dialogic
innovatie • interactie

Verkenning risicofactoren ransomware-aanvallen

ir. ing. Reg Brennenraedts MBA, ir. Tommy van der Vorst, Jessica Kats MSc, dr. Melanie Rieback, Anouk Vos MSc, ir. Nick Jelicic, Roos Jansen MSc, Tessel Blom MSc, Nino van Sambeek

Opdrachtgever:
WODC

Publicatienummer:
2021.148-2222

Datum:
Utrecht, 5 augustus 2022

Inhoudsopgave

Dank aan begeleidingscommissie voor hun waardevolle reacties in commentaren op dit rapport. De begeleidingscommissie bestond uit prof. dr. ir. Pieter van Gelder (TU Delft), dr. Jeroen van der Ham (University of Twente en NCSC), dr. Rutger Leukfeldt (THUAS en NSCR), dr. Joris Hulstijn (Tilburg University), dr. Isabelle van der Vegt (WODC) en drs. Casper van Nassau (WODC).

Citeren als: Dialogic (2022). *Verkenning risicofactoren ransomware-aanvallen*. In opdracht van WODC, Den Haag.

Managementsamenvatting

Introductie

In opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (hierna: WODC) heeft Dialogic een verkennend onderzoek naar risicofactoren voor ransomware-aanvallen uitgevoerd. Dit onderzoek heeft als doel het in kaart brengen en kwantificeren van factoren die ransomware-aanvallen beïnvloeden. Een tweede doelstelling is het bieden van inzicht in de mogelijkheden tot bewustwording onder bestuurders van middelgrote en kleine organisaties, zowel in de publieke als private sector. Het onderzoek beantwoordt de volgende onderzoeksvragen:

1. Welke risico's brengen ransomware-aanvallen met zich mee?
2. Hoe zien ransomware-aanvallen er tegenwoordig uit en welke instrumenten worden hierbij ingezet?
3. Welke soorten partijen zijn bij deze aanvallen betrokken?
4. Welke interne en externe factoren dragen bij aan ransomware-risico's voor een organisatie?
5. In hoeverre zijn deze factoren kwantificeerbaar?
6. Met welk instrument kunnen beleidsmakers in middelgrote en kleine organisaties bewust worden gemaakt maken van de risico's van ransomware?
7. Wat zijn belangrijke factoren voor bedrijven en organisaties om met het instrument aan de slag te gaan?

Voor de uitvoering van dit onderzoek is gebruik gemaakt van verschillende methoden: literatuuronderzoek, verkenning van bestaande risicotaxatiemodellen, verkenning van cybersecurityverzekeringen, interviews, casestudies van getroffen organisaties in Nederland en validatiesessies. In dit onderzoek wordt getracht de meest actuele situatie te schetsen van de vraagstukken die hier spelen.

Impact van ransomware-aanvallen

De eerste onderzoeksvraag luidt: *Welke risico's brengen ransomware-aanvallen met zich mee?*

Het risico op een cyberaanval is groot en groeiend. Ransomware is een specifieke cyberaanval. Hierbij richten criminelen zich meestal op het versleutelen van data van het slachtoffer en in mindere mate het voorkomen dat het slachtoffer toegang krijgt tot zijn eigen systemen. De kern van ransomware is dat het slachtoffer door de dader (typisch: vanwege de versleuteling van data) onder druk wordt gezet om iets tegen zijn of haar zin te doen. Meestal is dit het betalen van losgeld (*ransom*). Er zijn vier vormen van aanvallen. Bij *single extortion* worden bestanden versleuteld en worden slachtoffers gechanteerd door de dreiging toegang tot deze bestanden te verliezen. Bij *double extortion* worden naast versleuteling de gegevens gestolen en wordt gedreigd deze openbaar te maken. Bij *triple extortion* worden bovendien andere cyberaanvallen, zoals DDoS-aanvallen, op systemen van het slachtoffer uitgevoerd om het herstelproces complexer te maken. Tenslotte worden bij *quadruple extortion* ook de relaties van het slachtoffer gechanteerd met het openbaar maken van hun gegevens.

De impact die dergelijke aanvallen kunnen hebben op organisaties bestaat uit de volgende aspecten:

1. Additionele kosten voor de inhuur van capaciteit om op de aanval te reageren;
2. Kosten door verlies van data;

3. Kosten door openbaarmaking van data die bestaan uit (a) kosten door reputatieschade, (b) boetes, bijvoorbeeld als gevolg van de AVG en (c) schadevergoedingen;
4. Betaling van losgeld;
5. Kosten door verstoring bedrijfscontinuïteit;
6. Herstelkosten voor systemen.

De gemiddelde losgeldbetaling is lastig exact te bepalen, maar ligt waarschijnlijk tussen de $ 50.000 en $ 500.000. Het inschatten van de kosten van de verstoring van de continuïteit van ondernemingen is nog lastiger, maar lijkt een vaak veelvoud te zijn van de losgeldbetalingen. Van de andere posten is het lastig om dit kwantitatief te duiden en verschillen ook sterk per casus.

Tot slot zijn er ook maatschappelijke effecten van ransomware-aanvallen . Door ketenafhankelijkheden kan de verstoring van de bedrijfscontinuïteit van één aangevallen organisatie een grote impact hebben op andere organisaties in de keten, zoals klanten en leveranciers. De overtreffende trap hiervan zijn uiteraard aanvallen op vitale sectoren waardoor grote delen van de economie indirect getroffen zullen worden. Bovendien kunnen daders, doordat er koppelingen tussen de ICT-systemen van verschillende organisaties zijn, ook overspringen tussen organisaties. Een laatste maatschappelijk effect is een mogelijk afname van vertrouwen in de democratische rechtstaat doordat criminelen niet (kunnen) worden vervolgd.

Opzet van ransomware-aanvallen

De tweede onderzoeksvraag luidt: *Hoe zien ransomware-aanvallen er tegenwoordig uit en welke instrumenten worden hierbij ingezet?*

Een ransomware-aanval bestaat uit verschillende stappen waarin per stap van verschillende instrumenten gebruik gemaakt wordt.

1. **Initial access**. De aanvaller krijgt een eerste toegang ('foothold') bij het slachtoffer, vaak een account van een medewerker van een organisatie binnen een specifieke applicatie of op een specifieke server. Hiertoe wordt gebruik gemaakt van instrumenten die automatisch scannen op zwakheden in systemen. Ook wordt er veel gebruik gemaakt van (spear)phishing.
2. **Consolidatie toegang en positie**. Wanneer de aanvaller eenmaal een ingang heeft, zal deze proberen de toegang tot de systemen van het slachtoffer uit te breiden. Zo zal de aanvaller zoeken naar systemen met waardevolle informatie en toegang tot accounts proberen te verkrijgen met meer rechten op deze systemen. Deze stap vraagt relatief veel (niet-geautomatiseerd) handwerk en er wordt gebruik gemaakt van verschillende tools en software.
3. **Data-exfiltratie**. Bij sommige ransomware-aanvallen worden gegevens van het slachtoffer gestolen, waarna de aanvaller de dreiging van doorverkoop of publicatie van de data gebruikt als chantagemiddel. Bij exfiltratie wordt niet alleen gekeken naar bestanden die zich op de eigen server van een organisatie bevinden, maar, maar vaak gebruik gemaakt van clouddiensten (zoals Dropbox en OneDrive), webgebaseerde diensten (zoals Mega en WeTransfer) en zelfs van systemen die door het slachtoffer ingezet worden voor het maken van eigen back-ups.
4. **Ransomware deployment**. De eerste twee stappen waren generieke stappen die in veel verschillende cyberaanvallen gebruikt worden. Bij deze stap maakt de aanvaller de keuze om ransomware in te zetten om zo hun positie in systemen van slachtoffers snel te gelde te maken. De ransomware-software voert de daadwerkelijke 'gijzeling' van bestanden uit. Doel van deze stap is om een grote hoeveelheid (liefst waardevolle)

bestanden van een organisatie te versleutelen met een sleutel waarover alleen de aanvaller beschikt.

5. **Chantage en cash out.** In deze fase communiceert de aanvaller met het slachtoffer en maakt deze kenbaar wat het slachtoffer moet doen om de aanval te stoppen en de gegevens terug te krijgen of publicatie tegen te gaan.

Een ransomware-aanval kan zowel gericht als ongericht zijn. Bij een ongerichte aanval maakt het de aanvaller niet uit welke organisatie of persoon het slachtoffer wordt. Bij een gerichte aanval heeft een aanvaller a priori een specifieke organisatie in het vizier. Tegenwoordig is voornamelijk sprake van 'semi-gerichte' aanvallen op organisaties. Na de eerste stap (*initial access*) wordt bepaald welke toegangsgegevens interessant genoeg zijn om de volgende stap mee in te gaan. Dit proces herhaalt zich in de daaropvolgende stappen.

Betrokken actoren bij ransomware-aanvallen

De derde onderzoeksvraag is als volgt: *Welke soorten partijen zijn bij deze aanvallen betrokken?*

De eerste ransomware-aanvallen werden gepleegd door individuele criminelen, maar inmiddels is er sprake van een uitstekend functionerende supply chain van verschillende soorten actoren met een hoge mate van specialisatie. Het ransomware-ecosysteem opereert bijna alsof het een legitieme, goed ontwikkelde dienstensector is. Initiële toegang tot netwerken wordt bijvoorbeeld vaak via platformen verkocht aan de hoogste bieder. Er zijn verschillende soorten partijen die op verschillende manieren deze toegang proberen te verwerven. De kopers van de initiële toegang werken dit op hun beurt uit, consolideren deze positie en verkopen deze positie wederom aan de hoogste bieder. De daadwerkelijke ransomware-aanval komt pas in de fase erna. De partijen die ransomware-software ontwikkelen en beheren zijn niet altijd de partijen die deze software ook daadwerkelijk gebruiken. Vaak worden er affiliates ingezet die de aanval uitvoeren. Er zijn daarnaast datamanagers die gestolen data analyseren, verkopen en/of openbaar maken. In de laatste stap (chantage en cash out) zijn een breed scala aan partijen betrokken: onderhandelaars, helpdesks, witwassers, et cetera.

Verreweg het meest voorkomende motief voor ransomware-aanvallen is financieel gewin. Activisme komt slechts sporadisch voor. Ransomware-criminelen gedragen zich deels als rationele actoren: de kosten, opbrengsten en pakkans worden geregeld zorgvuldig afgewogen. Daders lijken relatief vaak uit landen te komen die voorheen deel uitmaakten van de Sovjet-Unie. In sommige gevallen vallen daders bepaalde soorten organisaties bewust niet aan. Voorbeelden zijn organisaties uit landen in de voormalige Sovjet-Unie en de zorgsector gedurende de Coronacrisis.

Risicofactoren voor ransomware-aanvallen

De vierde en vijfde onderzoeksvraag zijn: *Welke interne en externe factoren dragen bij aan ransomware-risico's voor een organisatie? In hoeverre zijn deze factoren kwantificeerbaar?*

Bij interne factoren gaat het over aspecten waar het mogelijke slachtoffer zelf controle over heeft. Voor het onderzoeken van de interne factoren is gekeken naar literatuur, (cyber)risicotaxatietools en cybersecurityverzekeringen. Door te tellen hoe vaak factoren in deze verschillende bronnen voorkomen is gekwantificeerd hoe groot deze risicofactor is. De onderstaande tabel toont de tien interne factoren die het vaakst in deze drie bronnen benoemd worden, gerangschikt naar omvang van de risicofactor. Een generieke interne risicofactor die de onderstaande factoren overkoepelt is het niet goed in kaart hebben welke systemen gebruikt worden. De uitkomsten zijn geverifieerd met interviews.

1. Geen goede back-up | fase: herstellen
2. Onvoldoende training medewerkers over phishing, scams, etc. | fase: voorkomen
3. Software is niet up-to-date | fase: voorkomen
4. Niet hebben van een *incident response plan* | fase: herstellen
5. Onvoldoende gebruik van (up-to-date) anti malware oplossingen| fase: voorkomen
6. Onvoldoende *privileged access strategy* | fase: beperken
7. Onvoldoende beveiligde accounts | fase: voorkomen
8. Onvoldoende continue monitoring | fase: beperken
9. Onvoldoende netwerksegmentatie | fase: beperken
10. Onvoldoende e-mailsecurity | fase: voorkomen

Naast de bovenstaande lijst is er een flinke serie met andere factoren die minder vaak benoemd worden. Dit zijn veelal technische maatregelen om te voorkomen dat infecties plaats kunnen vinden.

Bij externe factoren gaat het om de eigenschappen waar het mogelijke slachtoffer geen of beperkt controle over heeft. In lijn met de verschillende soorten impact die aanvallen op organisaties hebben komt hier naar voren dat de volgende aspecten de verwachte opbrengst voor daders (en hiermee het risico voor slachtoffers) verhogen (1) het hebben van een hogere omzet, (2) de inzet van IT-systemen waarvan uitval de bedrijfscontinuïteit kan verstoren en (3) de opslag van persoonsgegevens. Het hebben van een geschiedenis in het betalen van losgeld kan het risico voor organisaties mogelijk ook verhogen, al verschillen de meningen van experts op dit onderwerp. De volgende twee aspecten verlagen de kosten voor de dader: de lage pakkans en het niet te veel op de radar komen.

Beleidsopties om risico's te verkleinen

De zesde en zeven onderzoeksvragen luiden: *Met welk instrument kunnen bestuurders in middelgrote en kleine organisaties bewust worden gemaakt van de risico's van ransomware?* en *(Hoe) kunnen de vastgelegde factoren worden gebruikt in dit instrument?*

Uit onze analyse komt naar voren dat een bewustwordingscampagne voor bestuurders van kleine en middelgrote organisaties waarschijnlijk een doelmatig en doeltreffend instrument is om de kans op en de impact van ransomware-aanvallen te verminderen. Op dit moment worden zowel het risico als de impact van deze aanvallen onderschat door bestuurders van organisaties. De ICT'ers zijn zich veel beter bewust hiervan, maar blijkbaar wordt dit onvoldoende overgebracht op de bestuurders van deze organisaties. Omdat grote organisaties hun zaken op dit gebied vaak beter op orde hebben (en omdat ze vaak in een heel specifieke context opereren) is het logisch om de focus op middelgrote en kleine organisaties te leggen. Een goede campagne zou de volgende elementen moeten bevatten:

- De campagne moet confronterende feiten bevatten, zoals de gemiddelde schade die slachtoffers ervaren.
- Bestuurders moeten worden geprikkeld om stil te staan bij hun eigen situatie. Dat kan door ze te vragen wat het effect op hun organisatie is als (1) alle gegevens openbaar worden of (2) ICT drie weken niet gebruikt kan worden of (3) losgeld betaald moet worden ter grootte van bijvoorbeeld 5 procent van de omzet.
- De campagne moet concrete handelingsperspectieven bevatten door duidelijk te maken hoe en wat een organisatie minstens op orde moet hebben om goed beschermd te zijn tegen ransomware-aanvallen . De interne risicofactoren sluiten hier goed bij aan.
- De inhoud van de campagne moet actief onder de aandacht gebracht worden en bestuurders moeten een persoonlijk gerichte boodschap ontvangen. Hiervoor zijn verschillende kanalen mogelijk, maar het lijkt zinnig om aan te sluiten bij bekende relaties van de bestuurder zodat er een betrouwbare en bekende bron wordt gehanteerd.

- Door de hoge mate van heterogeniteit van deze doelgroep lijkt een sectorale aanpak voor de hand te liggen. In combinatie met het vorige punt zouden branche- en sectororganisaties een belangrijke rol kunnen spelen.
- Tot slot kan het presenteren van een sociale norm een krachtig instrument zijn. Bestuurders moeten het gevoel krijgen dat vergelijkbare organisaties ook stappen nemen om zich te beschermen tegen ransomware.

Er zijn uiteraard ook andere mogelijkheden om gedragsverandering en bewustwording te bereiken. Zo zou een bepaald niveau van cybersecurity kunnen worden afgedwongen door klanten, leveranciers, verzekeraars of zelfs de overheid. Dit kan gelden voor zowel ICT-dienstverleners als reguliere organisaties.

1 Introductie

In opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (hierna: WODC) heeft Dialogic een verkennend onderzoek naar risicofactoren voor ransomware-aanvallen uitgevoerd. Dit onderzoek heeft als doel het in kaart brengen en kwantificeren van factoren die ransomware-aanvallen beïnvloeden. Een tweede doelstelling is het bieden van inzicht in de mogelijkheden tot bewustwording onder bestuurders van middelgrote en kleine organisaties, zowel in de publieke als private sector. Het onderzoek beantwoordt de volgende onderzoeksvragen:

1. Welke risico's brengen ransomware-aanvallen met zich mee?
2. Hoe zien ransomware-aanvallen er tegenwoordig uit en welke instrumenten worden hierbij ingezet?
3. Welke soorten partijen zijn bij deze aanvallen betrokken?
4. Welke interne en externe factoren dragen bij aan ransomware-risico's voor een organisatie?
5. In hoeverre zijn deze factoren kwantificeerbaar?
6. Met welk instrument kunnen beleidsmakers in middelgrote en kleine organisaties bewust worden gemaakt maken van de risico's van ransomware?
7. Wat zijn belangrijke factoren voor bedrijven en organisaties om met het instrument aan de slag te gaan?

Voor de uitvoering van dit onderzoek is gebruik gemaakt van verschillende methoden: literatuuronderzoek, verkenning van bestaande risicotaxatiemodellen, verkenning van cybersecurityverzekeringen, interviews, casestudies van getroffen organisaties in Nederland en validatiesessies. In dit onderzoek wordt getracht de meest actuele situatie te schetsen van de vraagstukken die hier spelen.

1.1 Inleiding

In opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (hierna: WODC) heeft Dialogic Innovatie en Interactie (hierna: Dialogic) een verkennend onderzoek naar risicofactoren voor ransomware-aanvallen uitgevoerd. In dit hoofdstuk wordt de aanleiding van het onderzoek besproken (paragraaf 2). Daarna wordt de doelstelling (paragraaf 3) en de onderzoeksvragen (paragraaf 4) en de aanpak van het onderzoek op hoofdlijnen (paragraaf 5) behandeld. Tot slot bevat dit hoofdstuk een leeswijzer.

1.2 Aanleiding onderzoek

Er is een trend gaande waarin steeds meer organisaties slachtoffer worden van gerichte ransomware-aanvallen . Wereldwijd is er in 2020 minimaal $18 miljard aan losgeld betaald, waarbij het merendeel voor rekening is gekomen van private en publieke organisaties. [1] Tot voor kort vonden ransomware-aanvallen vooral plaats op grote schaal, waarbij op ongerichte wijze gepoogd werd bij grote aantallen (particuliere) gebruikers toegang te verkrijgen tot het systeem. Het verdienmodel van deze strategie was gebaseerd op schaalvoordeel, met doorgaans een laag losgeldbedrag. [2] Een klein bedrag van veel

instellingen lijdt nog steeds tot hoge opbrengsten. De laatste jaren zijn organisaties die een hoog losgeldbedrag kunnen betalen echter steeds vaker slachtoffer. Nederlandse voorbeelden zijn onder andere de aanval op de Universiteit Maastricht in december 2019, en wetenschapsfinancier NWO in februari 2021. In dit laatste geval was er sprake van een triple extortion aanval. De hoeveelheid ransomware-aanvallen neemt al jaren toe, maar nam een vlucht gedurende de Coronacrisis. [3] Het type cyberaanval waar organisaties de meeste zorgen over hebben is dan ook ransomware. [4]

Het Cybersecuritybeeld 2021 van de Nationaal Coördinator Terrorismebestrijding en Veiligheid geeft aan hoe het transnationale karakter van cybercriminaliteit de opsporing van daders en dienstverleners bemoeilijkt. [5] Bovendien treden buitenlandse overheden in wiens land veel van deze misdaad wordt geïnitieerd vaak niet op tegen deze vorm van criminaliteit. [6] In het Cybersecuritybeeld 2021 wordt dan ook gesteld dat het verhogen van de weerbaarheid om deze redenen van groot belang is. [5]

Om het risico op cyberaanvallen te verkleinen en de cyberweerbaarheid te verhogen, kunnen organisaties risicotaxaties (laten) uitvoeren. Hier bestaan al verschillende tools voor, zie bijvoorbeeld. [7] [8] [9] [10] [11] Vanwege de continue ontwikkelingen rondom ransomware-aanvallen en de ernstige gevolgen van dien heeft het Nationaal Cybersecurity Centrum (NCSC) behoefte aan een onderzoek naar de specifieke risicofactoren die een rol spelen bij dergelijke aanvallen. Als achterliggend probleem wordt gezien dat het management van middelgrote- en kleine organisaties, zowel privaat als semipubliek, te weinig middelen vrijmaakt worden voor cybersecurity omdat zij het risico onderschatten. Vanuit de ICT-afdeling is vaak het besef dat er meer gedaan moet worden aan cybersecurity, maar het is voor hen lastig het management hiervan te overtuigen. Beleidsmakers moeten dus bewust worden gemaakt van de risico's die de organisatie loopt en de kosten van een ransomware-aanval. Er is een beeld dat vooral organisaties die steeds afhankelijker worden van ICT zich onvoldoende bewust zijn van de risico's. Daarbij gaat het niet alleen om risico's voor één specifieke organisatie, maar zijn er ook duidelijke ketenafhankelijkheden: Een storing bij één partij zorgt voor andere effecten in de keten.

