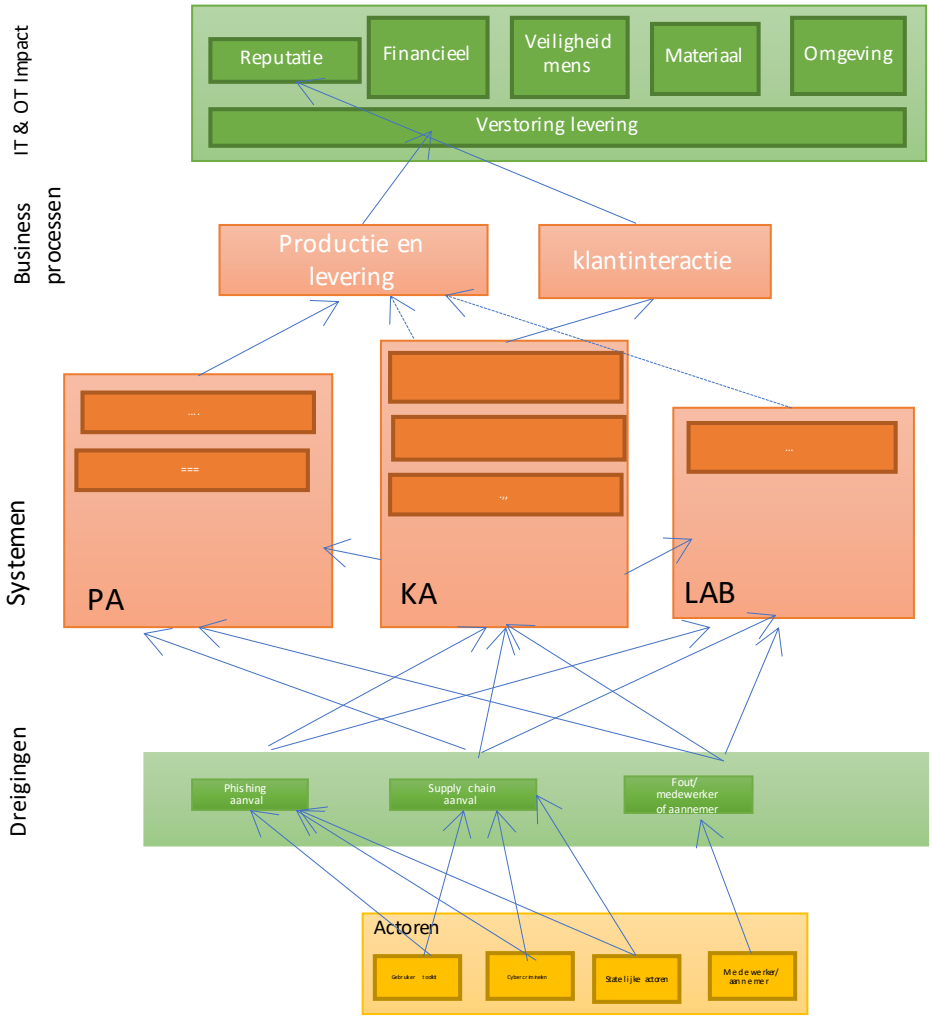
Op basis van de eerder uitgevoerde case studie in 2020 is een basismodel ontwikkeld en gebruikt voor de uitgevoerde case studies in het tweede jaar van het onderzoek (2021). Hiervoor is het eerder ontwikkelde model aangepast op basis van de eigenschappen van de sector waarin de case studies plaatsvonden en voor de onderzochte dreiging ransomware.
Dit hoofdstuk beschrijft het gebruikte basismodel en de ervaringen met dit model bij de twee uitgevoerde case studies.

4.2 Gebruikte basismodel

Het uitgangspunt van beide case studies in 2021 was het onderzoeken van het dreigingsscenario ransomware. In verschillende workshops is dit dreigingsscenario behandeld met betrekking tot systemen en bedrijfsprocessen van de case organisaties.

In het basismodel voor het kwantificeren van cyberrisico's (zie Figuur 2) wordt gekeken naar de verschillende fases van de dreiging: *threat, threat inside, damage* en *client impact*. Gerelateerd aan deze fases zijn er preventieve en reactieve maatregelen mogelijk in de vorm van detectie en mitigerende acties.

Op basis van informatie van beide case organisaties is dit model verder uitgewerkt, zoals weergegeven in Figuur 7. Per blok worden de belangrijkste elementen toegelicht.