1.3 Doelstelling onderzoek en onderzoeksvragen

Dit onderzoek heeft als doel **het in kaart brengen en kwantificeren van factoren die ransomware-aanvallen beïnvloeden**. Om welke factoren gaat het en zijn deze te kwantificeren? De oorspronkelijke doelstelling betrof ook de voorbereiding voor het ontwikkelen van een specifiek risicotaxatie-instrument voor ransomware, waaronder het vaststellen van de mate van kwantificeerbaarheid van de verschillende factoren. Het doel van een dergelijk instrument was het bieden van handvatten aan de doelgroep om interne kwetsbaarheden en bijbehorende maatregelen te concretiseren. In overleg met de begeleidingscommissie is deze doelstelling tijdens de uitvoering van het onderzoek aangepast. De reden hiervoor is tweeledig. Aan de ene kant bleken er al verschillende risicotaxatiemodellen te bestaan. De tweede reden is dat een dergelijk instrument niet noodzakelijkerwijs bijdraagt aan het vergroten van bewustwording van de risico's van ransomware.

Een tweede doelstelling is **het bieden van inzicht in de mogelijkheden tot bewustwording onder de doelgroep**. De doelgroep zijn bestuurders van middelgrote en kleine organisaties, zowel in de publieke als private sector. Zij moeten zich bewust zijn van de kans op een ransomware-aanval, de risicofactoren die deze kans vergroten en de gevolgen van een aanval. Daarnaast zouden zij ook inzicht in de risicofactoren moeten krijgen. Er zijn verschillende manieren om bewustzijn te creëren. Dit kan met een *tool*, maar

wellicht is een *factsheet*, *roadshow* of app logischer. Het NCSC publiceert bijvoorbeeld geregeld kennisproducten op haar website. [12] [2]

Het onderzoek beantwoordt de volgende onderzoeksvragen:

1. Welke risico's brengen ransomware-aanvallen met zich mee?
2. Hoe zien ransomware-aanvallen er tegenwoordig uit en welke instrumenten worden hierbij ingezet?
3. Welke soorten partijen zijn bij deze aanvallen betrokken?
4. Welke interne en externe factoren dragen bij aan ransomware-risico's voor een organisatie?
5. In hoeverre zijn deze factoren kwantificeerbaar?
6. Met welk instrument kunnen bestuurders in middelgrote en kleine organisaties bewust worden gemaakt van de risico's van ransomware?
7. (Hoe) kunnen de vastgelegde factoren worden gebruikt in dit instrument?

De eerste vijf onderzoekvragen hebben betrekking op de eerste doelstelling. De laatste twee vragen gaan over de tweede doelstelling.

1.4 Onderzoeksaanpak

Voor de uitvoering van dit onderzoek is gebruik gemaakt van verschillende methoden:

- **Literatuuronderzoek**: Er is veel literatuur over cybersecurity risico's in het algemeen en specifiek voor ransomware. Hierin is systematisch gezocht naar risicofactoren en (het verloop van) diverse ransomware-aanvallen . Op het eind van dit document is onder de kop *Verwijzingen* een overzicht van de literatuur te vinden. Er is overigens relatief weinig wetenschappelijke, actuele, p*eer reviewed* literatuur beschikbaar over dit onderwerp. Dat betekent er ook veel bronnen zijn gebruikt die geschreven zijn door marktpartijen die mogelijk een belang hebben bij bepaalde uitkomsten. Daarnaast zal een deel van de *grijze literatuur* gebaseerd zijn op minder grondig onderzoek dan bij wetenschappelijke literatuur typische het geval is.
  Voor het theoretisch kader in hoofdstuk 6, waarbij we ingaan op de wetenschap achter bewustwordingscampagnes, is wel een (hoofdzakelijk) wetenschappelijke literatuurstudie ingezet. Hierbij ligt de focus op de vakgebieden risicopsychologie en risicocommunicatie.
- Verkenning van bestaande **risicotaxatiemodellen**: Bestaande risicotaxatie-instrumenten zijn bekeken om zo de meest voorkomende onderdelen/factoren te identificeren.
- Verkenning **cybersecurityverzekeringen**: Verzekeraars bieden in toenemende mate verzekeringen aan die zich specifiek richten op cyberaanvallen. Hun verzekeringen zijn het resultaat van uitvoerige analyse en kwantificering van risico's. De in de verzekeringen geïdentificeerde risicofactoren zijn vergeleken met de resultaten uit het literatuuronderzoek en de bestaande risicotaxatiemodellen.
- **Interviews**: Er zijn 34 personen geïnterviewd die afkomstig waren uit verschillende groepen respondenten (onderzoekers/experts, politie, OM, ministeries, getroffen organisaties, incident response bedrijven, verzekeraars, security audit bedrijven). In Bijlage 1 is hiervan een overzicht opgenomen.
- **Casestudies** getroffen organisaties in Nederland richten zich op private en publiek organisaties waarvan bekend is dat ze zijn getroffen door een ransomware-aanval. Er is een brede inventarisatie van recente cases uitgevoerd, waarbij de focus lag op Nederlandse organisaties. Met enkele slachtoffers is

aanvullend een interview gehouden (zie Bijlage 1). De input van de case studies is gebruikt om de antwoorden op onderzoeksvragen te illustreren.

- **Validatiesessies** om de uitkomsten van het onderzoek te toetsen. In dit kader zijn twaalf personen gesproken, zie Bijlage 2. Er zijn drie lijnen gevolgd:
  - Vanuit CyberVeiligNederland zijn drie organisaties aangedragen die veel kennis en kunde hebben in dit dossier. De gesprekken hadden een breed perspectief waarbij alle aspecten van dit onderzoek aan bod kwamen. In deze gesprekken is daarnaast bijzondere aandacht geweest voor beleidsopties.
  - DTC heeft een oproep gedaan binnen hun community om deel te nemen aan dit onderzoek. Dit heeft geleid tot interviews met zeven organisaties. In deze gesprekken lag de focus primair op beleidsopties.
  - Bij de ONE conference is een voorstel gedaan om de uitkomsten te presenteren. Dit voorstel is geaccepteerd en de presentatie zal naar verwachting op 18 oktober 2022 plaatsvinden. Gezien de tijdslijnen konden de onderzoekers deze uitkomsten niet meer meenemen in dit rapport.

In dit onderzoek wordt getracht de meest actuele situatie te schetsen van de vraagstukken die hier spelen. Omdat er sprake is van een zeer dynamisch veld, is dit zeer relevant. Het beeld van vijf jaar geleden is beperkt relevant voor de huidige situatie. Aan de andere kant moeten we ook erkennen dat de verzameling van data per definitie achter loopt bij de actualiteit.

1.5 Leeswijzer

Om een voor de lezer goed te volgen redeneerlijn, wordt een opzet gehanteerd waarbij in opeenvolgende hoofdstukken steeds diepgang wordt aangebracht. De volgorde van de hoofdstukken komt overeen met de volgorde van de onderzoeksvragen. Het rapport start met de impact van ransomware-aanvallen op organisaties (hoofdstuk 2). Deze impact komt voort uit een bepaalde opzet van aanvallen, die in hoofdstuk 3 behandeld worden. De soorten actoren die de aanvallen uitvoeren komen in hoofdstuk 4 aan bod. In hoofdstuk 5 worden de interne en externe factoren die bij dragen aan de risico's behandeld en worden deze teven gekwantificeerd. Hoofdstuk 6 gaat in op beleidsopties. In Bijlage 1 is een overzicht van de interviewrespondenten opgenomen.

Er hoofdstuk start met een grijsblauw blok waarin de conclusies van dit hoofdstuk zijn opgenomen. Zo kan de lezer efficiënt dit document doornemen.

2 Impact van ransomware-aanvallen

De eerste onderzoeksvraag luidt: *Welke risico's brengen ransomware-aanvallen met zich mee?*

Het risico op een cyberaanval is groot en groeiend. Ransomware is een specifieke cyberaanval. Hierbij richten criminelen zich meestal op het versleutelen van data van het slachtoffer en in mindere mate het voorkomen dat het slachtoffer toegang krijgt tot zijn eigen systemen. De kern van ransomware is dat het slachtoffer door de dader (typisch: vanwege de versleuteling van data) onder druk wordt gezet om iets tegen zijn of haar zin te doen. Meestal is dit het betalen van losgeld (ransom). Er zijn vier vormen van aanvallen. Bij single extortion worden bestanden versleuteld en worden slachtoffers gechanteerd door de dreiging toegang tot deze bestanden te verliezen. Bij double extortion worden naast versleuteling de gegevens gestolen en wordt gedreigd deze openbaar te maken. Bij triple extortion worden bovendien andere cyberaanvallen, zoals DDoS-aanvallen, op systemen van het slachtoffer uitgevoerd om het herstelproces complexer te maken. Tenslotte worden bij quadruple extortion ook de relaties van het slachtoffer gechanteerd met het openbaar maken van hun gegevens.

De impact die dergelijke aanvallen kunnen hebben op organisaties bestaat uit de volgende aspecten:

1. Additionele kosten voor de inhuur van capaciteit om op de aanval te reageren;
2. Kosten door verlies van data;
3. Kosten door openbaarmaking van data die bestaan uit (a) kosten door reputatieschade, (b) boetes, bijvoorbeeld als gevolg van de AVG en (c) schadevergoedingen;
4. Betaling van losgeld;
5. Kosten door verstoring bedrijfscontinuïteit;
6. Herstelkosten voor systemen.

De gemiddelde losgeldbetaling is lastig exact te bepalen, maar ligt waarschijnlijk tussen de $50.000 en $500.000. Het inschatten van de kosten van de verstoring van de continuïteit van ondernemingen is nog lastiger, maar lijkt een vaak veelvoud te zijn van de losgeldbetalingen. Van de andere posten is het lastig om dit kwantitatief te duiden en verschillen ook sterk per casus.

Tot slot zijn er ook maatschappelijke effecten van ransomware-aanvallen . Door ketenafhankelijkheden kan de verstoring van de bedrijfscontinuïteit van één aangevallen organisatie een grote impact hebben op andere organisaties in de keten, zoals klanten en leveranciers. De overtreffende trap hiervan zijn uiteraard aanvallen op vitale sectoren waardoor grote delen van de economie indirect getroffen zullen worden. Bovendien kunnen daders, doordat er koppelingen tussen de ICT-systemen van verschillende organisaties zijn, ook overspringen tussen organisaties. Een laatste maatschappelijk effect is een mogelijk afname van vertrouwen in de democratische rechtstaat doordat criminelen niet (kunnen) worden vervolgd.

2.1 Inleiding

In dit hoofdstuk draait het om de economische impact die ransomware-aanvallen kunnen hebben op individuele organisaties, maar ook op de impact op de maatschappij. Het hoofdstuk start in de volgende paragraaf met verschillende vormen van ransomware-

aanvallen . In paragraaf 2.3 wordt ingegaan op de impact voor individuele organisaties. Tot slot komt in 2.4 de maatschappelijke impact van dergelijke aanvallen naar voren.

2.2 Vormen van ransomware-aanvallen

Het risico op een cyberaanval is groot en groeiend. Onderzoek van ABN AMRO ziet in de periode 2021-2022 een stijging van 29% naar 45% van de bedrijven die te maken hebben gehad met cybercriminaliteit vergeleken. [13] De Nederlandse politie registreerde vorig jaar 14.000 gevallen van cybercriminaliteit, een toename van bijna een derde in vergelijking met 2020 en een verdriedubbeling ten opzichte van 2019. [14] En ook Europees agentschap ENISA spreekt van een toename in cyberaanvallen gedurende de afgelopen twee jaar. [15] Interviewrespondenten zien met name een stijging van ransomware-aanvallen .

Ransomware is een aanval op basis van een specifieke vorm van *malware* (malafide software). Waar reguliere malware gericht is op het verstoren, beschadigen of het ongeoorloofd toegang verkrijgen tot een computersysteem richt ransomware zich op het *versleutelen* van informatie op een computersysteem. De kern van ransomware is dat het slachtoffer door de dader vanwege de versleuteling van data onder druk wordt gezet om iets tegen zijn zin te doen, typisch het betalen van losgeld (*ransom*). Nadat de bestanden zijn versleuteld wordt het slachtoffer medegedeeld dat de bestanden ontsleuteld kunnen worden na het betalen van een losgeldsom, vaak in de vorm van bitcoins of andere (slecht tot de ontvanger traceerbare) cryptomunten. Een ransomware-dader kan op verschillende manieren druk uitoefenen op het slachtoffer om over te gaan op betaling. Er zijn vier varianten van een ransomware-aanval, die oplopen in complexiteit. [16] [17]

1. **Single extortion**: Bestanden worden versleuteld. De dader chanteert het slachtoffer door aan te geven dat deze geen toegang kan krijgen tot deze bestanden zolang het losgeld niet betaald wordt.
2. **Double extortion**: Bestanden worden niet alleen versleuteld maar ook gestolen. De dader gijzelt niet alleen de data, er wordt ook gedreigd met het openbaren ervan.
3. **Triple extortion**: Er wordt data versleuteld, gestolen, en daarnaast worden ook aanvallen uitgevoerd om het herstelproces te belemmeren. Hiervoor kunnen bijvoorbeeld Distributed Denial of Service (DDoS) aanvallen worden ingezet. Dit heeft als doel om het slachtoffer te verstoren bij het terugrollen van eventuele back-ups, zodat de schade wordt vergroot (en de druk om losgeld te betalen hoger wordt).
4. **Quadruple extortion**: Bovenstaande, plus de dader benadert *klanten* (of andere relaties) van het slachtoffer (of dreigt hiermee) om zo druk uit te oefenen. Er wordt bijvoorbeeld naar kanten gemaild dat de organisatie getroffen is door ransomware en niet wil betalen, met het risico dat de klantgegevens worden openbaard.

In de interviews met experts is besproken in welke mate de bovenstaande vier varianten op dit moment voorkomen. Hieruit komt een beeld naar voren dat eerste variant (single extortion) in het verleden veel voorkwam, maar de laatste jaren steeds minder vaak gebruikt wordt. Doordat steeds meer organisaties hun back-ups op orde hebben, kunnen cybercriminelen minder eenvoudig druk uitoefenen via *single extortion*. De tweede variant (*double extortion*) lijkt op dit moment het dominante model. Zo kan er veel druk op slachtoffers worden uitgeoefend, maar blijven de inspanningen voor criminelen vrij beperkt. De derde en vierde variant (*triple extortion* en *quadruple extortion*) komen minder vaak voor en worden vooral ingezet bij grote organisaties en hoge bedragen. Beide opties vergen immers dat de aanvallers zich moeten verdiepen in de ICT-systemen van het slachtoffer (*triple extortion)* of de organisatieprocessen van het slachtoffer (*quadruple extortion)*. Ook uit literatuur komt naar voren dat het ontvreemden van data veel voorkomt. Eén onderzoek

geeft aan dat hier op dit moment is sprake van is bij meer dan 80% van de aanvallen [18], een ander onderzoek komt uit op ruim 50%. [19]

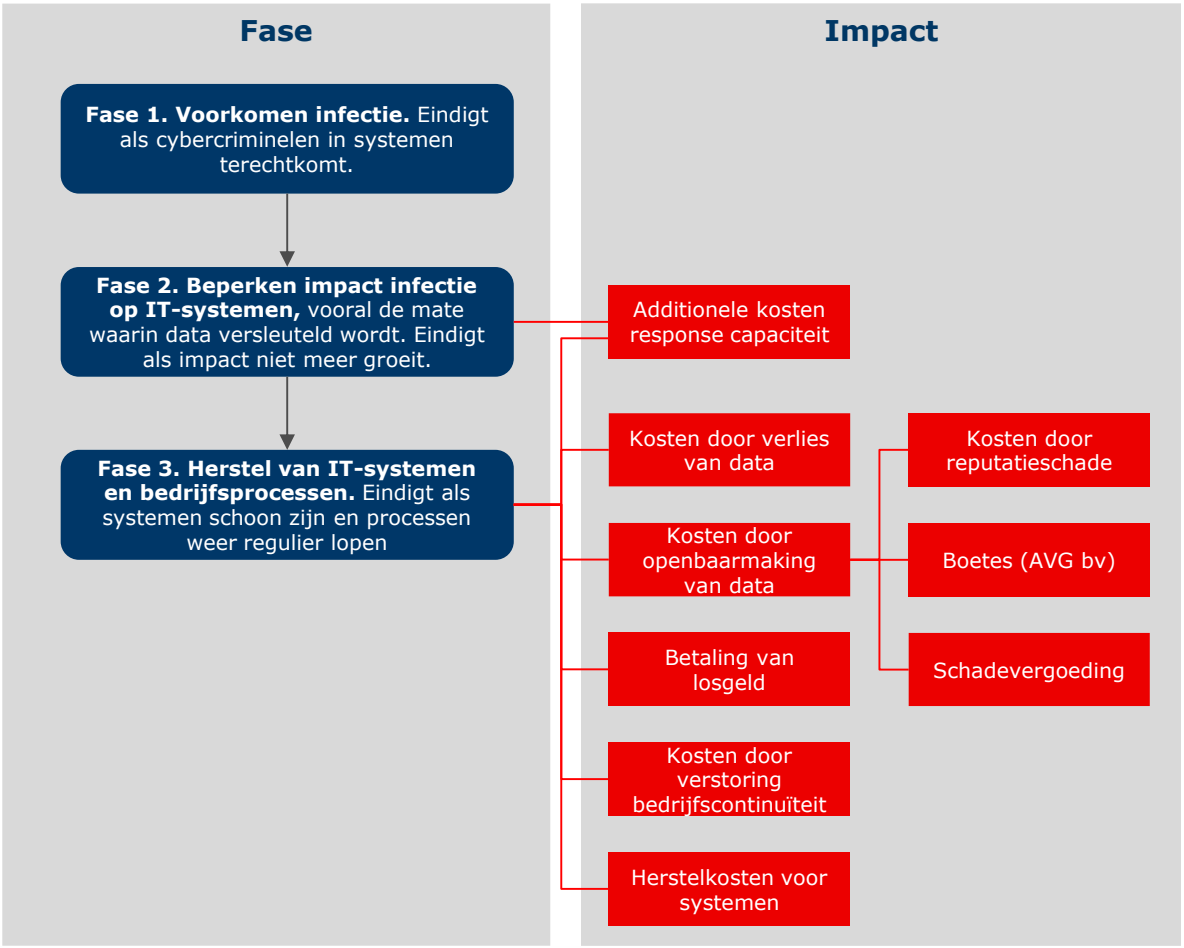
In dit rapport staat ransomware centraal die data gijzelt, de zogenaamde *cryptors*. [2] Sommige vormen van ransomware gijzelen echter volledige systemen: *lockers*. [2] Het gijzelen van data is echter op dit moment de dominante variant. [20] Daarom zal dit rapport het vooral het gijzelen van data centraal stellen. Voor de discussie maakt het overigens in veel gevallen weinig uit welke vorm gebruikt wordt.[1]

2.3 Impact op individuele organisaties

De impact van ransomware-aanvallen op individuele organisaties begint als een dergelijke aanval succesvol is. In de fase hiervoor heeft een organisatie zich in meer of mindere wijze ingespannen om een aanval te voorkomen. Om basis van een analyse van de literatuur en interviews komen de auteurs van dit rapport tot een model met drie fases: In de eerste fase ligt de focus op het *voorkomen van infecties*. In de tweede fase ligt de focus op het *beperken van de impact* van de infectie. In fase drie komt het *herstel van systemen* aan bod. De verschillende soorten impact worden hierna uitgewerkt.

In de onderstaande tekst worden de verschillende vormen van impact besproken en wordt dit zo veel mogelijk gekwantificeerd. Kwantificeren is echter lastig omdat slachtoffers niet altijd deze gegevens delen. Bovendien zijn sommige aspecten (reputatieschade, kosten door verlies van data) lastig te bepalen om het geen out-of-pocket kosten zijn. Maar wat zeker speelt, zijn de verschillen tussen organisaties. Uit interviews met experts komt naar voren dat er grote verschillen zijn in de soort impact die verschillende soorten organisaties ervaren. Een producent van levensmiddelen kan zeer gevoelig zijn voor de verstoring van de bedrijfsprocessen (*elke dag dat we storing hebben maken we geen omzet*) en tegelijkertijd weinig schade ondervinden van het openbaar maken van data (*dan kunnen consumenten tenminste zien dat we netjes werken)*. Maar voor een psychologenpraktijk kan dit exact andersom zijn: De continuïteit staat nauwelijks onder druk (*gesprekken met cliënten doen we wel met een kladblok*), maar het openbaar maken van data is rampzalig (*als alle patiëntendossiers openbaar worden, dan kunnen we wel bijna ophouden met de praktijk)*.

[1] Het gijzelen van data van de gebruiker in plaats van het gijzelen van systemen is uiteraard veel logischer omdat data veel unieker is dan systemen. Neem als voorbeeld een systeem met Windows 11 en als data 1.000 persoonlijke foto's. Als ransomware alleen Windows gijzelt, dan is het waarschijnlijk mogelijk om de hard disk te verwijderen, op een andere systeem aan te sluiten en de 1000 foto's veilig te stellen. De originele hard disk kan geformatteerd worden en Windows 11 opnieuw worden geïnstalleerd. Het kost wat werk, maar het probleem kan worden opgelost. Als alleen de 1.000 foto's versleuteld zijn, dan is er vaak een veel groter probleem als de foto's (1) geen back-up hebben en (2) van waarde zijn voor de gebruiker. Er is geen andere manier om ze terug te halen dan te betalen.



Figuur 1. Vormen van impact van een ransomware-aanval op een organisatie

2.3.1 Additionele kosten inzet response capaciteit

Een evidente kostenpost voor organisaties in het geval van een infectie of herstel van systemen is de additionele inzet van response capaciteit. In sommige gevallen kan dit door de eigen organisatie worden gedaan, maar vaak zullen er ook externe experts worden betrokken. Deze worden vaak als *Computer Emergency Response Team* (CERT) of Computer *Security Incident Response Team* (CSIRT) aangeduid. Aangezien het hier gaat om experts die onder grote tijdsdruk in een krappe markt opereren, zijn de kosten voor de inzet van deze partijen relatief hoog.[2]

2.3.2 Kosten voor verlies van data

Verlies van data kan optreden op (1) het losgeld niet betaald wordt en er geen (perfecte) back-up kan worden teruggezet of (2) het losgeld wel betaald wordt maar er geen (volledige) decryptie van de data kan plaatsvinden. Daarnaast kan er ook nog data verloren gaan in de periode waarin de systemen niet volledig operationeel zijn worden. Data kan dan immers minder goed worden opgeslagen. Gemiddeld wordt deze kostenpost als grootste risico gezien door organisaties. [21]

[2] Zie bijvoorbeeld de overweging bij de Cyberaanval op de Universiteit Maastricht [176]

De kosten voor het verlies van data zijn de primaire hefboom voor de daders waarmee slachtoffers onder druk worden gezet. In veel gevallen beseffen slachtoffers pas bij een aanval hoe waardevol de data voor hen is. Bij steeds meer organisaties bestaat de primaire output uit data, denk aan rapporten, rekenmodellen, ontwerpen, films, foto's, online content, et cetera. Maar ook voor organisaties met een fysieke primaire output, is data essentieel in het productieproces. Er zullen weinig fabrieken in Nederland zijn die zonder toegang tot hun data (lang) kunnen doorwerken.

2.3.3 Kosten voor openbaarmaking van data

Aan het begin van het hoofdstuk is aangegeven dat bij *double, triple* en *quadruple extortion* er ook wordt gedreigd met het openbaar maken van data. In sommige gevallen wordt de data volledig openbaar gemaakt zodat iedereen deze data kan inzien. In andere gevallen wordt de data verkocht aan de hoogste bieder.[3] De kosten voor de openbaarmaking van data vallen uiteen in drie aspecten die hieronder nader worden uitgewerkt.

Box 1. Voorbeeld van kosten voor verlies van data

In februari 2021 werd game-ontwikkelaar CD Project Red getroffen door een ransomware aanval. De cybercriminelen wist toegang te krijgen tot IT systemen. De broncode voor verschillende games en documenten van de afdelingen Accounting, Personeelszaken, Financiën en Juridische zaken wisten ze te bemachtigen. Deze criminelen dreigden de gegevens te verkopen aan de hoogste bieder. CD Project Red weigerde te betalen en de gegeven schijnen voor $7 miljoen te zijn verkocht. [22] [23]

Kosten door reputatieschade

Het openbaar worden van informatie kan voor bedrijven een flinke impact hebben op hun reputatie. Yahoo was het slachtoffer van een van de grootste hacks ooit, overigens geen ransomware aanval, waarbij honderden miljoen accounts gecompromitteerd werden. [24] De reputatieschade voor Yahoo hiervan werd geschat op $1 miljard. [25] Hoewel het hier ging om een groot aantal accounts, was de data op zichzelf niet eens heel gevoelig. De impact van datalekken op een website als Ashley Madison, een online datingservice voor mensen die getrouwd zijn of een relatie hebben, zal relatief veel groter zijn geweest. [26] Dit leidt niet alleen tot een afbreuk van de reputatie van de klanten waarvan de gegevens openbaar gemaakt zijn, maar uiteraard ook het bedrijf zijn. Klanten zullen minder vertrouwen hebben dat hun anonimiteit gewaarborgd is. Dichter bij huis zijn de datalekken van de GGD, die overigens niet door ransomware veroorzaakt werken, relevant. Hier worden miljarden geëist van de GGD. [27]

Boetes

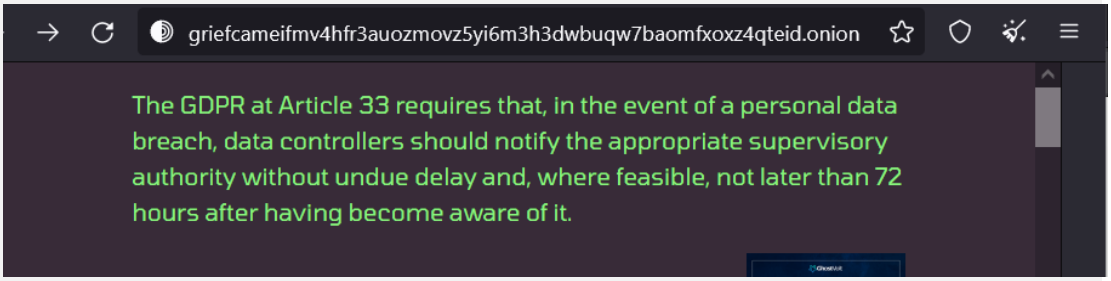
Bedrijven waarvan de data gestolen wordt, moeten hiervan een melding doen bij de autoriteiten. [28] Onder de AVG kan het openbaar worden van data bestraft worden met boetes. Criminelen gebruiken zelfs deze dreiging om extra druk te zetten op slachtoffers. [29] Daarnaast zijn er ook boetes mogelijk als die voort kunnen komen uit de verschillende meldplichten, zoals die voor datalekken en cyberincidenten voor essentiële organisaties.

Box 2. Voorbeeld van kosten door boetes

De ransomware groep 'Grief' probeert actief slachtoffers over te halen om over te gaan tot losgeld betaling door te dreigen met GDPR-boetes. 'Grief' hanteert double extortion:

[3] Zie bijvoorbeeld: [171]

Bestanden worden niet alleen versleuteld maar ook gestolen. De dader gijzelt niet alleen de data, er wordt ook gedreigd met het openbaren ervan. Wanneer slachtoffers de TOR-website van *Grief* bezoeken worden ze direct geconfronteerd met een disclaimer over de GDPR. Verder vermeldt Grief dat de losgeldeis vaak velen malen lager ligt dan de potentiële boetes die voorvloeien uit het openbaar maken van de data. [30]



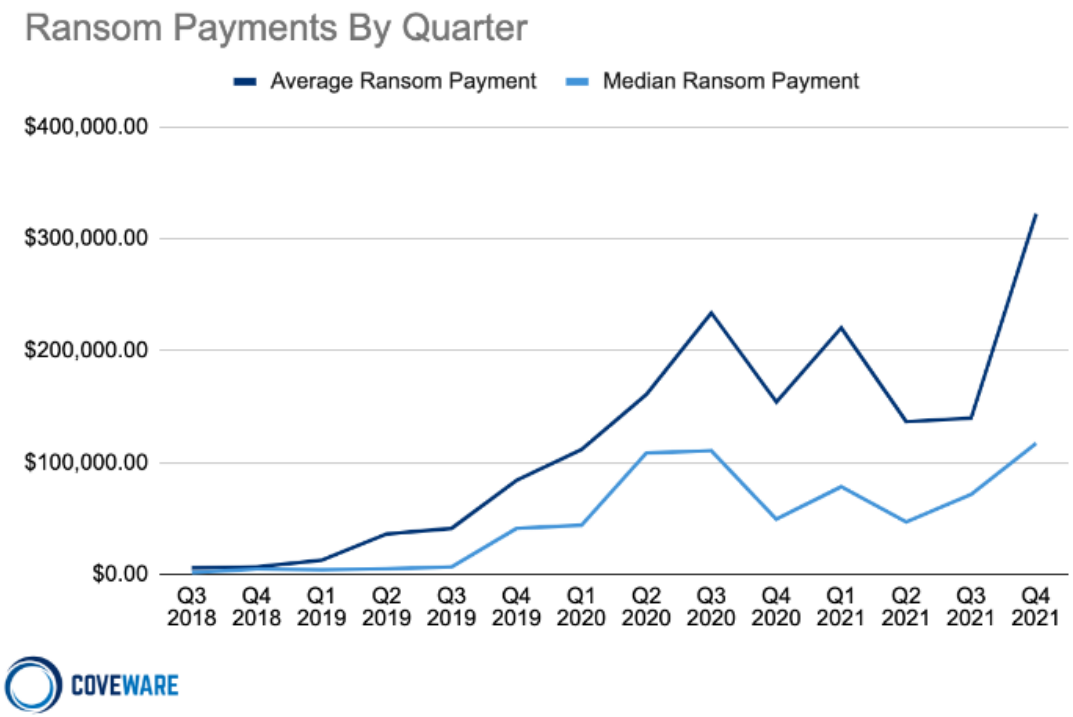
Figuur 2. Mededeling van Grief aan een slachtoffer

Schadevergoeding

Naast de bovenstaande twee aspecten kunnen de personen of organisaties waarvan de data gelekt is bij het ransomware-slachtoffer een schadevergoeding eisen. Als het gaat om de data van personen zal het vooral gaan om het lekken van persoonsgegevens. Wederom is Yahoo hier een goed voorbeeld, dat ruim $100 miljoen aan slachtoffers betaalde. [31] Als het gaat om de data van bedrijven dan zal het wellicht eerder gaan om een overtreding van bepalingen die in een *Non-Disclosure Agreement* (NDA) zijn vastgelegd.

2.3.4 Betaling van losgeld

Het betalen van losgeld is uiteraard een evidente kostenpost van ransomware-aanvallen . De gemiddelde omvang van de betalingen varieert over de tijd en leek lange tijd toe te nemen. [32] Recenter onderzoek toont een daling van de omvang van losgeldbetalingen. [33] [34]. Daarnaast lijken aanvallers zich goed bewust te zijn van wat een *redelijke prijs* is: het heeft geen zin om een aan Mkb'er 10 miljoen te vragen dat kan toch niet betaald worden. Grotere organisaties krijgen een hogere prijs voorgeschoteld die kan oplopen tot $10 miljoen. [32] De gemiddelde omvang van de een losgeldbetaling is echter lastig te bepalen, bronnen spreken over $54.000 [32], $41.000 [35], $145.000 [36], $21.000 [37], $170.000 [19], $175.000 [38], $312.000 [39] en $570.000 [40]. Een andere bron (zie Figuur 3. Betalingen aan losgeld over de tijd [18]) laat een sterk groeiende gemiddelde betaling zien. Het hoogst betaald losgeldbedrag is $40 miljoen. [41] Onderzoek wijst ook uit dat er een groot verschil is tussen het type ransomware dat gebruikt wordt en het losgeld dat vervolgens gevraagd wordt. [42] Ook in de interviews is deze vraag gesteld: de experts drukken de omvang van het losgeld uit in percentages van de jaaromzet. In hun ervaring is het losgeld 2% tot 5% van de jaaromzet van een organisatie.



Figuur 3. Betalingen aan losgeld over de tijd [18]

Box 3. Voorbeeld van kosten door boetes

De cybercriminelen hadden de Universiteit Maastricht in een onmogelijke positie gebracht. Er was geen sprake van het ophalen van data en de dreiging om het openbaar te maken, maar alles zat wel op slot net voor de tentamenperiode. Als de tentamenperiode niet door kon gaan, zou dat tot studievertraging leiden voor zo'n 13.000 studenten. Dat is een flinke bijkomende schade. Ook zou het herstel en weer up en running krijgen van de systemen weken tot maanden duren. Voorspelde schadebedragen liepen op tot in de miljoenen. Uiteindelijk heeft Universiteit Maastricht ervoor gekozen om een losgeldsom van €197.000 euro te betalen. [43]

2.3.5 Kosten door verstoring bedrijfscontinuïteit

Organisaties die getroffen worden door een ransomware-aanval zullen in veel gevallen een verstoring van hun bedrijfsprocessen ervaren. Het niet bij de data kunnen zorgt voor een verstoring van het primaire productieproces. Ruim 60% van de bedrijven die een ransomware-aanval hebben ondergaan, ervaren het verlies van productiviteit. [44] VDL had eind 2021 te maken met een aanval waarbij de productie een week plat kwam te liggen. [45] VDL had toentertijd een jaaromzet van €4,5 miljard en dus een weekomzet van kleine €100 miljoen. [45] Uit een ander onderzoek komt naar voren dat de kosten voor downtime gemiddeld 50x hoger liggen dan de kosten voor het betalen van het losgeld. [44] Ander onderzoek presenteren een factor 2 [46] of een factor 3 tot 5 [38]. Er zijn zelfs voorbeelden van organisaties die volledig ophouden te bestaan na een grote aanval. [47]

2.3.6 Herstelkosten voor systemen

Een laatste kostenpost zijn de herstelkosten voor systemen. Zeker bij complexere ICT-systemen kan data niet zomaar worden teruggezet (of ontsleuteld) zonder dat dit een impact heeft op de systemen. Zo zullen sommige systemen opnieuw geconfigureerd moeten

worden. Het is evident dat dit leidt tot substantiële herstelkosten voor de systemen. Voor de aanval op de Universiteit Maastricht is goede in kaart gebracht hoeveel tijd en geld hiermee gemoeid gaan. [43]

2.4 Impact op de maatschappij

Naast de impact op individuele bedrijven, hebben ransomware-aanvallen ook een bredere maatschappelijke impact. De NCTV geeft aan dat de inzet van ransomware maatschappij-ontwrichtende gevolgen kan hebben. [48]

2.4.1 Ketenafhankelijkheden

Bijna alle bedrijven opereren in een keten. Een verstoring van de bedrijfscontinuïteit in bedrijf A, zal een impact hebben op hun klanten en toeleveranciers. Een bedrijf dat zich hier heel bewust van is, is ASML. Zij verplichten hun leveranciers om een bepaald niveau van cybersecurity te realiseren en ondersteunen hen hierbij. [49] Toch is het vaak ook lastig om vooraf duidelijk te hebben waar kwetsbaarheden liggen. Albert Heijn had op een gegeven moment bijvoorbeeld geen kaas meer in de schappen vanwege een hack bij een logistiek bedrijf dat kaas vervoerde. [50]

2.4.2 Vitale sectoren

Ransomware-aanvallen op vitale sectoren zijn de overtreffende trap van ketenafhankelijkheden. In dit geval worden niet alleen leveranciers en klanten getroffen, maar hebben grote delen van de maatschappij last van een dergelijke aanval. Wellicht het beste voorbeeld hiervan is de *Colonial Pipeline* ransomware-aanval uit 2021. [51] Hierdoor werd de distributie van brandstof in het zuidwesten van de VS verstoord. Dichter bij huis heeft de aanval op een bedrijf in de Rotterdamse haven de werkzaamheden in de gehele haven tijdelijk stilgelegd met grote gevolgen van dien. [52] Recent heeft de FBI bekend gemaakt dat zeker drie vitale organisaties in de VS door een ransomware-infectie hebben ervaren. [53]

Box 4. Voorbeeld van aanval op vitale sectoren

Colonial Pipeline werd in mei 2021 slachtoffer van een ransomware-aanval. Tientallen miljoenen Amerikaanse huishoudens en ondernemingen zijn afhankelijk van de aanvoer van aardolie van het bedrijf. Werknemers van *Colonial Pipeline* konden niet inloggen en geen bestanden openen. De criminelen wisten 100GB aan bedrijfsgevoelige en vertrouwelijk informatie te stelen. Vanwege het landelijk belang heeft het bedrijf de criminelen $4,4 miljoen losgeld betaald. [54]

2.4.3 Steppingstone

Een derde manier waarop er een bredere maatschappelijk impact kan zijn, is als een aanvaller gebruik maakt van koppelingen van ICT-infrastructuur tussen bedrijven in de keten.[4] Er kan bijvoorbeeld sprake zijn van een VPN-koppeling tussen systemen die een aanzienlijk risico met zich meebrengt. [55] Hierdoor kan een aanvaller via een relatief slecht beveiligd bedrijf toch toegang krijgen tot de systemen van een bedrijf dat beter beveiligd lijkt te zijn. [56]

[4] Voor meer informatie, zie bijvoorbeeld [174]

2.4.4 Afbreuk van maatschappelijk vertrouwen

Een belangrijk element van digitale weerbaarheid is het vertrouwen dat de specialisten binnen de publieke en private sector in staat zijn de maatschappij tegen externe aanvallen te beschermen. [57] Als dit vertrouwen laag is en daders worden niet opgespoord, veroordeeld en hun criminele winsten worden afgepakt, dan is de schade niet alleen economisch van aard. Er ontstaat ook een afname van het vertrouwen in de democratische rechtsstaat als geheel. Sommige auteurs geven aan dit een belangrijke drijfveer is voor het rol van de Russische overheid in dit ecosysteem. [58] [59]

3 Opzet van ransomware-aanvallen

De tweede onderzoeksvraag luidt: *Hoe zien ransomware-aanvallen er tegenwoordig uit en welke instrumenten worden hierbij ingezet?*

Een ransomware-aanval bestaat uit verschillende stappen waarin per stap van verschillende instrumenten gebruik gemaakt wordt.