Figuur 7 Overzicht uitgewerkte model.

Bedrijfsprocessen en IT & OT impactfactoren

Voor de vitale processen geldt de mogelijke verstoring van de levering van de vitale dienst of het product als belangrijkste impact. De borging van de leveringszekerheid van vitale diensten of producten is voor beide case organisaties van het grootste belang. Daarnaast wordt ook reputatieschade als zeer belangrijk gezien. Andere impactfactoren zoals financiële impact en impact op de omgeving spelen een secundaire rol.

In overeenstemming met deze prioritering van de impact worden van de bedrijfsprocessen vooral de primaire processen rond de productie van het vitale product en de klantinteractie van belang geacht.

Dreigingen

Voor de case studies is het onderwerp ransomware als uitgangspunt genomen. In de uitwerking van dit scenario zijn er een aantal onderwerpen behandeld die in onderstaande alinea's worden besproken.

Actoren
Voor de case studies is uitgegaan van de volgende actoren[3]: scriptgebruikers, cybercriminelen, statelijke actoren en insiders/medewerkers.
Deze actoren verschillen in de mate van bekwaamheid, resources (in tijd en geld), motivatie en de mogelijkheden waarmee zij toegang tot de systemen van de betrokken organisaties kunnen krijgen.

Aanvalsvectoren
Voor de installatie van mogelijke malware/ransomware op de systemen zijn tijdens de workshops de volgende aanvalspaden behandeld:
- Via internet-facing kwetsbaarheden en verkeerde configuratie;
- Door een phishing aanval;
- Via de supply chain, bijvoorbeeld een malafide update;
- Via een fout van een medewerker of aannemer, waardoor er een besmetting op een van de systemen plaatsvindt.

Elk van deze aanvalspaden kan leiden tot initiële toegang tot de systemen. Voor het vergroten van de effectiviteit van de aanval zal de aanvaller vervolgens proberen andere systemen te infiltreren en te besmetten. De aanvalsvectoren zijn tijdens de workshops besproken aan de hand van de ransomware kill chain.

Figuur 8 De ransomware kill chain. (CSBN, 2021)

Hoofdindeling systemen
Bij de betrokken bedrijven uit de vitale sector wordt een aantal omgevingen onderscheiden:
- Procesautomatisering (PA);
- Kantoorautomatisering (KA);
- Laboratoriumautomatisering (LAB).

Procesautomatisering (PA)
De procesautomatisering draagt zorg voor aansturing en uitvoering van de kernprocessen. Binnen de PA kan in zijn algemeenheid onderscheid gemaakt worden tussen:
- De PA op locaties;
- De lokale besturing op de locaties;
- De centrale sturing.

Voor de beschouwde organisaties geldt dat de PA omgeving afgeschermd is van de LAB en de KA omgevingen en geen directe internetverbinding kent. Hierdoor is een directe besmetting via phishing of via internet-facing kwetsbaarheden niet mogelijk.

[3] Binnen het CSBN 2020 wordt een actor gedefinieerd als “Een persoon of samenstelling van personen die een cyberaanval uitvoert of de intentie daartoe heeft”. Voorbeelden zijn a) staten/ staatsgelieerde actor, b) criminelen, c) terroristen, d) hacktivisten, e) cybervandalen en scriptkiddies en f) insiders.

Een aanval via de supply chain of een fout van een medewerker of aannemer kunnen potentieel wel een risico vormen.

Kantoorautomatisering (KA)
De kantoorautomatisering draagt bij aan een groot aantal ondersteunende processen en de klantinteractie. Vanwege het karakter van de taken van de KA is dit een omgeving met meer externe connecties in vergelijking met de andere omgevingen.

Laboratoriumautomatisering (LAB)
De laboratoriumautomatisering ondersteunt de controles op de kwaliteit.
Ook de LAB omgeving wordt benaderd via de KA omgeving.

Maatregelen
Zoals eerder aangegeven in Figuur 2 kunnen maatregelen tegen ransomware op verschillende manieren invloed uitoefenen op de organisatie. In de workshops zijn maatregelen besproken die, gegeven een verstoring in de systemen, de impact hiervan op de bedrijfsprocessen verminderen. Deze maatregelen zijn als volgt:

- Doordraaien met bestaande instellingen. Wanneer de KA of centrale sturing verstoord raakt is de verwachting dat de PA nog enige tijd zonder nadelige gevolgen kan doordraaien met de bestaande instellingen.
- Er bestaan verschillende terugvalniveaus in de besturing, waardoor de besturing ook lokaal kan worden overgenomen of zelfs op handbediening kan worden overgegaan. Er kan onderscheid gemaakt worden tussen:
  - Regulier – centraal op afstand besturen;
  - Lokale besturing;
  - Besturing via PLC;
  - Handbediening.
- Calamiteitenplannen. De bedrijven beschikken over calamiteitenplannen om met onvoorziene omstandigheden om te gaan.
- Afspraken met collega-bedrijven over de overname van bepaalde taken.

Preventieve maatregelen
Er zijn maatregelen genomen om te voorkomen dat systemen besmet raken, of dat een eventuele besmetting zich kan verspreiden. Hiervan zijn onder andere de volgende maatregelen besproken:

- Beperken van user rechten en accounts;
- Test emails ter voorbereiding op phishing mails;
- Patch management systeem;
- Netwerk scheiding;
- Virtuele scheiding van IT en OT devices;
- Toepassing IEC norm 62443[4] voor PA omgeving.

[4] https://en.wikipedia.org/wiki/IEC_62443

Detectie en respons
Voor maatregelen die voor detectie en responscapaciteit zorgen zijn de volgende aspecten besproken:

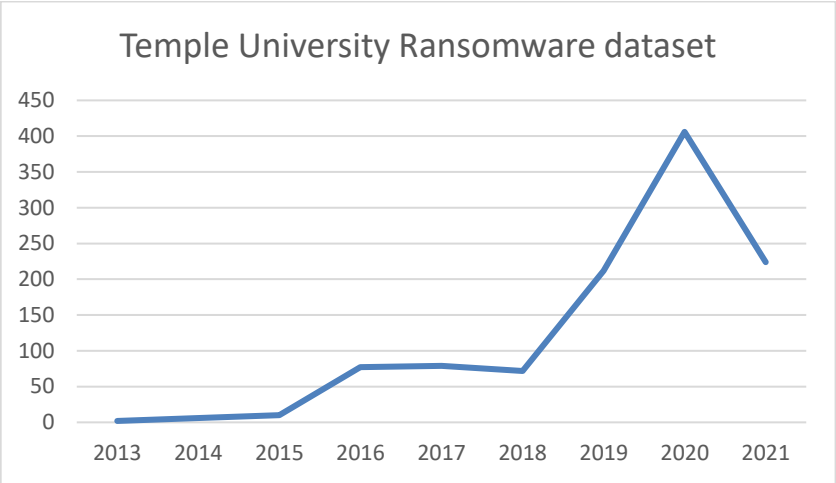
- Logging;
- Spam filters;
- Multilayer firewall en filter van netwerkverkeer;
- Anti-virus en malwareprogramma's;
- Intrusion detection systemen;
- Incident respons proces.

4.3 Specifieke gegevens voor de case studies

In hoofdstuk 3 is toegelicht wat de verschillende trends, actoren en aanvalsvectoren zijn met betrekking tot ransomware. Deze sectie zal zich specifiek richten op ransomware binnen de vitale infrastructuur en de trends, actoren en aanvalsvectoren die daarin worden waargenomen.

Aangetaste sectoren
De berichtgeving over succesvolle ransomware aanvallen toont dat geen enkele sector veilig is voor ransomware aanvallen. Naast overheidsinstanties worden ook industrieën zoals gezondheidszorg, onderwijs en informatietechnologie aangevallen (Rege, 2021; Sobers, 2021). De vitale infrastructuren die voorzieningen leveren zoals water, elektriciteit en gas, staan voornamelijk onderaan de lijst. In totaal zijn maar 2%-4% van alle ransomware aanvallen gericht op deze industrieën (Siegel, 2021; Rege, 2021). Belangrijke kanttekening bij deze cijfers is dat ze gebaseerd zijn op wereldwijde cijfers en cijfers uit de Verenigde Staten. We constateren een gebrek aan vergelijkbare gegevens over deze dreiging in Nederland.
Dit betekent overigens niet dat deze percentages verwaarloosbaar zijn. Het Cybersecurity Beeld 2021 zegt hierover het volgende: "Hoewel gerichte ransomware-aanvallen op de vitale processen nog niet in Nederland hebben plaatsgevonden, komen deze reeds in het buitenland voor." (NCTV, 2021, p.9) Denk hierbij bijvoorbeeld aan recente cyberaanvallen zoals hacks op een waterbedrijf in Florida, de Colonial pipeline hack en de hack op een waterbedrijf in Queensland Australië. In Queensland is de hack pas na 9 maanden gedetecteerd.