1. **Initial access.** De aanvaller krijgt een eerste toegang (‘*foothold*’) bij het slachtoffer, vaak een account van een medewerker van een organisatie binnen een specifieke applicatie of op een specifieke server. Hiertoe wordt gebruik gemaakt van instrumenten die automatisch scannen op zwakheden in systemen. Ook wordt er veel gebruik gemaakt van *(spear)phishing.*
2. **Consolidatie toegang en positie.** Wanneer de aanvaller eenmaal een ingang heeft, zal deze proberen de toegang tot de systemen van het slachtoffer uit te breiden. Zo zal de aanvaller zoeken naar systemen met waardevolle informatie en toegang tot accounts proberen te verkrijgen met meer rechten op deze systemen. Deze stap vraagt relatief veel (niet-geautomatiseerd) handwerk en er wordt gebruik gemaakt van verschillende tools en software.
3. **Data-exfiltratie**. Bij sommige ransomware-aanvallen worden gegevens van het slachtoffer gestolen, waarna de aanvaller de dreiging van doorverkoop of publicatie van de data gebruikt als chantagemiddel. Bij exfiltratie wordt niet alleen gekeken naar bestanden die zich op de eigen server van een organisatie bevinden, maar vaak gebruik gemaakt van clouddiensten (zoals Dropbox en OneDrive), webgebaseerde diensten (zoals Mega en WeTransfer) en zelfs van systemen die door het slachtoffer ingezet worden voor het maken van eigen back-ups.
4. **Ransomware deployment.** De eerste twee stappen waren generieke stappen die in veel verschillende cyberaanvallen gebruikt worden. Bij deze stap maakt de aanvaller de keuze om ransomware in te zetten om zo hun positie in systemen van slachtoffers snel te gelde te maken. De ransomware-software voert de daadwerkelijke ‘gijzeling’ van bestanden uit. Doel van deze stap is om een grote hoeveelheid (liefst waardevolle) bestanden van een organisatie te versleutelen met een sleutel waarover alleen de aanvaller beschikt.
5. **Chantage en cash out.** In deze fase communiceert de aanvaller met het slachtoffer en maakt deze kenbaar wat het slachtoffer moet doen om de aanval te stoppen en de gegevens terug te krijgen of publicatie tegen te gaan.

Een ransomware-aanval kan zowel gericht als ongericht zijn. Bij een ongerichte aanval maakt het de aanvaller niet uit welke organisatie of persoon het slachtoffer wordt. Bij een gerichte aanval heeft een aanvaller a priori een specifieke organisatie in het vizier. Tegenwoordig is voornamelijk sprake van ‘semi-gerichte’ aanvallen op organisaties. Na de eerste stap (*initial access*) wordt bepaald welke toegangsgegevens interessant genoeg zijn om de volgende stap mee in te gaan. Dit proces herhaalt zich in de daaropvolgende stappen.

3.1 Inleiding

In dit hoofdstuk wordt ingegaan op de opzet van ransomware-aanvallen . Hierbij wordt tweede onderzoeksvraag beantwoord: *Hoe zien ransomware-aanvallen er tegenwoordig uit en welke instrumenten worden hierbij ingezet?* Dit hoofdstuk begint met een toelichting op de structuur van de verschillende stappen die er gezet kunnen worden: *De ransomware kill chain*. In de vijf volgende paragrafen worden de verschillende delen van de keten nader uitgewerkt. Het hoofdstuk sluit af met paragraaf 3.8 waarin de mate van gerichtheid van ransomware-aanvallen is uitgewerkt. Overigens kent hoofdstuk 3 uiteraard een sterke link met hoofdstuk 4: In hoofdstuk 3 gaan we in op de wijze van opereren, in hoofdstuk 4 op de actoren die deze acties daadwerkelijk uitvoeren en een crimineel netwerk vormen.

3.2 De ransomware *kill chain*

Een *kill chain* is een militaire term voor een verzameling stappen die een aanvaller moet zetten om een bepaald type aanval succesvol te kunnen plaatsen. [60] Door de stappen in een kill chain systematisch te analyseren kan een aanval worden versterkt (door de keten op te bouwen uit stappen die de vijand het moeilijkst kan tegengaan/verstoren) en/of defensieve maatregelen worden bepaald (door te analyseren op welke stappen defensieve maatregelen mogelijk zijn en deze te treffen). [60] Het concept is door Lockheed Martin vertaald naar cyberaanvallen in de vorm van het Cyber Kill Chain (CKC)-raamwerk. [61] In dit raamwerk worden zeven stappen onderscheiden (Figuur 4, verticaal). Het raamwerk geeft daarnaast zes mogelijke soorten acties vanuit defensief perspectief (Figuur 4, horizontaal) die per stap zouden kunnen worden ingevuld.

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance						
Weaponization						
Delivery						
Exploitation						
Installation						
C&C						
Actions on Objectives						

Figuur 4. De 'actiematrix' uit het Cyber Kill Chain-raamwerk, die de kill chain-stappen (verticaal) koppelt aan categorieën van te nemen defensieve maatregelen (horizontaal) [61]

Het uitwerken van ransomware-aanvallen langs een kill chain-raamwerk is een goede manier om systematisch de factoren die bepalend zijn bij het slagen van een ransomware-aanval te analyseren. In de literatuur en daarbuiten zijn al diverse uitwerkingen gemaakt voor ransomware-aanvallen . Op basis hiervan en de gevoerde gesprekken komen de auteurs van dit rapport tot een iets andere indeling van de stappen. Op hoofdlijnen ziet de door de auteurs van dit rapport gevonden ransomware *kill chain* eruit zoals getoond in Figuur 5. Data-exfiltratie wordt overgeslagen indien er sprake is van *single extortion*. Bij de drie andere soorten aanvallen wordt de hele keten doorlopen. Merk dat deze kill chain een link heeft met de classificatie van impact (voorkomen van infectie, beperken van impact en herstel van systemen) in het vorige hoofdstuk, zie pagina 18. Het voorkomen van de infectie door het (potentieel) slachtoffer is gekoppeld aan het verkrijgen van initiële toegang door de

dader. Het beperken van de infectie door het slachtoffer hangt samen met het consolideren van de positie door de aanvaller. Het beperken van de impact door het slachtoffer, hangt samen met de laatste drie stappen van de aanvaller. Hoewel de exacte invulling van de onderstaande stappen zich sterk ontwikkelt over de tijd, blijft de onderstaande kill chain relatief stabiel. Zo is de exacte wijze waarop initiële toegang wordt verkregen op dit moment heel anders dan vijf of tien jaar geleden, maar het verkrijgen van deze initiële toegang was zowel toen als nu noodzakelijk voor het uitvoeren van een aanval.

Figuur 5. De ransomware kill chain

In de literatuur worden verschillende invullingen van de kill chain genoemd, door bepaalde stappen juist wel of niet te accentueren of uit te splitsen. Een voorbeeld van ketens is "*campaign, infection, staging, scan, encrypt, payday*" [62] (hierin wordt 'consolidatie' uitgesplitst in *staging* en 'scan'-stappen) en "*infection, escalation, encryption, credentials*" [63] (geen exfiltratie, al lijkt de laatste stap het exfilteren van wachtwoorden of de encryptiesleutel te betreffen). Ter vergelijking geeft [64] een meer generieke keten voor malware-aanvallen: "*initial access, credential theft, lateral movement, persistence, payload" (de 'payload"* kan hierbij naast ransomware in feite ook iets anders zijn, zoals '*scareware'* of applicaties die advertenties tonen – varianten die vandaag de dag minder populair lijken te zijn dan in het verleden). In [65] worden de aspecten *defense evasion* (het voorkomen van 'vroege' detectie van de aanval) en "impact" (naast het gijzelen van bestanden kan dat bijvoorbeeld het platleggen van de systemen zijn) toegevoegd. In het vervolg van dit hoofdstuk worden deze stappen afzonderlijk besproken.

De kill chain beschrijft overigens het proces van een ransomware-aanval van technisch perspectief en vanuit het perspectief van een aanvaller. In de praktijk is de keten vanuit het perspectief van een slachtoffer langer. Aanvullende stappen zijn bijvoorbeeld het doen van een aangifte en het opnieuw inrichten van de eigen systemen. Een aanvaller zou in de chantage ook met deze stappen rekening kunnen houden (door te eisen dat geen aangifte wordt gedaan, door te zorgen dat back-ups niet bruikbaar zijn, et cetera). Hieronder worden de verschillende stappen één voor één uitgewerkt.

3.3 Stap 1: Verkrijgen van initiële toegang

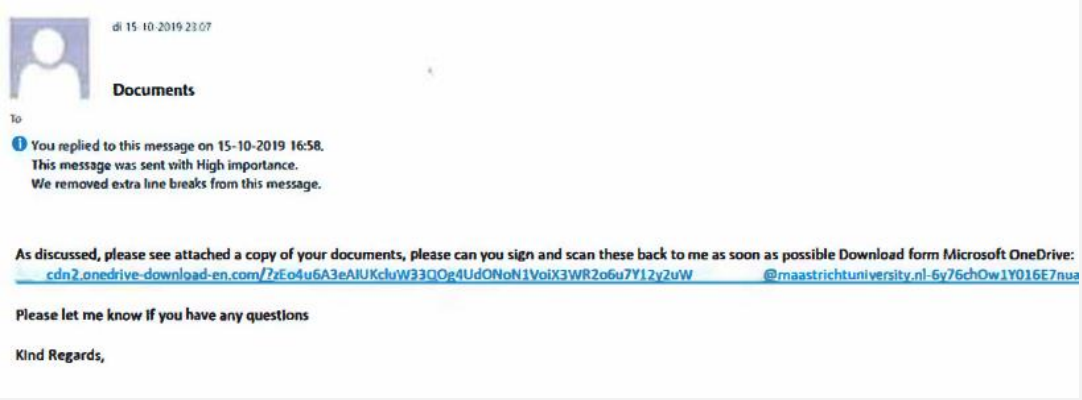
In deze fase verkrijgt de aanvaller een eerste toegang (*foothold*) bij het slachtoffer. Denk hierbij aan het verkrijgen van toegang tot een account van een medewerker van een bedrijf in een specifieke applicatie of op een specifieke server. Deze stap valt samen met *de reconnaissance*-fase uit het CKC-raamwerk.

In deze fase wordt primair gebruik gemaakt van informatie over zwakke systemen, die wordt verkregen door het uitvoeren van massale, geautomatiseerde scans, zoals *portscans* en dergelijke. Zwakke accountgegevens, in het bijzonder zwakke wachtwoorden, kunnen onder andere voortkomen uit eerdere hacks van (grotere) bedrijven of platforms (gebruik makend van het feit dat gebruikers vaak wachtwoorden 'hergebruiken'). Het kan ook gaan om 'standaardwachtwoorden' (wachtwoorden die standaard zijn ingesteld bij een nieuw systeem en ten onrechte niet zijn gewijzigd bij ingebruikname) of zwakke wachtwoorden (die door vaak te proberen kunnen worden 'geraden'). In sommige gevallen ligt de informatie over zwakheden zelfs figuurlijk of letterlijk 'op straat', denk aan verloren laptops of USB-sticks of informatie uit openbare bronnen.

Naast 'passieve' informatieverzameling kan in deze stap gebruik worden gemaakt van actieve methoden, zoals *phishing* (nepmails), waarbij *spearphishing* de gerichte variant is (de inhoud van de phishingboodschap is hierbij sterk aangepast aan de ontvanger) en social engineering. Dat laatste kan worden ingezet om beschermingen zoals multi-factorauthenticatie te omzeilen.

Box 5. Voorbeeld van initial access op basis van phishing

Criminelen verkregen de eerste toegang bij de Universiteit Maastricht via phishing. In deze e-mails werden werknemers verleid om op een link te klikken. Nadat een werknemer de link opende werd malware geïnstalleerd waarmee toegang tot het netwerk kon worden verschaft. [43]


di 15-10-2019 23:07

Documents

To

You replied to this message on 15-10-2019 16:58.
This message was sent with High importance.
We removed extra line breaks from this message.

As discussed, please see attached a copy of your documents, please can you sign and scan these back to me as soon as possible Download form Microsoft OneDrive:
cdn2.onedrive-download-en.com/?zEo4u6A3eAIUKcluW33QOg4UdONoN1VoiX3WR2o6u7Y12y2uW @maastrichtuniversity.nl-6y76chOw1Y016E7nua

Please let me know if you have any questions

Kind Regards,

In [66] legt een Nederlandse hacker uit hoe hij toegang kreeg tot systemen van de Belastingdienst. In een openbare code-repository op Github vond hij toegangscodes van systemen van de Belastingdienst. Uit het artikel: "*Toen hij echter probeerde in te loggen én een fiscusmedewerker vervolgens de door hem opgevraagde MFA-prompt bevestigde, was dat toch wel een van de opvallendste keren dat hij bij bedrijven wist binnen te dringen*"

Het ongericht verzamelen van mogelijke doelwitten kan worden geautomatiseerd, wat het vele malen efficiënter maakt dan gerichte verkenning. Er kan met minder moeite meer potentiële doelwitten worden gevonden. Dit maakt deze fase van ransomware-aanvallen over het algemeen ook 'ongericht', al kunnen er natuurlijk nog altijd redenen zijn voor aanvallers om specifieke organisaties of specifieke soorten organisaties te verkennen.

Box 6. Voorbeeld van initial access op basis van exploits

Cybercriminelen maken (ook) gebruik van (on)bekende *exploits* om toegang te krijgen tot systemen. Voornamelijk *exploits* waarvoor (nog) geen oplossing beschikbaar is (*zero-day exploits*) kunnen erg schadelijk zijn. Een recent voorbeeld hiervan is het beveiligingslek in Log4j dat in december 2021 werd ontdekt (Log4Shell). [67] Log4j is een softwarebibliotheek die veel wordt gebruikt in Java-applicaties (voornamelijk aan de 'serverkant') voor het bijhouden van logbestanden. Dergelijke applicaties zijn uit talloze componenten opgebouwd – een systeembeheerder zal in veel gevallen niet eens weten dat een Java-applicatie onder de motorkap Log4j gebruikt. Het lek in Log4j maakt het mogelijk om, simpelweg door het veroorzaken van het loggen van een bepaalde tekst (bijvoorbeeld door deze tekst simpelweg in te voeren in een systeem) op afstand code uit te voeren op dat systeem. Sinds het bekend worden van de *exploit* proberen cybercriminelen zo snel mogelijk te profiteren terwijl cybersecurity experts werken aan een patch en het updaten van systemen.

3.4 Stap 2: Consolidatie toegang en positie

Wanneer de aanvaller eenmaal een 'ingang' heeft zal deze proberen de toegang tot de systemen van het slachtoffer uit te breiden. Zo zal de aanvaller zoeken naar (andere) systemen met waardevolle informatie (*lateral movement*), toegang tot accounts proberen te verkrijgen met meer rechten op deze systemen (*privilege escalation*), zwakheden in deze systemen verkennen, et cetera.

Anders dan de vorige stap is het uitvoeren van deze handelingen grotendeels 'handwerk' (niet-geautomatiseerd) en daarnaast specifiek gericht op het voorbereiden van een ransomware-aanvallen . In het CKC-raamwerk valt deze stap onder de *delivery* fase, en voor een deel onder *weaponization*. Het ontwikkelen van de benodigde *tools* en methoden om de positie te consolideren/escaleren is vaak echter al vooraf gedaan. Deze software is eveneens op marktplaatsen te krijgen en zal in de meeste gevallen door gespecialiseerde personen/organisaties (en dus niet de aanvaller zelf) zijn ontwikkeld. Daarnaast kan er gebruik worden gemaakt van diverse (legale en gangbare) tools die primair zijn bedoeld voor het efficiënt uitvoeren van systeem- en netwerkbeheer.

Box 7. Voorbeeld van consolidatie toegang en positie

Een veelgebruikte route (voor zowel *initial access* als laterale beweging) is via Windows Remote Desktop. Deze techniek, die werkt op basis van het 'Remote Desktop Protocol' (RDP) en standaard aanwezig is in de meeste Windows-installaties, kan worden gebruikt om computers op afstand te besturen. Normaalgesproken wordt dit gebruikt voor het op afstand beheren van (server)systemen, het op afstand assisteren van gebruikers en bijvoorbeeld thuiswerken op een bedrijfscomputer.

Wanneer een organisatie geen aanvullende maatregelen heeft genomen, kunnen cybercriminelen die in het bezit zijn van correcte inloggegevens accounts gebruiken om via RDP ransomware op een machine uit te voeren. In de periode 2018-2021 is de relevantie van RDP-kwetsbaarheden afgenomen. [18] Op 11 Januari 2022 is desondanks nog een nieuwe RDP *exploit* gevonden waarmee zelfs accounts zonder RDP privileges gebruikt kunnen worden om alsnog toegang te krijgen tot de RDP software. [68].

Deze fase kan relatief snel worden uitgevoerd, maar duurt in een aantal gevallen meerdere weken tot maanden. Een specifiek aandachtspunt is het ontwijken van defensieve maatregelen (denk aan *firewalls*, intrusie-detectiesystemen, *logging*, et cetera). In sommige gevallen zal een aanval in deze fase worden afgebroken, wanneer de aanval te complex blijkt vanwege genomen maatregelen, er te weinig te halen blijkt, of wanneer een ander doelwit interessanter is. Ook kan aanvaller ontdekt worden en kan zijn toegang worden geblokkeerd.

3.5 Stap 3: Data-exfiltratie

Zoals eerder toegelicht worden bij *double, triple* of *quadruple extortion* ransomware-aanvallen de gegevens van het slachtoffer niet alleen versleuteld (encryptie), maar ook nog eens ontvreemd, waarna de aanvaller de dreiging van doorverkoop of publicatie van de data gebruikt als chantagemiddel. Deze exfiltratie is onderdeel van de *Exploitation*-stap in het CKC-raamwerk, maar zo specifiek voor ransomware (en overigens ook met andere middelen te detecteren en tegen te gaan) dat dit is benoemd als een separate stap in de kill chain. Het doel van exfiltratie is om (voor het doelwit, of klanten van het doelwit, of voor de maatschappij) waardevolle of gevoelige gegevens ongezien van de systemen van het

slachtoffer te kopiëren naar een door de aanvaller gecontroleerde locatie. Overigens wordt de gelekte data ook gebruikt om in de onderhandelingen met het slachtoffer extra druk uit te oefenen: een klein deel van de data wordt bewust gelekt om te laten zien dat ze dit ook echt kunnen. [69]

Bij exfiltratie wordt vaak dankbaar gebruik gemaakt van het feit dat veel organisaties gebruik maken van clouddiensten zoals Dropbox en OneDrive. [70] Diezelfde diensten, waarvan het gebruik binnen de organisatie (vanaf bijvoorbeeld werkstations) is toegestaan, kan een aanvaller in sommige gevallen dan ook moeiteloos gebruiken om informatie weg te sluizen. [70] Daarnaast kan gebruik worden gemaakt van webgebaseerde diensten (Mega of zelfs WeTransfer) – webverkeer is veelal op domeinniveau gecontroleerd/beperkt en de inhoud van uitwisseling vaak gecodeerd. Het is denkbaar dat aanvallers gebruik maken van systemen van het slachtoffer die juist bedoeld zijn voor het maken van eigen back-ups.

3.6 Stap 4: Inzetten van ransomware

De vorige twee stappen geven de aanvaller toegang tot systemen van het slachtoffer. Daarmee zijn het vrij generieke elementen die in veel verschillende cyberaanvallen gebruikt worden. Nadat deze eerste twee stappen zijn genomen heeft de aanvaller de keuze welke actie ondernomen wordt. Er kan bijvoorbeeld gekozen worden om gevoelige (politieke, economische, militaire) data te stelen en zo lang mogelijk onopgemerkt te blijven. Er kan ook gekozen worden om een organisatie (en in het verlengde hiervan wellicht een deel van de maatschappij) zo grondig mogelijk te ontregelen. Het uitrollen van ransomware is een andere keuze die aanvallers kunnen maken. Het stelt het in staat om hun positie in systemen van slachtoffers snel te gelde te maken.

Als voor het uitrollen van ransomware gekozen wordt, dat wordt dat in deze stap uitgevoerd op de systemen van het slachtoffer. Deze software voert de daadwerkelijke 'gijzeling' van bestanden uit (in de regel door deze te coderen of zelfs te wissen). Deze stap valt onder '*Exploitation* in het CKC-raamwerk. Doel van deze stap is om een grote hoeveelheid (liefst waardevolle) bestanden van een organisatie te coderen met een sleutel waarover alleen de aanvaller beschikt. Om dit laatste te bewerkstellingen wordt gebruik gemaakt van asymmetrische encryptie (die overigens wijdverspreid is en ook legaal wordt toegepast in bijvoorbeeld het beveiligen van de communicatie met websites). Specialistische software codeert op basis van een *public key* en (alleen) de aanvaller beschikt over de *private key* waarmee kan worden gedecodeerd. De software die wordt gebruikt kan over een aantal aanvullende 'trucs' beschikken. Zo zal deze in de regel een poging doen back-ups (denk aan Windows' "vorige versies") uit te schakelen. Omdat encryptie een intensief proces is zal de software ook proberen zo lang mogelijk onopgemerkt proberen te blijven.