Trends in ransomware
Zoals benoemd in de voorgaande alinea is tot dusver de vitale infrastructuur in Nederland nog niet uitgevallen als gevolg van ransomware aanvallen. Desalniettemin zien we wel een veranderende trend in aanvallen op de vitale infrastructuur. Zo benoemde de Canadese inlichtingendienst (Communications Security Establishment) dat in 2021 de helft van alle ransomware aanvallen gericht waren op de vitale infrastructuur en er sprake was van een toename van 151% (in vergelijking met 2020). Hetzelfde beeld komt naar voren uit de vitale infrastructuur dataset van Temple University, waarin een exponentiele groei wordt aangegeven sinds 2019 zoals weergegeven in Figuur 9 (Rege, 2021).



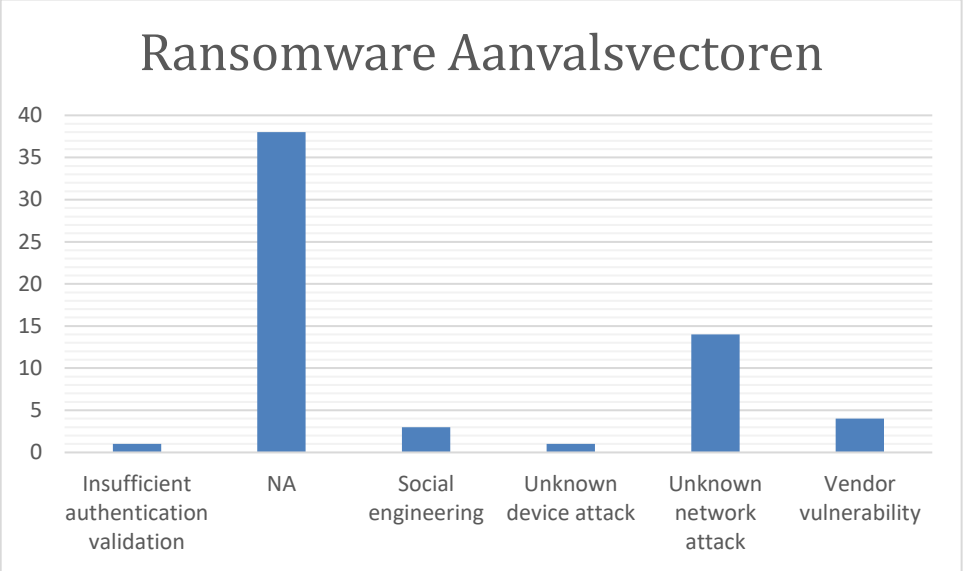
Figuur 9 Aantal ransomware incidenten met betrekking tot vitale infrastructuur per jaar tot november 2021 (Rege, 2021).

Ransomware actoren

Specifiek kijkend naar energie- en waterbedrijven zien we dat 78%-100% van de ransomware aanvallen financieel gemotiveerd zijn en 0%-33% door spionage. Daarbij komt dat 98% van alle aanvallen van buitenaf komt en maar 2% vanuit de organisatie (Verizon, 2021). De dataset van de universiteit van Queensland waar verschillende cyberaanvallen in kaart worden gebracht, toont dat binnen de vitale infrastructuur alle aanvallen door externe daders zijn gepleegd (Tsen, Ko, & Slapničar, 2020). Ook Allianz geeft aan dat een groot deel van de cyberaanvallen van buitenaf komt en dat 81% van de schadeclaims van buiten het bedrijf afkomstig zijn. Tien procent van de incidenten is voortgekomen door een eigen medewerker. Dit ging echter over alle sectoren en niet alleen over de sectoren met vitale aanbieders (Allianz Global Corporate & Specialty, 2021).