Het instrument dat wordt ingezet is een specifieke ransomware variant. De onderstaande tabel toont de meest recente "marktaandelen". Dit is echter maar een deel van de "markt", er zijn op dit moment naar schatting meer dan 100 types ransomware actief. [4]

Tabel 1. Marktaandelen van soorten ransomware eind 2021 [18]

#	Ransomware type	Marktaandeel %	Ontwikkeling sinds Q3 2021
1	Conti V2	19,4%	-
2	LockBit 2.0	16,3%	+2
3	Hive	9,2%	+5
4	Mespinoza	4,1%	-2
5	Zeppelin	3,6%	+1
5	BlackMatter	3,6%	+4
6	Karakurt	3,1%	Nieuw
6	Suncrypt	3,1%	+2
6	AvosLocker	3,1%	Nieuw

3.7 Stap 5: Chantage en cash out

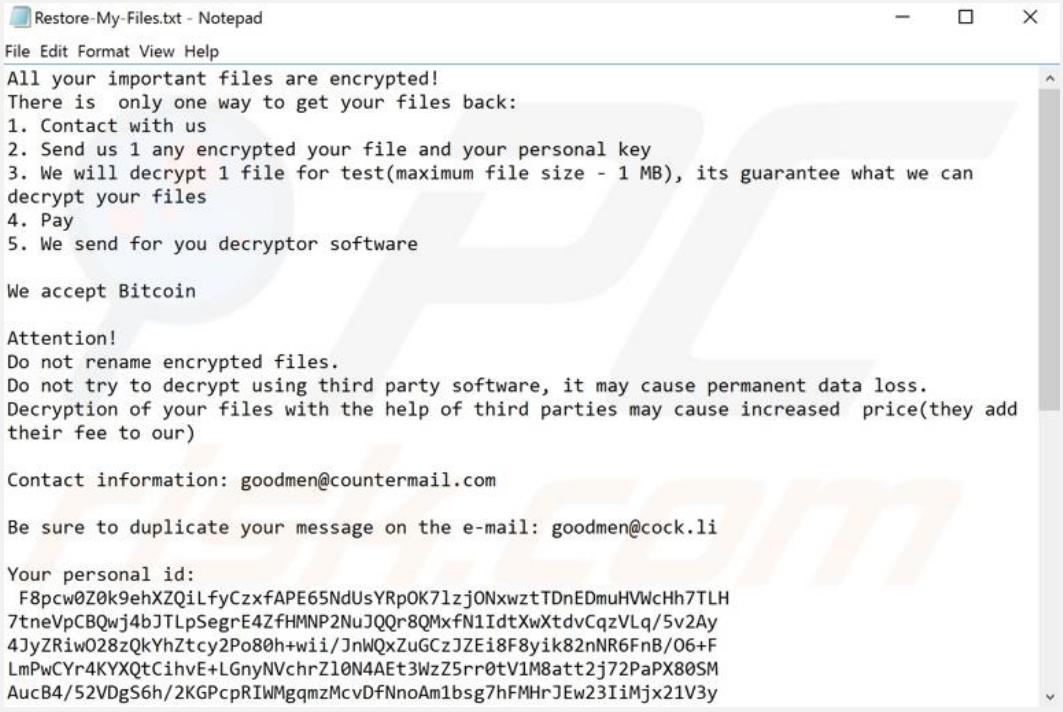
In deze fase communiceert de aanvaller met het slachtoffer en maakt deze kenbaar wat het slachtoffer moet doen om de aanval te stoppen en de gegevens terug te krijgen. Vaak zorgt de ransomware-software voor een melding op de getroffen systemen, maar communicatie kan ook daarbuiten plaatsvinden. Bij professioneel georganiseerde aanvallen zijn er vormen van communicatie waarbij het er haast op lijkt dat de aanvaller een 'klantenservice' aanbiedt, zie Box 8.

De aanvaller heeft een aantal routes om de aanval te gelde te maken. De meest voor de hand liggende is het tegen betaling decoderen van gegijzelde bestanden. Tegen betaling zal de aanvaller instructies verstrekken over hoe de bestanden kunnen worden gedecodeerd. In sommige gevallen zal de aanvaller hiervoor speciale decryptiesoftware hebben geschreven. Voor het decoderen is daarnaast een encryptiesleutel nodig. Om te controleren dat er daadwerkelijk wordt onderhandeld met de aanvaller wordt vaak eerst om 'bewijs' gevraagd (in de vorm van een aantal gedecodeerde bestanden). Om extra druk te zetten kunnen aanvallers een termijn stellen waarbinnen betaald moet worden (en waarbuiten de bestanden definitief ontoegankelijk zullen worden – de aanvaller hoeft hiervoor overigens alleen de sleutel weg te gooien).

Box 8. Voorbeeld van chantage en cash out

In Tabel 1 is aangegeven dat LockBit 2.0 een vorm van ransomware is, die op dit moment een flink *marktaandeel* heeft. Het slachtoffer ziet dat dat bureaubladachtergrond van zijn systeem gewijzigd is in de onderstaande afbeelding. [71] Het wordt direct duidelijk gemaakt de belangrijke bestanden zijn gestolen en versleuteld.

Er wordt verwezen naar een bestand (RESTORE-MY-FILES.TXT) dat op het bureaublad is geplaatst. De onderstaande afbeelding toont een voorbeeld van de inhoud van een dergelijk bestand. [72]



Er wordt stap voor stap uitgelegd hoe het slachtoffer moet betalen en de documenten kan decoderen. Allereerst wordt duidelijk gemaakt dat er contact moet worden opgenomen met de *klantenservice*: goodmen@coutermail.com. Zo kan worden aangetoond dat zij daadwerkelijk bestanden kunnen ontsleutelen. Na betaling krijgt het slachtoffer de software om alle bestanden te ontsleutelen,

Wanneer ransomware-software op de 'juiste' wijze is geïmplementeerd (namelijk door gebruik te maken van asymmetrische encryptie met ten minste een nieuw sleutelpaar per slachtoffer) is er geen enkele mogelijkheid voor het slachtoffer om de sleutel op andere wijze

in handen te krijgen. Zwakheden in de encryptie of bijvoorbeeld de sleuteluitwisseling en sleutelopslag van de aanvaller kunnen ervoor zorgen dat slachtoffers hun bestanden ook zónder medewerking van de aanvaller kan decoderen. De WannaCry-encryptor genereert een cryptografische sleutel op het apparaat van het slachtoffer, waarmee vervolgens bestanden worden gecodeerd. Na het genereren van de sleutel blijft deze sleutel door een programmeerfout in het geheugen van de computer staan. Met speciale software is deze sleutel (zolang de WannaCry-software niet is afgesloten) uit te lezen. [73] Bovenstaand voorbeeld maakt duidelijk dat organisaties voorzichtig en bedachtzaam moeten handelen bij een ransomware-aanval. In het genoemde voorbeeld zou het direct uitschakelen van getroffen systemen bijvoorbeeld de mogelijkheid tot het extraheren van de sleutel tenietdoen.

In deze vijfde stap komt ook het verschil tussen de *double, triple* en *quadruple* extortion goed naar voren. Bij *double extortion* krijgt de chantage vorm door te dreigen met openbaarmaking. Bij *triple extortion* worden daarnaast digitale bedrijfsprocessen verstoord zodat het herstellen van de systemen lastiger wordt. Hierdoor kan er extra druk worden gezet op het slachtoffer. Tot slot zien we bij *quadruple extortion* dat de druk op het slachtoffer nog sterker wordt opgevoerd doordat zakelijke relaties op de hoogte gesteld worden of zelfs ook tot slachtoffer gemaakt worden.

De kill chain beschrijft het proces van een ransomware-aanval van technisch perspectief en vanuit het perspectief van een aanvaller. In de praktijk is de keten vanuit het perspectief van een slachtoffer langer. Aanvullende stappen zijn bijvoorbeeld het doen van een aangifte en het opnieuw inrichten van de eigen systemen. Een aanvaller zou in de chantage ook met deze stappen rekening kunnen houden (door te eisen dat geen aangifte wordt gedaan, door te zorgen dat back-ups niet bruikbaar zijn, et cetera).

3.8 Gerichtheid van aanvallen

Een ransomware-aanval kan zowel gericht als ongericht zijn. Bij een ongerichte aanval maakt het de aanvaller niet uit welke organisatie of persoon het slachtoffer wordt. Bij een gerichte aanval heeft een aanvaller a priori een specifieke organisatie in het vizier. Zoals hieronder wordt toegelicht worden vandaag de dag (in aantal) voornamelijk 'semi-gerichte' aanvallen op organisaties waargenomen, waarbij sprake is van gerichte aanvallen op organisaties geselecteerd uit een ongerichte set mogelijke doelwitten.

3.8.1 Ongerichte aanvallen

Een ongerichte aanval komt voort uit een groot aantal 'leads' (mogelijke doelwitten). Zolang het verkrijgen van 'leads' relatief goedkoper is dan de verwachtingswaarde (slaagkans maal *pay-out*) kan een crimineel op deze wijze met relatief kleine inspanning veel geld verdienen. Zoals eerder opgemerkt is het geautomatiseerd vinden van doelwitten (in een *target rich environment*) op dit moment relatief eenvoudig en goedkoop.

Ongerichte ransomware-aanvallen richtten zich in eerste instantie op consumenten. [20] Deze aanvallen waren in feite volautomatisch: de ransomware-software bevatte (ook) een *worm*-component die bijvoorbeeld andere computers in het netwerk infecteert, of andere personen poogt te infecteren door e-mails te sturen naar het hele adresboek van een geïnfecteerde gebruiker. Tegenwoordig worden veel meer aanvallen op organisaties waargenomen. Deze aanvallen zijn 'semi-geautomatiseerd' en 'semi-gericht', wat betekent dat er (in ieder geval) handmatig een doelwit wordt geselecteerd.

3.8.2 Semi-gerichte aanvallen

Bij de doelwitselectie komt, zoals eerder genoemd, ook vaak informatieverzameling over het doelwit kijken. Een IP-adres uit een gekochte set met IP-adressen van zwakke systemen wordt herleid tot een organisatie. Een aanvaller zal willen weten wat de omvang en omzet van de organisatie is om de haalbare *pay-out* en daarmee de eigen *business case* te kunnen bepalen. De relatie tussen omvang van het doelwit en het aantal aanvallen is echter allesbehalve lineair. [74] De herleidbaarheid van een IP-adres naar een organisatie zou een rol kunnen spelen. Wanneer een organisatie via een dienstaanbieder geconnecteerd is op het internet staat het IP-adres op naam van de aanbieder en is lastiger te achterhalen om welke organisatie het gaat, dan wanneer de organisatie groot genoeg is om zélf direct op internet te connecteren (via een eigen 'AS').

Bij semi-gerichte aanvallen wordt veelal gebruik gemaakt van *off the shelf*-tools en bekende zwakheden in systemen. Omdat voor dergelijke zwakheden in de regel al wel patches (updates) beschikbaar zijn, leidt dit ertoe dat met name organisaties die slecht of niet updates toepassen in principe een hoger risico hebben om hier slachtoffer van te worden. [75] Tegelijkertijd is het voor grotere organisaties met complexere ICT-systemen vrijwel ondoenlijk om alle systemen te allen tijde up-to-date te houden (te meer omdat het blindelings uitvoeren van patches ook niet altijd zomaar kan zonder eerst goed te testen, organisaties soms al moeite hebben hun ICT-landschap in kaart te brengen, et cetera).

Bij semi-gerichte aanvallen wordt (in gevoerde gesprekken) de hypothese gesteld dat het opwerpen van een groot aantal relatief kleine maatregelen waarschijnlijk erg effectief zou kunnen zijn. Een aanvaller moet dan relatief veel tijd steken in een aanval, terwijl de andere mogelijke doelwitten wellicht wél sneller en eenvoudiger kunnen worden geëxploiteerd.

3.8.3 Volledig gerichte aanvallen

Naast de ongerichte aanvallen worden er ook sterk gerichte aanvallen uitgevoerd. Hierbij wordt vooraf het slachtoffer bepaald en gaat een aanvaller alles in het werk stellen om de aanval te laten slagen. Dergelijke aanvallen vereisen behoorlijk wat mankracht en kennis. Hierbij komt al snel de vraag naar voren in welke gevallen een dergelijke zeer kostbare aanval te verantwoorden is. De auteurs van dit rapport vermoeden dat dan moet gaan om zeer gevoelige (militaire, economische, of politieke) gegevens en organisaties met vitale functies in een economie. De vraag is echter in welke mate een ransomware-aanval de strategische doelen van de aanvaller dient. Als een aanvaller een positie heeft opgebouwd waarmee toegang wordt verkregen tot zeer gevoelige politieke, militaire of economische informatie, dan lijkt het veel logischer om deze positie zo lang mogelijk te behouden en zo veel mogelijk data te blijven exfiltreren. Bij een ransomware-aanval is het slachtoffer daarentegen direct op de hoogte van infiltratie in zijn systemen.

4 Betrokken actoren bij ransomware-aanvallen

De derde onderzoeksvraag is als volgt: *Welke soorten partijen zijn bij deze aanvallen betrokken?*

De eerste ransomware aanvallen werden gepleegd door individuele criminelen, maar inmiddels is er sprake van een uitstekend functionerende *supply chain* van verschillende soorten actoren met een hoge mate van specialisatie. Het ransomware-ecosysteem opereert bijna alsof het een legitieme, goed ontwikkelde dienstensector is. Initiële toegang tot netwerken wordt bijvoorbeeld vaak via platformen verkocht aan de hoogste bieder. Er zijn verschillende soorten partijen die op verschillende manieren deze toegang proberen te verwerven. De kopers van de initiële toegang werken dit op hun beurt uit, consolideren deze positie en verkopen deze positie wederom aan de hoogste bieder. De daadwerkelijke ransomware-aanval komt pas in de fase erna. De partijen die ransomware-software ontwikkelen en beheren zijn niet altijd de partijen die deze software ook daadwerkelijk gebruiken. Vaak worden er affiliates ingezet die de aanval uitvoeren. Er zijn daarnaast datamanagers die gestolen data analyseren, verkopen en/of openbaar maken. In de laatste stap (chantage en *cash out*) zijn een breed scala aan partijen betrokken: onderhandelaars, helpdesks, witwassers, et cetera.

Verreweg het meest voorkomende motief voor ransomware-aanvallen is financieel gewin. Activisme komt slechts sporadisch voor. ransomware-criminelen gedragen zich deels als rationele actoren: de kosten, opbrengsten en pakkans worden geregeld zorgvuldig afgewogen. Daders lijken relatief vaak uit landen te komen die voorheen deel uitmaakten van de Sovjet-Unie. In sommige gevallen vallen daders bepaalde soorten organisaties bewust niet aan. Voorbeelden zijn organisaties uit landen in de voormalige Sovjet-Unie en de zorgsector gedurende de Coronacrisis.

4.1 Inleiding

In dit hoofdstuk wordt ingegaan op de diverse betrokken actoren bij een ransomware-aanval. Hiermee wordt antwoord gegeven op onderzoeksvraag 3: *Welke soorten partijen zijn bij deze aanvallen betrokken?* In paragraaf 4.2 wordt een overzicht van de ransomware *supply chain* gepresenteerd. Paragraaf 4.3 gaat in op de specifieke functies daarbinnen en paragraaf 4.4 staat stil bij de specifieke daderprofielen. Voor dit onderzoek is geen diepgaand criminologische onderzoek uitgevoerd, maar is aangesloten bij de methodes die in het eerste hoofdstuk zijn beschreven.

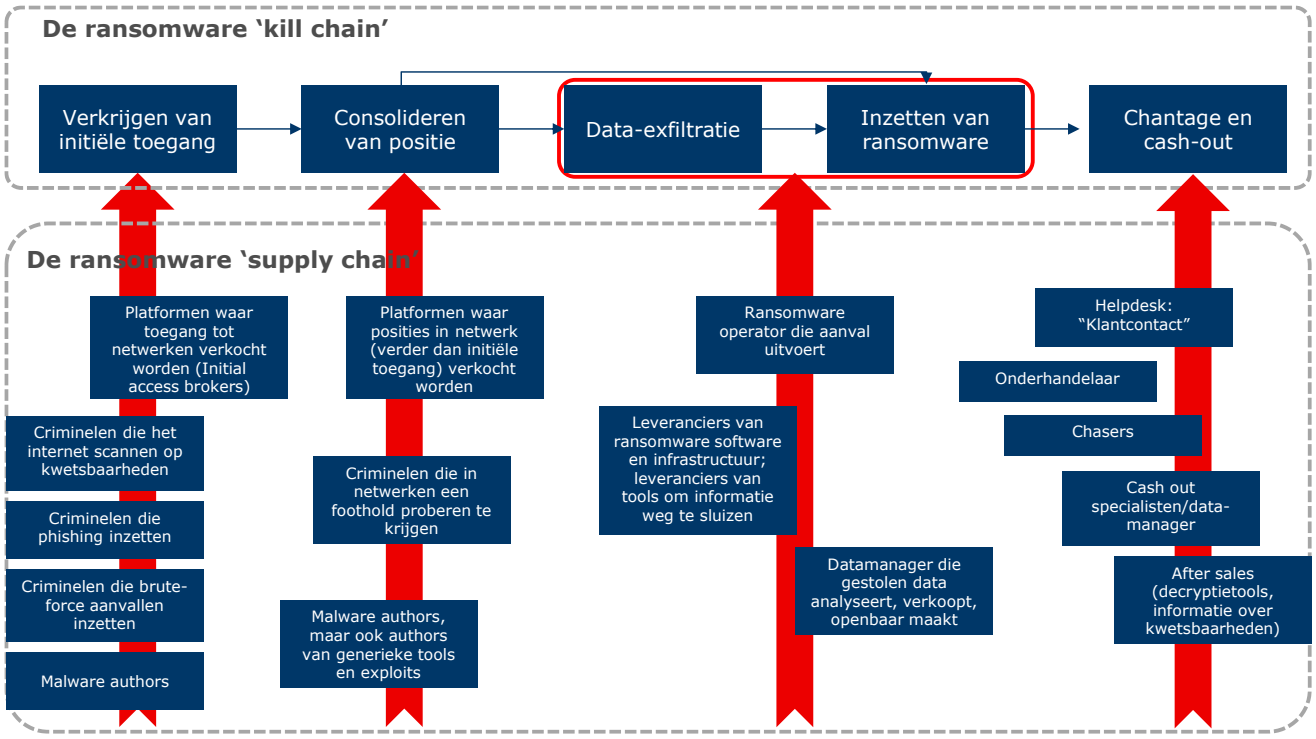
4.2 De ransomware supply chain

Het imago van een puber of de *lone wolf* die op zijn zolderkamer een organisatie hackt, gaat niet (meer) op voor de meeste ransomware-aanvallen . In de meeste gevallen worden aanvallen uitgevoerd door geprofessionaliseerde criminele organisaties. Deze aanvallers beschikken over een uitstekend functionerende *supply chain* van verschillende soorten actoren met een hoge mate van specialisatie kennen. Het ecosysteem opereert bijna alsof het een legitieme, goed ontwikkelde dienstensector is: er is een klantenservice, onderhandelaars en zelfs een business intelligence afdeling die doelwitten analyseert op

kwetsbaarheden (welke software gebruikt deze organisatie?) en hoeveel losgeld een organisatie zou kunnen betalen (wat is de omzet?).

In onderstaande figuur is de eerder getoonde kill chain aangevuld met de verschillende 'functies' uit de *supply chain*. Deze analyse is gemaakt op basis van literatuurstudie, met name [76] [5], en is gevalideerd en aangevuld in interviews. In de volgende paragrafen worden de verschillende blokjes toegelicht. De *supply chain* van een ransomware-aanval is professioneel en complex, maar vooral ook fluïde en gelegenheidsafhankelijk. Een flink aantal rollen wordt beschreven, maar afhankelijk van de aanval verschilt de wijze invulling van deze rol, de mate waarin één partij verschillende rollen op zich neemt en of de rol überhaupt bestaat.