Aanvalsvectoren ransomware

Volgens het Verizon rapport (2021) wordt het merendeel van de aanvallen in de nutsvoorzieningen uitgevoerd via social engineering met aanhoudende phishing campagnes, wat betekent dat medewerkers onbewust op vijandelijke links klikken en malware installeren. Daarnaast geeft het rapport aan dat bij 44% van de aanvallen waar geen gebruik werd gemaakt van social engineering het om ransomware ging. Overige data over aanvalsvectoren zijn erg gelimiteerd. Naast het Verizon rapport geeft de ransomware database van de Universiteit van Queensland als één van de weinige bronnen inzicht in de verschillende aanvalsvectoren die worden gebruikt. Het voornaamste inzicht uit deze database is dat bij het merendeel van de aanvallen op de vitale infrastructuur de aanvalsvectoren niet bekend zijn, zoals weergegeven in Figuur 10 (Tsen, Ko, & Slapničar, 2020).



Figuur 10 Overzicht van verschillende aanvalsvectoren binnen de vitale infrastructuur met betrekking tot ransomware N-61. (Tsen, Ko, & Slapničar 2020).

4.4 Ervaringen en resultaten van de case studies

Dit hoofdstuk bevat een geanonimiseerde beschrijving van de case studies. In een aanpalende vertrouwelijke rapportage zijn de resultaten teruggekoppeld aan de organisaties waarvoor de cases zijn uitgevoerd. In dit onderdeel worden de ervaringen en resultaten toegelicht.

Beschikbaarheid gegevens
Voor de case studies bleek relatief veel informatie beschikbaar. De bedrijven die bij de case studies betrokken zijn hadden ervaring met het uitvoeren van risicoanalyses. Hierdoor kon het basismodel verrijkt worden met specifieke gegevens voor de sector. De volgende type gegevens waren beschikbaar bij de case organisaties:

- gegevens over de eigen systemen, de architectuur en de samenhang met de bedrijfsprocessen;
- gegevens over de genomen maatregelen tegen de dreiging van ransomware.

Het basismodel dat opgesteld is zonder samenwerking met de sector bleek door de beschikbaarheid van deze gegevens en ervaringen goed werkbaar. Slechts minimale aanpassingen waren nodig om het basismodel toepasbaar te maken voor de organisatie.

Indeling actoren
Voor de organisaties die deelnamen aan de case studies geldt dat zij zich het meest zorgen maakten over statelijke actoren en cybercriminelen. Deze worden gezien als de actoren met de meeste tijd, middelen en kennis om daadwerkelijk een aanval uit te voeren. De insiders/medewerkers werd als een beperkte dreiging gezien en zouden voornamelijk verantwoordelijk zijn voor het per ongeluk installeren van malware in plaats van daadwerkelijk een kwaadwillige actie uit te voeren. De deelnemers zagen scriptgebruikers niet als een serieuze dreiging omdat zij verwachtten dat de reeds genomen maatregelen voldoende bescherming bieden tegen dit type actor.

Type aanvalsvector
Gegevens over de inschattingen van de effectiviteit van een aanval bleken nauwelijks beschikbaar te zijn. Voor de inschatting van de kans van slagen van een gekozen aanval bleken verschillen tussen de beide case organisaties te bestaan ten gevolge van de genomen maatregelen.
Voor beide organisaties bleek het een uitdaging te zijn om een kans inschatting te maken van de aanvalsmethoden voor verschillende actoren. Er werden veel voorbeelden benoemd van hoe een aanvalsmethode mogelijk zou kunnen verlopen alsmede de waarschijnlijkheid van de verschillende aanvalspaden. Het vertalen van deze voorbeelden en waarschijnlijkheden in concrete getallen blijft echter lastig.

Maatregelen
De organisaties uit beide casestudies beschikten over een reeks van verschillende maatregelen om een aanval te voorkomen of te mitigeren. Bij de workshops is aandacht besteed aan de balans tussen de preventieve maatregelen en de cyberdetectie- en responsmaatregelen. Voor aanvallers met hoge expertise kan niet worden uitgesloten dat zij succesvol binnenkomen. In dit geval ligt de nadruk meer op het voorkomen van de verspreiding en een snelle detectie en respons.

Algemene bevindingen casestudies
Samenvattend is uit de case studies en workshops gebleken dat beide organisaties de nodige ervaring met risico analyses hebben en deze op regelmatige basis uitvoeren. Daarbij hebben de organisaties een goed overzicht van hun systemen en processen en over waar en hoe een ransomware aanval kan worden uitgevoerd. Het basismodel heeft beide organisaties inzicht gegeven in de mogelijke aanvalspaden en de mogelijke impact op de bedrijfsprocessen. Daarbij is het van belang om tijdens het opstellen van het model een balans te vinden in de mate van detail die wordt toegevoegd. Toen de betrokken organisatie te veel details wilde toevoegen werd de benodigde inspanning voor het maken van de inschattingen te groot. Bij te weinig detail konden de aanvalspaden en mogelijke maatregelen onvoldoende worden onderscheiden. Daarnaast vonden sommige deelnemers het moeilijk om een kans inschatting te maken wegens een gebrek aan gegevens. Het onderling afwegen van de waarschijnlijkheid van de aanvalspaden was in deze situaties wel mogelijk.

5 Conclusies

5.1 Met betrekking tot de methode

De in 2020 ontwikkelde methode bestaat uit twee elementen: een basismodel en een stappenplan om dit model door middel van een aantal workshops te verrijken tot een specifieker model voor de case studie. Deze werkwijze bleek in beide case studies hanteerbaar.
In beide case studies bleek het voor de organisaties een uitdaging om op basis van het model gedetailleerde kansinschattingen te maken. Voor deelonderwerpen in het model was dit wel mogelijk (zoals de kans op een geslaagde phishing aanval), maar voor de effectiviteit van de vervolgacties (maatregelen) tegen ransomware aanvallen bleken de inschattingen moeilijker te maken.

Als positieve effecten van de aanpak zijn benoemd:
- het bijeenbrengen van de expertise binnen de organisatie, variërend van crisismanager en ICT, procesautomatisering en cyber kennis;
- het gezamenlijk onderkennen en bespreken van mogelijke aanvalspaden.

Als aandachtspunten gelden:
- Voor een deel van het model bleek het niet mogelijk om tijdens de workshops betrouwbare inschattingen te maken over het risico dat organisaties lopen tegen cyberdreigingen.
- Het omgaan met een groot aantal variabelen die soms lastig van elkaar te scheiden zijn blijft een uitdaging (de kans dat iets gebeurt hangt bijvoorbeeld af van de vaardigheid en motivatie van de actor).
- Het bepalen van de juiste mate van detail is een uitdaging. Te veel detail is voor de gebruikers van het basismodel onwerkbaar, vanwege de hoeveelheid werk die dat met zich meebrengt. Daarnaast is er voor veel inschattingen onvoldoende data beschikbaar. Te weinig detail biedt geen onderscheidend vermogen en maakt het maken van kansinschattingen moeilijk, omdat gebruikers niet kunnen overzien wat mogelijk allemaal een rol speelt voor hun eigen organisatie.

5.2 Beschikbaarheid gegevens

Bij de eerste case studie in 2020 bleek het lastig om kwantitatieve inschattingen te maken door een gebrek aan gegevens. In vergelijking tot deze eerste case studie beschikten beide case organisaties van 2021 over meer basisgegevens voor de te maken inschattingen. Zo waren bijvoorbeeld gegevens over de effectiviteit van phishing aanvallen voorhanden en was meer informatie beschikbaar over de maatregelen en de mogelijke impact.
De door het onderzoeksteam vooraf verzamelde gegevens hebben bijgedragen om een scherper beeld te creëren en een eerste inschatting te maken voor een deel van de elementen. Zonder deze gegevens is de vertaling van het basismodel naar de specifieke werkelijkheid van een organisatie een te grote stap.
Met name voor de impact (blok 1) en de dreiging (blok 3) bleek het mogelijk om gegevens aan te leveren die het maken van inschattingen ondersteunen.

Algemene observaties:

- *De mogelijke impact van aanvallen:* gegevens over de impact van cyberdreigingen bleken slecht toegankelijk en deels onbetrouwbaar.
  De gegevens die beschikbaar zijn leggen de nadruk op de financiële aspecten en implicaties van een aanval en minder op andere aspecten die ook relevant zijn in de context van vitale sectoren. Voor de vitale infrastructuur is primair de verstoring van de vitale processen van belang (duur en grootte). Het onderzoeksteam heeft alternatieve bronnen geïdentificeerd waar deze gegevens mogelijk wel voor handen zijn:
  - gegevens uit openbare bronnen, waaronder databases met vitale infrastructuur incidenten en academische databases rond ransomware incidenten (t.b.v. inzicht in de effecten van verstoringen);
  - statistieken en data van het CBS of gegevens van verzekeringsmaatschappijen (t.b.v. duiden financiële impact), deze hebben het meeste potentie.
- *De dreiging*: over de aard en trends van de dreiging is relatief veel informatie beschikbaar. Het betreft bijvoorbeeld informatie over veelvoorkomende aanvalsvectoren en trends in de aantallen en soorten aanvallen. Deze informatie is deels beschikbaar in NCSC rapportages en in Amerikaanse bronnen.
- *Gegevens over de weerbaarheid van de systemen:* dit betreft gegevens die zowel vanwege de systemen zelf als de gekozen beveiligingsmaatregelen sterk organisatie-specifiek zijn. Hiervoor kan wel gebruik gemaakt worden van algemeen gehanteerde metrics, maar de inschatting dient in sterke mate op de organisatie te worden afgestemd.