Doordat er sprake is van een groot aantal functies binnen de *supply chain* en een groot aantal actoren die hierin een rol spelen, is het moeilijk om te stellen dat een aanval is uitgevoerd door één bepaalde groep criminelen. Het is een samenspel van een groot aantal actoren en functies die samen leiden tot de aanval. Er zijn veel verschillende actoren betrokken bij een ransomware-aanval en ieder heeft zijn eigen specialisatie en soms pakt een actor meerdere functies op.



Figuur 6. De ransomware supply chain

4.3 Functies binnen de supply chain

Hieronder wordt per stap uit de kill chain een beschrijving van de benodigde functies aangegeven:[5]

[5] Voornaamste bronnen [5] [76]. De diverse functies binnen de *supply chain* zijn verder ingevuld met behulp van interviewrespondenten.

4.3.1 Verkrijgen van initiële toegang

Bovenaan de keten die toeziet op het verkrijgen van initiële toegang zijn de *initial access brokers* (IAB's). Dit zijn de partijen die toegangsgegevens van organisaties en burgers verkopen. De *initial access brokers* verkopen dus toegang tot netwerken. Deze toegang kunnen ze zelf verkrijgen, maar ze kunnen ook weer hebben uitbesteed. De informatie over initiële toegang wordt op het *dark web* of via Telegram doorverkocht aan de partijen die deze positie gaan consolideren. De prijzen variëren van enkele tientjes tot soms wel enkele duizenden euro's.[6] [76]

Er zijn verschillende manieren om initiële toegang te krijgen. Sommige criminelen stropen het internet af op zoek naar systemen met (on)bekende kwetsbaarheden. Andere partijen maken gebruik van *phishing* of *brute-force* aanvallen. [77] In veel gevallen maken deze partijen op hun beurt gebruik van software die door *malware authors* is gemaakt. [77]

Box 9. Voorbeeld van access brokers

Access brokers zoals Wazawaka en Babam verkopen toegang tot geïnfecteerde Pc's en VPN credentials. Zo is het bekend dat de ransomware gang LockBit positieve recensies heeft achtergelaten op het overkopen van Babam-compromised netwerken op het Exploit cybercrime forum.

4.3.2 Consolideren van positie

Nadat toegang is verkregen, vindt consolidatie van de positie binnen het netwerk plaats. Het netwerk wordt zo goed mogelijk in kaart gebracht. Toegang tot de juiste rechten wordt verkregen, idealiter een admin-account waarmee toegang tot de hele organisatie wordt verworven. Hier kan een hacker dagen tot weken mee bezig zijn, zo concluderen wij op basis van interviews met cybersecurityexperts. Verschillende hacker tools (additionele malware) kunnen hiervoor worden ingezet, andere inloggegevens kunnen worden afgevangen en er kunnen achterdeurtjes gebouwd worden volgens deze experts. Alles om bestendigheid in het netwerk te creëren en langzaam op te schuiven naar het doel.

Bij deze stap zijn -volgens de geïnterviewde cybersecurityexperts- mogelijk een aantal functies betrokken, zoals schrijvers van malware (dit kan ook indirect als de additionele malware wordt ingekocht) en criminelen die gespecialiseerd zijn in het krijgen van een *foothold* in netwerken. Er zijn ook voorbeelden van criminele benden die personeel werven onder het mom van legitieme *pentesting*, terwijl hun personeel feitelijk een positie aan het consolideren zijn. [78] Werknemers denken dus dat ze in opdracht van een bedrijf op zoek zijn naar kwetsbaren binnen de systemen van dat bedrijf, terwijl ze in werkelijkheid betrokken zijn bij een misdrijf. Net als bij *initial access* worden ook deze gegevens via platformen doorverkocht. Het is evident dat deze informatie vaak waardevoller is dan de *initial access*. De kopers van deze informatie bevinden zich namelijk al in de volgende stap.

4.3.3 Data-exfiltratie en inzetten van ransomware

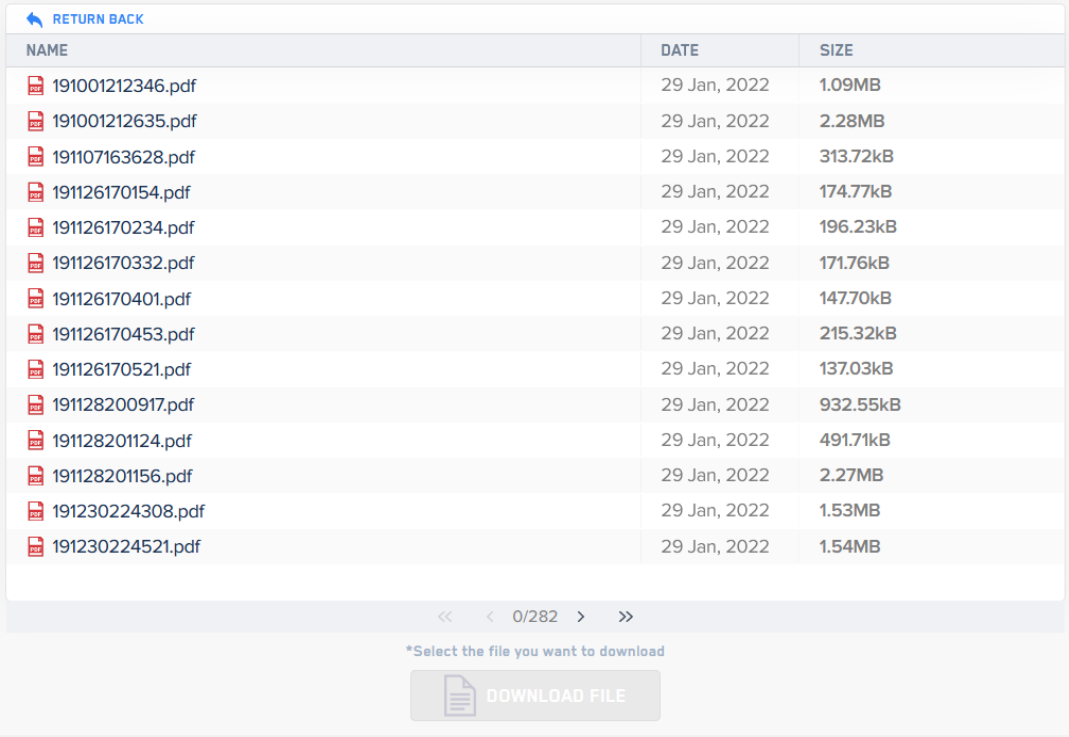
Als het netwerk goed in kaart is gebracht en toegang tot de gewenste systemen is verkregen, kan eventueel worden overgegaan op het wegsluizen van waardevolle, gevoelige informatie. Dit kan geautomatiseerd (hier bestaan diverse tools voor) maar ook handmatig. Veelvoorkomende doelbestanden zijn onder meer financiële gegevens, klantinformatie en

[6] Informatie van organisaties die 24/7 dienstverlening hebben (zoals een distributiebedrijf) zijn relatief veel geld waard, omdat zij veel schade ervaren wanneer hun bedrijf wordt stilgelegd. Dat betekent voor hackers dus een hogere kans op betaling. Zie ook hoofdstuk 2.

intellectueel eigendom/handelsgeheimen. [76] Deze informatie wordt dan te koop aangeboden op het *dark web* of via Telegram, of kan als middel dienen om het slachtoffer af te persen door (te dreigen met) publicatie. [76] Datamanagers analyseren en structureren de data die de criminelen hebben buit gemaakt en maken het klaar om online te zetten. [76] Doorgaans publiceren de datamanagers eerst een klein setje data in de hoop dat een slachtoffer alsnog betaalt. [76] Hier is dus afstemming nodig met de onderhandelaars. Wordt er niet betaald, dan wordt langzaamaan alle data (soms enkele honderden tot zelf enkele terabytes aan data) geüpload. [76] Deze documenten zijn dan downloadbaar voor iedereen.

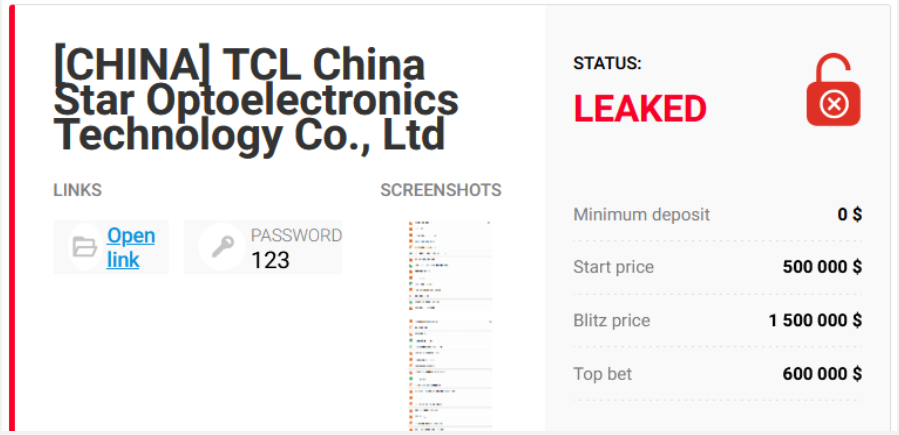
Box 10. Voorbeeld van het verkopen van data.

Double extortion is een van de meest gangbare modus operandi die wordt gehanteerd door ransomwaregroepen. Er zijn door de onderzoekers bijna 50 websites gevonden die worden gerund door ransomware gangs. Op het gros hiervan zijn bestanden van slachtoffers te downloaden. Doorgaans betreft dit slechts een aantal bestanden waarmee duidelijk wordt gemaakt naar het slachtoffer wat voor data er allemaal buit gemaakt is.



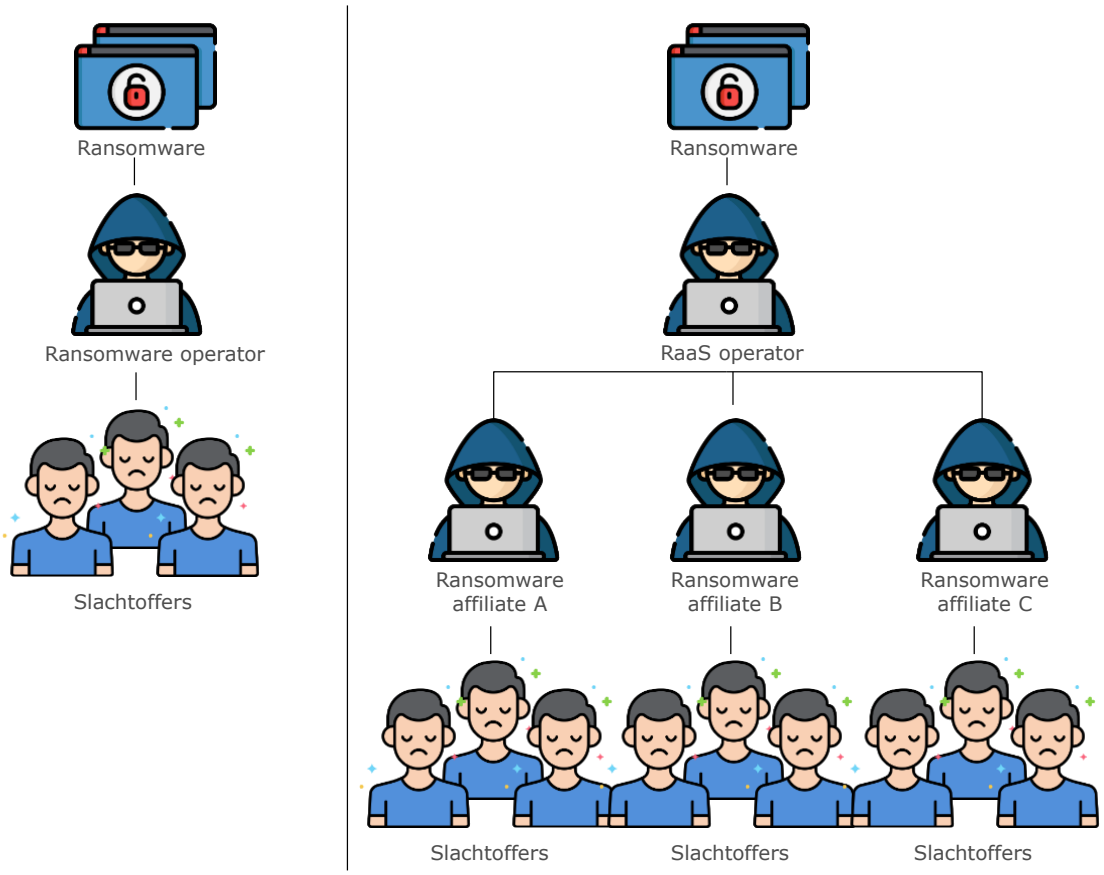
Figuur 7. Op de website van LockBit 2.0 wordt deels getoond wat er buit gemaakt is en 'samples' kunnen worden gedownload. Bron: eigen analyse Dialogic

Daarnaast zijn er ook marktplaatsen en Telegramgroepen waar datasets worden geveild. Ransomware gangs proberen met deze veilingen, ondanks dat er geen losgeld is betaald, toch geld te verdienen aan een aanval. De bedragen die worden geboden lopen tot in de honderdduizenden euro's.



Figuur 8. Een veiling van data op de LockData TOR pagina.

Er is vaak een onderscheid te maken tussen de partij die ransomware-software ontwikkelt, beheert en exploiteert (ransomware operators) en de partij die de ransomware-software daadwerkelijk inzet. Ransomware operators die deze software beheren hebben uiteraard geen onbeperkte capaciteit. Op basis van de interviews met cybersecurityexperts concluderen de auteurs van dit rapport dan ook dat in de Champions League van ransomware-aanvallen slechts een paar professionele groeperingen actief zijn. Deze 'eindbazen' (de ransomware operators) ontwikkelen nieuwe software en methoden, en kiezen ervoor om zelf de touwtjes in handen te houden of om deels hun ransomware te verhuren aan uitvoerders die ook wel *affiliates* worden genoemd. [76] Zij nemen Ransomware-as-a-Service af. In interviews met cybersecurityexperts horen de auteurs van dit rapport verhalen van operators die op den duur 'met pensioen' gaan en hun ransomware vervolgens verhuren aan affiliates. Figuur 9 toont schematisch hoe dit systeem vorm krijgt. Op deze manier krijgen operators inkomsten per aanval, maar blijven ze zelf buiten schot. De commissie bedraagt doorgaans 70% tot 80% van het losgeld dat betaald wordt. [76] De operator krijgt tussen de 20% en 30% van het losgeld. [76] Via onder meer forums worden affliates geworven en om toegang te krijgen tot een forum dit gebeurt, moet gestemd worden door mensen die al op het forum zitten [76] Dit controlemechanisme is vooral bedoeld om de politie buiten de deur te houden. [76]



Figuur 9. Ransomware operatormodel (links) versus affiliates-model (rechts). Bron: Dialogic

Box 11. Voorbeeld van recente strubbelingen in samenwerkingen

In de afgelopen maanden zien experts barstjes verschijnen in de relaties binnen ransomwaregroeperingen. Affiliates hebben openbaar kritiek op elkaar en lekken codes, tools en *playbooks* van ransomware operators om hun frustraties te uiten over vermeende onrechtvaardigheden. Vaak gaat dit over geld (*affiliates* vinden dat zij een groter aandeel van het losgeld verdienen). [79]

Andersom twijfelen ransomware operators ook geen moment om een *affiliate* te laten vallen als deze zich niet aan de afspraken houdt (bijv. over het niet aanvallen van bepaalde sectoren of landen) of een domme zet doet. De aanval op de *Colonial Pipeline* heeft zelfs zoveel ongewenste aandacht getrokken van de FBI dat de operators hun *affiliate* programma hebben stopgezet. [80]

4.3.4 Chantage en cash-out

De laatste stap bestaat uit de uiteindelijke financiële afhandeling van de afpersing: de onderhandelingen tussen dader en slachtoffer, het eventueel betalen door het slachtoffer, het wegsluizen van het betaalde losgeld, het witwassen door de dader en eventuele 'aftersales'.

Bij de grotere aanvallen onderhandelt een tussenpersoon namens de ransomware operator of *affiliate* met het slachtoffer. [76] Het percentage van de omzet van een bedrijf bepaalt daarbij doorgaans de hoogte van het losgeldbedrag (tussen de 0,4% en 2% van de jaarlijkse omzet van een organisatie). [76] De onderhandelaar moet vooral betrouwbaar overkomen

om de transactie een betere kans van slagen te geven. [76] Onderhandelaars werken doorgaans in ploegendiensten in chatboxen. [76] Soms volgt er na onsuccesvolle onderhandelingen nog een extra groep in de *supply chain*: de *chasers*. [76] Zij zijn te vergelijken met een digitale knokploeg. Zij doen hetzelfde als de onderhandelaars, maar voeren de druk flink op met bedreigingen. [76]

Een cash out specialist of datamanager voert het technisch beheer van de databases uit om slachtoffers na betaling hun sleutel terug te kunnen geven, aldus de geïnterviewde cybersecurityexperts. Een helpdesk ondersteunt slachtoffers, bijvoorbeeld bij het ontsleutelen. Helpdesks zijn vaak 24/7 beschikbaar en spreken goed Engels. Soms worden er zelfs nog *after sales* aangeboden, zoals een rapport met de vastgestelde kwetsbaarheden van de netwerken van het slachtoffer of ontsleuteltools. [81]

Dit model kan verder worden uitgebreid. Zo worden er bijvoorbeeld aan de achterkant nog gespecialiseerde witwassers ingehuurd. Het geld komt terecht bij de ransomware operators (of affiliates) en zij zetten de Bitcoin om in 'echt' geld of investeren het weer in een nieuwe aanval.

Dit model kan verder worden uitgebreid. Zo worden er bijvoorbeeld aan de achterkant nog gespecialiseerde witwassers ingehuurd. Het gesimplificeerde verdienmodel ziet er volgens de geïnterviewde cybersecurityexperts als volgt uit: Het geld komt terecht bij de ransomware operators (of affiliates) en zij zetten de Bitcoin om in 'echt' geld of investeren het weer in een nieuwe aanval. In de praktijk ligt dit uiteraard iets genuanceerder en complexer.

4.4 Daderprofielen

Als het gaat om daderprofielen, komen een aantal opvallende zaken aan het licht:[7]

Afkomst

Veel ransomware-groeperingen komen uit Rusland en Oekraïne volgens de geïnterviewde cybersecurityexperts. In de interviews komt dit duidelijk naar voren en er worden verschillende redenen genoemd waarom dit zo zou kunnen zijn. Zo krijgen kinderen in het oude Sovjetsysteem op een hoog niveau bètavakken, zijn er veel technische universiteiten, maar is er weinig werk in de IT. Ook is de meerderheid van de bevolking relatief arm, heeft het weinig carrièreperspectief en hebben sommigen een negatief beeld van het Westen. Dat is een potentiële *breeding ground* voor cybercriminelen. Daarnaast fungeert Rusland als veilig onderkomen voor veel cybercriminelen, doordat ze weigert samen te werken met opsporingsdiensten uit andere landen. Wat de concentratie Russische en Oekraïense groeperingen ook versterkt is het feit dat veel bestaande groeperingen enkel Russischsprekende (of op z'n minst het Cyrillisch schrift kennende) affiliates en ander 'personeel' zoeken, aldus de geïnterviewden. Fora op het *dark web* en Telegramgroepen spelen daarin een belangrijke rol. Russischtalige fora zijn enorm ontwikkeld en veelomvattend volgens de geïnterviewde cybersecurityexperts. Volgens één geïnterviewde expert neemt de relevantie van het *dark web* af en die van Telegramgroepen toe.