5.3 Doorontwikkeling

In het derde en laatste jaar van het onderzoeksprogramma (2022) wordt dit project voortgezet. De werkzaamheden in 2022 zijn erop gericht om de ontwikkelde methode te ontsluiten voor het NCSC en haar doelgroepen. Dit wordt gedaan door het ontwikkelen van 1) een factsheet waarin de methode op toegankelijke wijze wordt beschreven en 2) een toolkit waarin het onderliggende rekenmodel, aansprekende voorbeelden en ondersteunende databronnen bij elkaar worden gebracht.

Om dit te bereiken worden de volgende stappen ondernomen:

- het aanscherpen en vastleggen van de methode op basis van de use cases ten behoeve van de factsheet;
- het verzamelen en ontwikkelen van databronnen, voorbeelden en archetypes om de doelgroepen te ondersteunen bij het organisatie-specifiek maken en vullen van het rekenmodel (Archetypes zijn vooraf gestructureerde en ingevulde onderdelen van het hoofdmodel. Organisaties kunnen deze archetypes gebruiken om mee te beginnen, om vervolgens zelf het model aan te passen naar behoefte. Hierdoor hoeft men niet vanaf scratch te beginnen en wordt de drempel verlaagd om met kwantificering aan de slag te gaan.);
- het bij elkaar brengen van alle informatie in een overzichtelijk geheel in de vorm van een toolkit.

6 Bronnen

Allianz Global Corporate & Specialty SE. (2021, oktober). *Ransomware trends: Risks and Resilience*. https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/agcs-ransomware-trends-risks-and-resilience.pdf

Bodeau, D. J., Graubart, R. D., McQuaid, R. M., & Woodill, J. (2018, september). *Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring*. Mitre. https://www.mitre.org/sites/default/files/publications/pr-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf

Judith Boot (2021) Impact Rapport: Analyse en bevindingen over de impact van cyber incidenten. Rapport opvraagbaar bij auteurs.

Centraal Bureau voor de Statistiek (CBS). (2021, mei). *Cybersecuritymonitor 2020*. https://www.cbs.nl/nl-nl/publicatie/2021/18/cybersecuritymonitor-2020

Communications Security Establishment Canada. (2021, 6 december). *Ministers urge Canadian organizations to take action against ransomware*. Canada.Ca. Geraadpleegd op 12 december 2021, van https://www.canada.ca/en/communications-security/news/2021/12/ministers-urge-canadian-organizations-to-take-action-against-ransomware.html

Cybersecurity & Infrastructure Security Agency. (2020, september). *Ransomware guide*. https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

Financial Crimes Enforcement Network. (2021, oktober). *Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021*. FinCen. https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf

Franke U, Turell J., Johansson I, (2021, pre-print CRITIS conferentie). *The cost of incidents in essential services—data from Swedish NIS reporting?*

Keeper Security, inc. (2021). *Ransomware impact report 2021*. https://www.keeper.io/hubfs/2021_Ransomware_Impact_Report/2021_Ransomware_Impact_Report.pdf

Lagarde, R., Koens, T., Zeijlemaker, S., Samwel, P., Paske, B., Verweij, E., Kerkdijk, R., & Wolthuis, R. (2017). *Library of Cyber Resilience Metrics* (R. Kerkdijk, Red.). TNO. http://resolver.tudelft.nl/uuid:57da4ef3-7600-479d-954c-e1a4a5122a1e

Langenkamp, L, Egmond M van, Klaver, M. (2020), Kwantificering cyberrisico's: rapportage 2020.