Rol van de voormalige Sovjet

Diverse ransomware software (o.a. LockBit) is zo geschreven dat deze niet werkt in post-Sovjet landen, zie Box 12. Die landen blijven dus enigszins buiten schot. Of dat het gevolg

[7] Dit betreft een integrale analyse op basis van interviews en literatuurstudie. De analyse blijft op hoofdlijnen. Er zijn overigens diverse onderzoeken die daderkenmerking van cybercriminelen tot in detail hebben bestudeerd, zie bijvoorbeeld [177]

is van statelijke inmenging of eerder een soort activisme is, is onduidelijk. De invloed van statelijk actoren blijft speculeren. Dat het mikpunt vooral ligt op het westen (de OECD-landen) past wel bij het doorgaans negatieve beeld dat post-Sovjet landen van het Westen hebben, volgens enkele geïnterviewde beleidsmakers. Anekdotische informatie geeft ook aan dat Russische groeperingen de toepassing van ransomware-aanvallen zien als het heffen van een soort belasting op het westen.

Box 12. Voorbeeld van ransomware die niet overal werkt

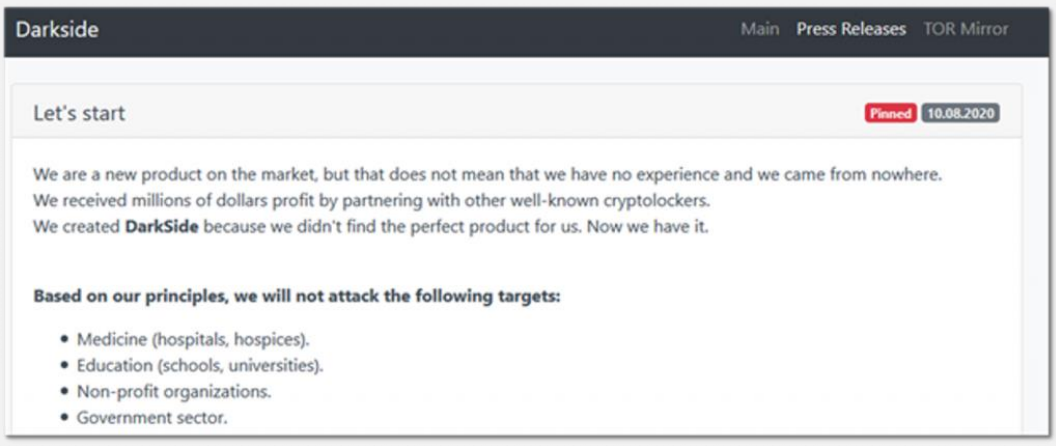
De ransomware ontwikkeld door LockBit werkt niet in de landen uit de voormalige Sovjet-Unie. Op de "*conditions for partners"* pagina van LockBit staat: "*LockBit 2.0 does not function in post-Soviet countries.*". De malware van LockBit controleert bijvoorbeeld het IP-adres, de taalinstellingen van de computer of het soort toetsenbord om te controleren waar ter wereld het slachtoffer zich bevindt.

Ethiek

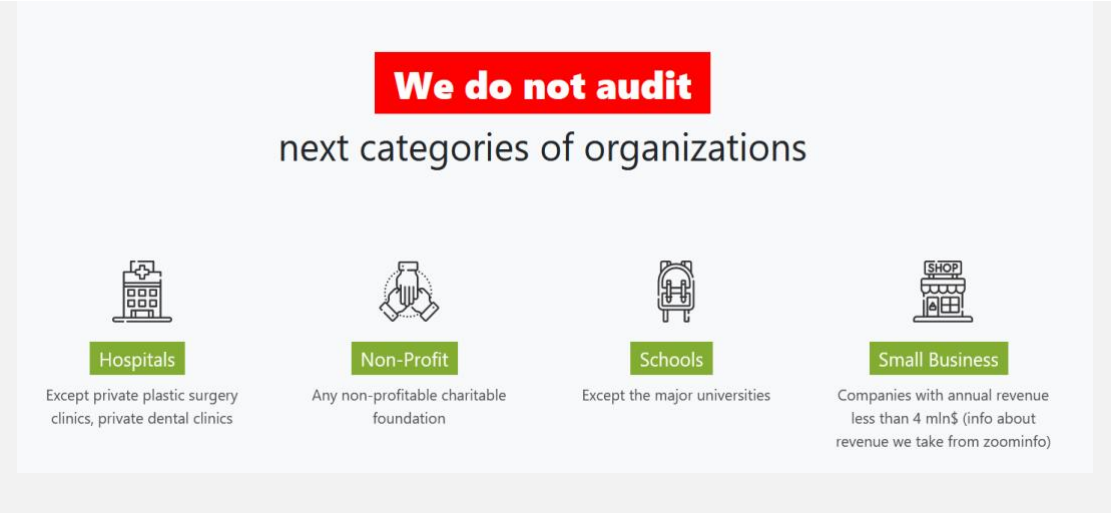
Ethiek speelt een (kleine) rol voor cybercriminelen. Zo verbieden enkele ransomware-groeperingen hun affiliates om ziekenhuizen aan te vallen. [82] Dit is enerzijds vanuit ideologie – een extreem voorbeeld zijn groepen die 'goede daden' in plaats van losgeld vereisen voor het ontsleutelen van de gegijzelde bestanden. [83] Anderzijds lopen groeperingen meer risico om een reactie uit te lokken als ze essentiële diensten aanvallen, aldus de geïnterviewde cybersecurityexperts. De *Colonial Pipeline* aanval is hier een mooi voorbeeld van. Dat heeft geleid tot een klopjacht van de FBI, zie ook Box 11. Hoewel ransomware operators hun affiliates screenen, 'gehoorzamen' ze toch soms niet, blijkt uit interviews met cybersecurityexperts. Dan worden ze na een aanval verbannen uit de groep. Uit deze interviews blijkt dat hoewel ethiek een rol speelt, de pakkans echter toch vaak doorslaggevend is.

Box 13. Voorbeeld van ransomwaregroepen die bepaalde sectoren niet zegt aan te vallen

De ransomware groep 'DarkSide' heeft aangegeven in specifieke organisaties niet te *targetten* op principiële gronden. Het gaat dan om zorginstellingen, onderwijsinstellingen, non-profit organisaties en de overheidssector.



Met de opkomst van de coronapandemie hebben verschillende ander groepen zoals DoppelPaymer, MAZE, Nefilim en CLOP aangegeven geen zorginstellingen aan te vallen. Ze geven aan dat dit soms 'per ongeluk' kan gebeuren (met name bij een geautomatiseerde aanval of affliates die niet gehoorzamen) en in dit geval de decryptie gratis zullen aanbieden. [84] De groep Babuk geeft op hun website aan dat ze geen ziekenhuizen, *non-profits*, scholen of kleine bedrijven 'auditten'.



Motief en gedrag

Verreweg het meest voorkomende motief voor ransomware-aanvallen is financieel gewin. [85] Dat blijkt ook uit de professionele opzet van de *supply* chain.

ransomware-criminelen gedragen zich bij uitstek als rationele actoren. [85] Waar bij veel andere vormen van criminaliteit de theorie niet opgaat, is hier de *Rational Choice Theory* zeker relevant. De kosten, opbrengsten en pakkans worden zorgvuldig afgewogen. Soms worden hier zelfs formules op los gelaten.

Organisatie

Georganiseerde misdaad en cybercrime zijn nauw met elkaar verbonden, volgens de geïnterviewde cybersecurityexperts. Hoewel ransomware uiteraard vaak ook georganiseerde misdaad betreft, zijn deze groeperingen ook soms actief in de meer zichtbare criminaliteit. Bij het oprollen van cyberbendes worden steeds vaker bijvoorbeeld drug en wapens gevonden. Daarnaast gaan – volgens deze geïnterviewden – meer zichtbare criminele organisaties, zoals bijvoorbeeld motorclubs, aan de slag met phishing en ransomware.

4.4.1 Dadergroepen

Er zijn grofweg twee typen dadergroepen: zelfstandig opererende ransomware groeperingen en groepen die in opdracht van statelijke actoren werken. [86] Deze 'staatgesteunde' groepen (ook wel *Advanced Persistent Threat* (APT) groepen genoemd) vallen veelal onder landen als Rusland, China en Noord-Korea. Ze richten zich vaak op belangrijke industriële sectoren, met als doel het stelen van bedrijfs- en staatsgeheime informatie en/of het ontwrichten van kritieke infrastructuur in andere landen. [86] Verschillende geïnterviewde experts geven echter ook aan dat er banden zijn tussen criminelen en statelijke actoren. Wellicht heeft Oekraïnecrisis dit duidelijker voor het voetlicht gebracht: Ransomware-groep Conti houdt er bijvoorbeeld expliciet een politieke agenda op na en heeft zich duidelijk gemengd in de oorlog. [87]

Veruit de meeste ransomware-criminelen zijn financieel gemotiveerd. [85] Ransomware leent zich dan ook uitstekend voor financieel gewin. [85] Toch zijn er nog enkele andere typen daders te onderscheiden, met elk hun eigen motivaties en modus operandi (zie Tabel 2). De kans dat verschillende typen daders ransomware als middel gebruiken voor hun doel verschilt uiteraard. Een natiestaat kan ransomware inzetten, maar heeft een scala aan andere, betere methoden om druk uit te oefenen op andere partijen om geopolitieke doelen

te realiseren. Systemen in de Oekraïne werden eind februari 2022 aangevallen met *wipers* die data niet versleutelden met simpelweg verwijderden. [88] Hetzelfde geldt voor hacktivisten. Zij kunnen ransomware gebruiken om organisaties onder stuk te zetten om bepaalde acties te staken, maar ook hier zijn tal van andere methoden mogelijk. Hoewel de andere typen daders ook ransomware gebruiken (zie bekende voorbeelden), liggen andere cyberaanvallen wellicht meer voor de hand.

Tabel 2. Overzicht van verschillende typen daders, hun primaire motivatie en een voorbeeld van de modus operandi. [8]

Typen daders	Motivatie	Voorbeeld van modus operandi
Natiestaten	Geopolitiek	Stuxnet: worm die kerncentrales in Iran onbruikbaar maakte, zie bijvoorbeeld [89]
(Cyber)criminelen	Financieel gewin	DarkSide Group: hack op de Colonial Pipeline voor losgeld, zie bijvoorbeeld [51]
Hacktivists	Ideologie	DDoS aanval op Scientology door Anonymous. Zie bijvoorbeeld [90]
Terroristische organisaties	Ideologisch geweld	Stelen van militaire en overheidsinformatie en doorspelen naar ISIS door Th3Dir3ctorY. Zie bijvoorbeeld [91]
Sensatiezoekers	Voldoening	LulzSec die een Sony hack plaatsten en onuitgebracht materiaal vrijgaven. Zij hanteerden het motto: *The world's leaders in high-quality entertainment at your expense.* Zie bijvoorbeeld [92]
Ontevreden (ex-)medewerker	Wraak	Hack waarbij een ontevreden oud-medewerker Office365 profielen van medewerkers verwijderde. Zie bijvoorbeeld [93]
Tieners	Nieuwsgierigheid	Tiener die zijn technische vaardigheden wil testen en tentoonstellen door een bank te hacken, zie bijvoorbeeld [94]
Daders van ander typen misdrijven	Rookgordijn creëren	Organisatie of medewerkers installeert ransomware op het eigen netwerk om te voorkomen dat gevoelige of financiële informatie wordt gevonden of om bewijs te verbergen, zie bijvoorbeeld [95]

[8] Bron integrale analyse van literatuur (onder meer [85]) en input uit interviews

5 Risicofactoren voor ransomware-aanvallen

De vierde en vijfde onderzoeksvraag zijn: *Welke interne en externe factoren dragen bij aan ransomware-risico's voor een organisatie? In hoeverre zijn deze factoren kwantificeerbaar?*

Bij interne factoren gaat het over aspecten waar het mogelijke slachtoffer zelf controle over heeft. Voor het onderzoeken van de interne factoren is gekeken naar literatuur, (cyber)risicotaxatietools en cybersecurityverzekeringen. Door te tellen hoe vaak factoren in deze verschillende bronnen voorkomen is gekwantificeerd hoe groot deze risicofactor is. De onderstaande tabel toont de tien interne factoren die het vaakst in deze drie bronnen benoemd worden, gerangschikt naar omvang van de risicofactor. Een generieke interne risicofactor die de onderstaande factoren overkoepelt is het niet goed in kaart hebben welke systemen gebruikt worden. De uitkomsten zijn geverifieerd met interviews.

1. Geen goede back-up | fase: herstellen
2. Onvoldoende training medewerkers over phishing, scams, etc. | fase: voorkomen
3. Software is niet up-to-date | fase: voorkomen
4. Niet hebben van een incident respons plan | fase: herstellen
5. Onvoldoende gebruik van (up-to-date) anti malware oplossingen| fase: voorkomen
6. Onvoldoende privileged access strategy | fase: beperken
7. Onvoldoende beveiligde accounts | fase: voorkomen
8. Onvoldoende continue monitoring | fase: beperken
9. Onvoldoende netwerksegmentatie | fase: beperken
10. Onvoldoende e-mailsecurity | fase: voorkomen

Naast de bovenstaande lijst is er een flinke serie met andere factoren die minder vaak benoemd worden. Dit zijn veelal technische maatregelen om te voorkomen dat infecties plaats kunnen vinden.

Bij externe factoren gaat het om de eigenschappen waar het mogelijke slachtoffer geen of beperkt controle over heeft. In lijn met de verschillende soorten impact die aanvallen op organisaties hebben komt hier naar voren dat de volgende aspecten de verwachte opbrengst voor daders (en hiermee het risico voor slachtoffers) verhogen (1) het hebben van een hogere omzet, (2) de inzet van IT-systemen waarvan uitval de bedrijfscontinuïteit kan verstoren en (3) de opslag van persoonsgegevens. Het hebben van een geschiedenis in het betalen van losgeld kan het risico voor organisaties mogelijk ook verhogen, al verschillen de meningen van experts op dit onderwerp. De volgende twee aspecten verlagen de kosten voor de dader: de lage pakkans en het niet te veel op de radar komen.

5.1 Inleiding

Dit hoofdstuk gaat in op risicofactoren voor ransomware-aanvallen . Deze vallen uiteen in twee soorten risico's. Interne risicofactoren (paragraaf 5.2) zijn de aspecten waar een (potentieel) slachtoffer zelf controle over heeft. De wijze waarop cybersecuritymaatregelen worden getroffen, zijn hier uiteraard het beste voorbeeld van. Daarnaast kijkt paragraaf 5.3 naar externe risicofactoren. Dit zijn eigenschappen van een organisatie waar zij geen (noemenswaardige) invloed op heeft. Denk aan de omvang van de organisatie of de sector waarin zij actief is.

5.2 Interne risicofactoren

Het identificeren en kwantificeren van de interne risicofactoren is een centrale onderzoeksvraag in dit onderzoek en heeft navenant veel aandacht gekregen. Tabel 3 toont een overzicht van de uitkomsten. Hierbij wordt onderscheid gemaakt op basis van de drie fases die ook in eerdere hoofdstukken benoemd werden: (1) het voorkomen van infecties, (2) het beperken van de impact van infecties en (3) het herstellen na een infectie. [9] Per fase zijn de risicofactoren gesorteerd op de mate van relevantie. Voor de kolommen literatuur, cybersecurityverzekeringen en risicotaxatietools geeft de score aan bij hoeveel bronnen een risicofactor werd benoemd, voor de kolom interviews gaat het om de relatieve frequentie. De eerste twee fases zijn niet uniek voor ransomware-aanvallen . Er is veel aandacht voor het voorkomen van aanvallen. Voorkomen is beter dan genezen. Toch is ook het beperken van de impact na de infectie een zeer relevant aspect. Bij grofweg de helft van de infecties kon in 2021 voorkomen worden dat er daadwerkelijk data werd versleuteld. [19] Het herstellen van systemen is in deze analyse redelijk specifiek voor ransomware-aanvallen.

In dit hoofdstuk is het belangrijk om de juiste samenhang tussen de factoren te beseffen. Het is nadrukkelijk niet het geval dat een organisatie zijn risico's goed afdekt als zij de meest waardevolle risicofactor goed afdekt. Organisaties moeten in alle drie fases, verschillende risicofactoren goed afdekken om het risico te beperken. Elke extra stap die genomen wordt, maakt het risico kleiner. Maar het risico volledig uitsluiten is niet mogelijk. Een generieke interne risicofactor die de onderstaande factoren overkoepelt is *het niet goed in kaart hebben welke systemen gebruikt worden*. Alleen als je weet *wat* je moet beveiligen, dan kan je het beveiligen.

Tabel 3. Overzicht van de grootste interne risicofactoren

Fase	Risicofactor	Literatuur	Interviews	Cybersecurity verzekeringen	Risicotaxatietools
Voorkomen	Software is niet up-to-date	18/20	Vaak	5/5	3/5
Voorkomen	Onvoldoende training medewerkers over *phishing, scams,* et cetera	16/20	Heel vaak	5/5	4/5
Voorkomen	Onvoldoende gebruik van (up-to-date) anti malware oplossingen	13/20	Vaak	3/5	4/5
Voorkomen	Onvoldoende beveiligde accounts	10/20	Vaak	3/5	4/5
Voorkomen	Onvoldoende e-mailsecurity	8/20	Soms	1/5	2/5
Voorkomen	Andere, specifieke aspecten	Varieert	Varieert	Varieert	Varieert
Beperken	Onvoldoende *privileged access strategy*	9/20	Vaak	3/5	5/5
Beperken	Onvoldoende continue monitoring	8/20	Vaak	2/5	4/5
Beperken	Onvoldoende netwerksegmentatie	6/20	Vaak	2/5	4/5
Herstellen	Geen goede back-up	18/20	Heel vaak	4/5	5/5
Herstellen	Niet hebben van een *incident respons plan*	7/20	Soms	4/5	5/5

[9] Om een logische clustering van risicofactoren te bewerkstelligen, is deze driedeling gekozen. In de literatuur komen ook andere manieren om deze fases in te delen naar voren. De Amerikaanse standaardiseringorganisatie splitst de eerste fase nog in *identificeren* en *voorkomen* en de twee fase in *detecteren* en *reageren*. [175]. Cyberveilig Nederland werkt met drie gelijksoortige fases die ze IN, DOOR en UIT noemt. [178]

Een manier om het bovenstaande verder te kwantificeren is (1) het uitdrukken van de scores op literatuur, verzekeringen en tools in een percentage en (2) het gemiddelde van deze drie scores nemen. Zo ontstaat een percentage dat uitdrukt hoe vaak een risicofactor gemiddeld benoemd wordt. De onderstaande tabel toont dit overzicht.[10]

Tabel 4. Overzicht van de grootste interne risicofactoren gerangschikt naar gemiddelde frequentie bronnen

Rang	Fase	Risicofactor	Gemiddelde frequentie bronnen
1	Herstellen	Geen goede back-up	90%
2	Voorkomen	Onvoldoende training medewerkers over *phishing, scams,* et cetera	87%
3	Voorkomen	Software is niet up-to-date	83%
4	Herstellen	Niet hebben van een *incident respons plan*	72%
5	Voorkomen	Onvoldoende gebruik van (up-to-date) anti malware oplossingen	68%
6	Beperken	Onvoldoende *privileged access strategy*	68%
7	Voorkomen	Onvoldoende beveiligde accounts	63%
8	Beperken	Onvoldoende continue monitoring	53%
9	Beperken	Onvoldoende netwerksegmentatie	50%
10	Voorkomen	Onvoldoende *email security*	33%

De onderstaande box toont de aanpak voor de bovenstaande analyse.

Box 14. Methodologische verantwoording voor de analyse van de risicofactoren

Om de risicofactoren te identificeren en kwantificeren is gebruik gemaakt van vier onderzoekslijnen: literatuurstudie, interviews, analyse van cybersecurityverzekeringen en een analyse van risicotaxatietools. Deze vier lijnen worden hieronder nader uitgewerkt.