Lella, I., Theocharidou, M., Tsekmezoglou, E., Malatras, A., Ardagna, C., Corbiaux, S., Sfakianakis, A. & Douligeris, C. (Reds.). (2021a, oktober). *ENISA threat landscape 2021*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Lella, I., Theocharidou, M., Tsekmezoglou, E., Tsekmezoglou, A., European Union Agency for Cybersecurity, Garcoa, S., Valeros, V. & Czech Technical University in Prague (Reds.). (2021b, juli). *ENISA threat landscape for supply chain attacks* . ENISA. https://doi.org/10.2824/168593

Luiijf H, Klaver M, (2021, december), *Analysis and lessons identified on critical infrastructures and dependencies from an empirical data set.*

Marsh, Microsoft, KIVU & CMS. (2021, augustus). *The Changing Face of Cyber Claims 2021*. MARSH. https://www.marsh.com/nl/nl/services/cyber-risk/insights/the-changing-face-of-cyber-claims.html?utm_source=google-adwords&utm_medium=paid-search&utm_campaign=alwayson&utm_content=cyberclaimsreport&gclid=EAIaIQobChMI1e_Wm_3R9AIVC6h3Ch259AT2EAAYASAAEgIduvD_BwE

McCandless, D. & Maslekar, S. (2021, 13 september). *Ransomware Attacks*. Information Is Beautiful. Geraadpleegd op 3 december 2021, van https://informationisbeautiful.net/visualizations/ransomware-attacks/

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) & Nationaal Cyber Security Centrum (NCSC). (2021, juni). *Cybersecuritybeeld Nederland 2021 (CSBN 2021)* (Nr. 1). Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021

NetDiligence, (2021), *Cyber claims study, 2021 report.*

NIS Coordination Group, CG Publication 02/2018, (2018) *Reference document on Incident Notification for Operators of Essential Services Circumstances of notification, draft versie.*

NIS Coordination Group, CG Publication 03/20, (2020, december). *Annual Report NIS Directive Incidents 2019.* https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

Ransomware Task Force (2021, april), *Combating Ransomware.* https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf

Rege, A. (2013–2021, november). *Critical Infrastructures Ransomware Attacks (CIRWAs) Incident Dataset* (11.7) [Dataset]. Temple University College of Liberal Arts. https://sites.temple.edu/care/cira/

Siegel, B. (2021, 10 november). *Ransomware Payments Decline in Q4 2020*. Coveware: Ransomware Recovery First Responders. Geraadpleegd op 3 december 2021, van https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020#vectors

Sobers, R. (2021, juli). *81 Ransomware Statistics, Data, Trends and Facts for 2021 | Varonis*. Varonis. Geraadpleegd op 3 december 2021, van https://www.varonis.com/blog/ransomware-statistics-2021

Tsen, E., Ko, R. & Slapnicar, S. (2004–2020). *Dataset of data breaches and ransomware attacks over 15 years from 2004* [Dataset]. The University of Queensland. https://doi.org/10.14264/dfe5027

Verizon. (2021, mei). *2021 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/

Waldron, K. (2019, oktober). *Resources for Measuring Cybersecurity*. Rstreet. https://www.rstreet.org/wp-content/uploads/2019/10/Final-Cyberbibliography-2019.pdf

Wolthuis, R., Phillipson, F., Rochat, P., Van Ingen, B., Zeijlemaker, S. & Gorter, D. (2019). *Quantifying Cyber Security Risks*. TNO. http://resolver.tudelft.nl/uuid:045ee95e-e0d2-4380-9d24-566f99e03c59

Distributielijst Rapport TNO 2022 R10535 (P2108)

JENV

Programmabegeleider NCSC Rik van Dijk, Onderzoeker r.van.dijk@minjenv.nl	pdf
Co-referent NCSC Martin Pekarek, Teamleider onderzoekscluster m.e.pekarek@minjenv.nl	pdf
Directie X	
- x@minjenv.nl	pdf
- h.hanoeman@minjenv.nl	pdf
- b.ter.luun@minjenv.nl	pdf

POLITIE

Directie Strategie en Innovatie	
- Innovatie@politie.nl	pdf
- onderzoekscoordinatie@politie.nl	pdf
- sven.hamelink@politie.nl	pdf
- kirsten.hehemann@politie.nl	pdf

TNO

Referent, Directeur Roadmap National Security Drs. R.A.J.M. Pellemans	email-alert
VP-manager VPVM Dr. T.W.J. van Ruijven	email-alert
VP-manager KOP T.H.E.E.A. Krabbendam MSc	email-alert
Projectleider T.C.C. van Schie MSc	email-alert
Programmaleider G.R. Jansen-Ferdinandus MSc	email-alert
E. van der Weide MSc	email-alert
TNO Bibliotheek locatie Den Haag	hard copy & cd