Voor de **literatuurstudie** hebben de auteurs van dit rapport allereerst twintig hoogwaardige bronnen geïdentificeerd waarin de risicofactoren werden benoemd [96] [97] [98] [99] [100] [40] [101] [102] [103] [104] [105] [106] [107] [108] [109] [110] [111] [112] [113] [114]. De selectie van de bronnen is als volgt vormgegeven: Via de zoekmachine Google is gezocht naar bronnen die betrekking hadden op het voorkomen (*prevent*) van ransomware of de risicofactoren (*risk factors*) voor een ransomwarebesmetting. Alleen de URL's die verwezen naar bronnen die een uitvoerige beschrijving gaven en van een respectabele organisatie en/of auteur waren zijn

[10] Merk op dat bij deze methode de drie bronnen (literatuur, verzekeringen en tools) allen even zwaar meewegen. Alle frequenties van literatuur, verzekeringen en tools kunnen ook worden opgeteld en door het aantal bronnen (20 plus 5 plus 5) worden gedeeld. Zo telt literatuur een factor vier hoger mee dan de andere twee bronnen. Het effect hiervan is beperkt, het voornaamste verschil is dat het "niet hebben van een incident respons plan" een drie plekken op de ranking zakt.

geselecteerd.[11] De onderzoekers zijn zich ervan bewust dat een deel van de bronnen geschreven is door marktpartijen die mogelijk een belang kunnen hebben. Op basis van de meest uitvoerigere bronnen zijn definities van risicofactoren bepaald. Het streven hierbij is dat er sprake is van een verzameling risicofactoren die wederzijds uitsluitend en collectief uitputtend (*Mutually Exclusive, Collectively Exhaustive*, MECE) zijn. In de praktijk blijkt dat dit goed werkt, maar in theorie zijn er soms factoren die elkaar overlappen. (Denk bijvoorbeeld aan training voor medewerkers op het gebied van wachtwoorden. Dit kan vallen zowel in de factor *training van medewerkers* als *beveiliging van accounts*.) Een volgende stap die is uitgevoerd is het analyseren van documentatie. Per document is bekeken welke factoren benoemd worden. De uitkomst hiervan is een score per risicofactor tussen de 0 (nooit genoemd) en 20 (in elke bron genoemd). In praktijk waren er enkele iteraties waarbij definities van risicofactoren werden bijgesteld, door het samenvoegen of scheiden ervan. Uit de analyse komt naar voren dat meer dan 20 bronnen weinig tot geen impact op de analyse zal gaan hebben.

In de **interviews** hebben respondenten gevraagd naar de voornaamste risicofactoren voor ransomware-aanvallen . Dit is uiteraard in elk interview aan bod gekomen. Het viel de auteurs van dit rapport op dat veel respondenten dit een flauwe vraag vinden: *Waarom vragen wij dit aan hen als wij dit ook prima kunnen opzoeken?* (Uit de literatuuranalyse blijkt uiteraard dat zij hier gelijk in hebben). Typisch geven zij als spontaan antwoord de meest relevante aspecten die ook uit de literatuurstudie naar voren komen. De auteurs van dit rapport hebben beperkt doorgevraagd of de elementen die zij niet spontaan noemen ook als risico gelden. Op basis van een integrale analyse van de verslagen is ingeschat in welke mate antwoorden gegeven worden.

Voor een analyse van de **cyberverzekeringen** hebben de auteurs van dit rapport gebruik gemaakt van vijf bronnen van verzekeringspolisaanvragen. [115] [116] [117] [118] [119] De reden om verzekeringspolisaanvragen te gebruiken, is dat de auteurs van dit rapport van mening zijn dat het aannemelijk is dat verzekeraars een prima beeld hebben van de (interne) risicofactoren en op basis hiervan verzekeringen afsluiten. De aanvraagformulieren zijn geanalyseerd op basis van de classificatie van factoren die voortkwam uit de literatuurstudie. Het beeld dat uit deze analyse naar voren komt is dat de verzekeraars risico's op gelijke waarde inschatten als de literatuur, met het niet up-to-date hebben van software en onvoldoende phishing training voor medewerkers als voornaamste.

De laatste analyse die de auteurs van dit rapport hebben uitgevoerd, is een analyse van andere **risicotaxatietools**. [7] [8] [9] [10] [11] Deze risicotaxatietools zijn gemaakt om organisaties een beeld te geven van de cyberrisico's die zij lopen. Ten opzichte van verzekeringen, zijn deze tools specifieker gericht op ransomware (en minder op generieke cybersecurity). Daarom ligt in de tools wat meer de focus op het beperken van en herstellen na een ransomware aanval.

[11] De volgende bronnen zijn uitgesloten: (1) alle bronnen die door Google Advertenties worden weergegeven, (2) bronnen die te sterk vereenvoudigd gegevens presenteren en (3) bronnen die overduidelijk alleen tot doel hebben om personen of bedrijven te verleiden om bepaalde diensten af te nemen of producten aan te schaffen.

5.2.1 Voorkomen infectie: Software is niet up-to-date

Het niet up-to-date zijn van software is de grootste risicofactor die wordt benoemd als het gaat om het voorkomen van infecties. Bij deze eerste risicofactor gaat het om generieke software, zoals operating systemen (Windows, MacOS, iOS, Android) maar ook om firmware van apparatuur. Het gaat dus niet om anti-malware software. Aan de lopende band worden er nieuwe kwetsbaarheden gevonden in software. Hiervoor worden door de producenten software updates ("patches") uitgegeven die snel geïnstalleerd moeten worden. Immers, met het bekend worden van de kwetsbaarheid aan de kant van de producent, weten ook kwaadwillende actoren welke kwetsbaarheden er zijn. Om in aanmerking te komen voor een cyberverzekering is het, mede door bovenstaande redenen, een vereiste om binnen een bepaalde tijd (deze kan verschillen per verzekeringsmaatschappij, maar varieert tussen de één en zes maanden) patches en updates door te voeren op kritieke systemen. [120]

In de literatuur wordt er geregeld aandacht besteed aan legacy systemen. Dit zijn oudere systemen waarbij migratie naar nieuwe systemen nog niet uitgevoerd is. Een goed voorbeeld hiervan is Windows XP, waar op dit moment nog ongeveer 0,37% van de Nederlandse systemen op draait. [121] Op dit moment is de ondersteuning voor XP beëindigd. [122] Dat betekent dat er geen patches meer worden uitgegeven en de kwetsbaarheden blijven voorbestaan.

5.2.2 Voorkomen infectie: Onvoldoende training medewerkers over phishing

Bij phishing proberen criminelen via email (maar soms ook SMS, WhatsApp of telefoon) gebruikers te verleiden om *foute links* aan klikken. Dit kunnen websites zijn die zich als een andere website voordoen om zo (inlog) gegevens te stelen. Het kunnen ook links naar bestanden zijn die malware installeren op systemen. Phishing is de meest gebruikte entry point voor een ransomware aanval. Meer dan de helft van de gerapporteerde aanvallen vond plaats via phishing. [123] [46] In Nederland specifiek is dit zelfs 76%. [46] Kleine bedrijven vallen sneller voor phishing e-mails. [46] Medewerkers van een organisatie moeten voldoende kennis hebben om phishing te herkennen. Uit onderzoek blijkt dat één op de drie medewerkers in een organisatie op een phishing link klikt en één op de acht ook daadwerkelijk gegevens gaat invullen. [3] Training kan dit uiteraard terugbrengen, maar nog steeds blijft het risico aanwezig. Zelfs als één persoon de link aanklikt, kan er een risico ontstaan. Mensen blijven in veel gevallen de zwakste schakel in de veiligheidsketen. [44] Om in aanmerking te komen voor een cyberverzekering moet dan vaak ook binnen zes maanden na afsluiting verplicht een privacybewustwordingstraining plaatsvinden. [120]

5.2.3 Voorkomen infectie: Onvoldoende gebruik van (up-to-date) anti malware oplossingen

Een heel evidente manier om malware te voorkomen is het inzet van anti-malware oplossingen. Windows Defender wordt standaard geleverd bij Windows 10 en 11 en biedt als het up-to-date is, redelijke bescherming.[12] [124] Voor servers en andere zakelijke oplossingen zijn uiteraard andere anti-malware oplossingen beschikbaar die geïnstalleerd en up-to-date gehouden moeten worden. Dit wordt ook geëist door verzekeringsmaatschappijen en in enkele gevallen zijn zelfs slechts alleen gerenommeerde antivirusprogramma's afdoende en moeten ze ook geïnstalleerd worden op Apple computers. [120]

[12] De waarin een anti-malware oplossing veilig is, is een dagkoers. De bron beschrijft dat dit systeem op dat moment veilig was, maar dat is uiteraard geen garantie dat dat vandaag of morgen ook het geval zal zijn.

5.2.4 Voorkomen infectie: Onvoldoende beveiligde accounts

Het hebben van onvoldoende beveiligde accounts is uiteraard ook een risicofactor. Het wachtwoordbeleid van een organisatie bepaalt dit voor een deel. Hier spelen vragen als hoe complex moet een wachtwoord zijn (aantal karakters, type karakters) en hoe vaak moet een wachtwoord worden veranderd. Ook moet worden voorkomen dat wachtwoorden voor meerdere toepassingen (zoals websites) worden gebruikt.

Naast wachtwoorden wordt MFA (*multi factor authentication*) de laatste jaren steeds meer gebruikt. [125] Naast iets wat de gebruiker weet (het paswoord en de inlognaam) moet er dan ook toegang worden verkregen door iets wat de gebruiker heeft of is. Een voorbeeld van het eerste zijn telefoons, een bestand of een random reader zoals sommige banken doen. Een voorbeeld van eigenschappen van de gebruikers zijn face scans, vingerafdrukken, iris scans, et cetera. MFA kan voor een flinke verhoging van de veiligheid van accounts zorgen en voor verzekeringsmaatschappijen moeten op alle systemen met externe toegang MFA zijn geïmplementeerd. [120]

5.2.5 Voorkomen infectie: Onvoldoende email security

Email is voorkeursmethode voor veel criminelen om phishing uit te voeren. [126] Het gebruik van email security kan de kans hierop verkleinen. Een methode die kan worden ingezet is SPF. Met dit protocol wordt getracht te achterhalen of de verzenders van een email ook daadwerkelijk gerechtigd zijn om namens een domeinnaam mail uit te sturen. [127] Daarnaast worden ook DKIM en DMARC ingezet om mail veiliger te maken. [128] Een andere manier om mail veiliger te krijgen is het werken met een email security gateway.

5.2.6 Voorkomen infectie: varia

In de literatuur wordt nog een reeks andere factoren genoemd die het risico op een infectie vergroten. De onderstaande tabel geeft hier een overzicht van.

Tabel 5. Minder vaak genoemde risicofactoren

Risicofactor	Aantal keer genoemd
Geen web content filtering (*proxies*, gateways, *safe browsing lists*)	7/20
Geen maatregelen veiligheid MS-Office (in het bijzonder macro's)	6/20
Onvoldoende beveiliging van *endpoints*	6/20
Gebruik van RDP met beperkte beveiliging	5/20
Gebruik en onvoldoende isolatie van *legacy* systemen	3/20
Onvoldoende inzet van *firewalls*	3/20
Gebruik verouderde SMB protocollen	2/20
Geen deelname aan deelprogramma's cybersecurityinformatie	2/20
Geen overzicht van de assets en hun kwetsbaarheden	2/20
Geen third party pentesting	2/20
Geen beperking in de apps die gebruikers kunnen installeren	2/20
Geen *reporting* plan hoe personeel verdachte situatie kan doorgeven	1/20
Gebruik maken van zwakke *managed service providers*	1/20
Geen goede VPN	1/20

Risicofactor	Aantal keer genoemd
Systeembeheerders die hun accounts ook voor mail en *browsing* gebruiken	1/20

5.2.7 Beperken impact: Onvoldoende privileged access strategy

Elke gebruiker van een systeem heeft bepaalde rechten. De minst geprivilegieerde gebruikers kunnen slecht een beperkt deel van de data uitlezen. De meest geprivilegieerde gebruikers kunnen alle handelingen uitvoeren. Het is binnen een organisatie zaak dat er goed wordt nagedacht welke personen (of systemen) welke privileges krijgen. Indien hier niet goed over wordt nagedacht, dan kan dat bijvoorbeeld betekenen dat vanuit elk account alle data kan worden versleuteld (of verwijderd).

5.2.8 Beperken impact: Onvoldoende continue monitoring

Als er een infectie heeft plaatsgevonden dan gaan criminelen aan het werk om hun positie uit te breiden. Ze willen met zo veel mogelijk privileges een zo groot mogelijk deel van het netwerk kunnen controleren en data kunnen exporteren. Tegelijkertijd willen ze ongezien blijven zodat zij hun positie kunnen blijven uitbreiden en hun aanval kunnen timen.[13] Organisaties moeten dus continue in de gaten houden of er zich ongebruikelijk gedrag binnen hun systemen voordoet. Worden er bijvoorbeeld accounts aangemaakt, krijgen accounts een upgrade in privileges, wordt er veel data geëxporteerd, et cetera. Zo kan een aanval worden afgewend of op zijn minst in impact worden verkleind.

5.2.9 Beperken impact: Onvoldoende netwerksegmentatie

Om te voorkomen dat criminelen onbeperkt door systemen kunnen zwerven is het goed als er netwerksegmentatie is. Als er een muur staat tussen twee systemen dan blijft het aanvalsoppervlakte beperkter. Netwerksegmentatie kan worden gerealiseerd door daadwerkelijk een fysieke scheiding aan te brengen, het is echter ook mogelijk om verschillende logische netwerken te definiëren op een fysiek netwerk.

5.2.10 Herstel: Geen goede back-up

Nadat een aanval heeft plaatsgevonden en data is versleuteld is het uiteraard essentieel om een goede back-up te hebben van je data. Belangrijke aspecten hierbij zijn: [129]

- Locatie & media van de back-up volgens de 3-2-1-aanpak. Bij voorkeur drie kopieën, op twee verschillende media waarvan er één op een fysieke andere locatie is opgeslagen.
- Frequentie van de back-up. Als dit te laag is, gaat alsnog veel data verloren.
- Testen van de back-up. Is het werkelijk ook mogelijk om de back-up terug te zetten (en hoelang duurt dat in de praktijk?)

5.2.11 Herstel: Niet hebben van een incident respons plan

Het hebben van procedures hoe om te gaan met incidenten, maakt het voor organisaties veel eenvoudiger om slagvaardig te opereren. De IT-volwassenheid van een bedrijf bepaalt hoelang het duurt voordat een bedrijf weer terug naar normaal is. Slechts 59% weinig

[13] Het is dan ook vast geen toeval dat de ransomwareaanval op Mediamarkt vlak voor Black Friday plaatsvond. [172]

ervaren bedrijven zijn binnen een week terug naar normaal, terwijl 73% van de ervaren bedrijven dit wel zijn. [130]

5.3 Externe risicofactoren

Het vorige hoofdstuk toonde al dat de daders deels gedreven worden door geldelijk gewin en -in vergelijking met andere criminelen- relatief goed afgewogen beslissingen nemen. Vanuit dit perspectief zouden externe risicofactoren kunnen worden geordend door te redeneren vanuit de business case voor de aanvaller: Hoe verhouden opbrengsten en kosten zich? De kant van de opbrengsten bestaat uit de hoogte van het losgeld en de kans dat dit betaald wordt. Uit onderzoek komt naar voren dat de kans op het betalen van losgeld nadat data is versleuteld op ongeveer 30% ligt. [19] Aan de kant van de kosten liggen vooral de personele inzet voor het uitvoeren van de aanval en pakkans. Een grove schatting van de business case laat zien dat gemiddelde opbrengsten per aanval liggen op $140.000, de gemiddelde kosten op $2.500 en het aantal arrestaties per aanval op 0,008. [131]

Aan de andere kant moeten de auteurs van dit rapport ook erkennen dat de insteek van deze paragraaf gebaseerd is op een beeld van volledig rationale aanvallers die weloverwogen beslissingen nemen. Dit verklaart een deel van de externe risicofactoren, maar zeker niet alles. In interviews is aangegeven dat een deel van de aanvallen veel minder weloverwogen en logisch zijn. Criminelen zijn vaak simpelweg opportunistisch en *pakken wat ze snel pakken kunnen*.

5.3.1 Opbrengsten voor de aanvaller

De hoogte van het losgeld en de kans op het betalen van het losgeld kunnen niet los van elkaar gezien worden. De daders hebben een prikkel om de hoogte van losgeld zo in te schatten dat het exact overeenkomt met de *betalingsbereidheid* van het slachtoffer. Als ze het losgeld te laag inschatten, dan lopen ze inkomsten mis. Als ze het te hoog inschatten, dan wordt er niet betaald. Op deze manier doorgeredeneerd, zou vooral gekeken moeten worden naar factoren die de betalingsbereidheid van slachtoffers bepalen. Op basis van het tweede hoofdstuk zouden de volgende factoren naar voren moeten komen: (1) slachtoffers met systemen die een hoge herstelkosten kennen en/of een flinke additionele inzet van ICT-ers nodig hebben bij een ransomware-aanval, (2) slachtoffers die hoge kosten kennen door verlies van data, (3) slachtoffers die hoge kosten kennen bij openbaarmaking van data, (4) slachtoffers die hoge kosten kennen door verstoring van bedrijfscontinuïteit. Nog één aspect moet worden meegenomen: Hoe kan de aanvaller op afstand eenvoudig inschatten hoe groot deze factoren zijn? Aanvallers maken steeds meer gebruik maken van business intelligence en via diensten als Zoominfo informatie over potentiële slachtoffers opvragen. [132] Als bekend is in welke sector een organisatie actief is, wat de omzet van een bedrijf is, hoeveel medewerkers in dienst zijn, dan kan in theorie een aardige inschatting worden gemaakt van de betalingsbereidheid.

Omzet

Hoger de omzet van een organisatie, hoe hoger de totale kosten van een ransomware aanval zijn [38]. Aan de andere kant worden ook kleinere bedrijven steeds vaker slachtoffer worden omdat aanvallen steeds meer geautomatiseerd worden wordt het winstgevender voor criminelen om Mkb'ers aan te vallen. De frequentie van gerapporteerde aanvallen op bedrijven met minder dan 250 werknemers is met 57% toegenomen tussen 2020 en 2021. [123]. Toch worden grote bedrijven relatief vaak aangevallen: Mondiaal bedraagt ongeveer 70% van ransomware aanvallen organisaties met minder dan 1000 werknemers [46], terwijl deze organisaties een kleiner deel van het totaal aantal organisaties uitmaken. In Nederland zijn er bijvoorbeeld ruim 2 miljoen bedrijven, waarvan slechts ongeveer 750 meer dan 1000

werknemers hebben. [133] Ander onderzoek laat zien dat slechts 6% van de aanvaller gericht is op bedrijven met 1 tot 10 werknemers [18], terwijl hun aandeel in de economie veel groter is. [133] Een andere bron laat zien dat de omvang van de organisatie positief samenhangt met de kans op een ransomware-aanval. [19]

Continuïteit

Bedrijven waarbij de uitval van IT-systemen een grote impact heeft op de continuïteit zijn ook extra kwetsbaar. Verschillende geïnterviewden geven aan dat organisaties vaak niet goed bewust zijn van hun eigen kwetsbaarheden als gevolg van de afhankelijkheid van IT. De grootste toename in ransomware aanvallen het afgelopen jaar vond plaats bij bedrijven in de bouw- en maakindustrie. [123] [130] [130] [123] Een reden hiervoor kan zijn dat een interruptie van de werkzaamheden leidt tot zware verliezen, waardoor bedrijven in deze industrieën eerder geneigd zijn om de ransomware *demand* te betalen. [130] Ook andere onderzoeken geven aan dat de maakindustrie een aantrekkelijk doel is doordat de continuïteit kan worden verstoord. [3] De ICT-vaardigheden van een organisatie hebben overigens een flinke impact op de hersteltijd, maar zelfs van de zeer vaardige organisaties is ruim 25% binnen één week niet volledig hersteld van een aanval. [46] Een ander onderzoek laat zien dat de gemiddelde periode waarin bedrijfsoperaties gemiddeld 20 dagen verstoord zijn. [18]

Persoonsgegevens

Het hebben van een grote hoeveelheid persoonsgegevens is een andere risicofactor. Waar in 2018 minder dan 2% van de datalekken voortkwam uit ransomware-aanvallen , is dit nu gestegen naar 10%. [3] Meer dan 10% van de slachtoffers hebben een substantiële boete moeten betalen naar aanleiding van ransomware-aanval en een flink deel hiervan komt voort uit boetes voor het schenden van privacy. [46]

Betalen van losgeld

Het hebben van een historie op het gebied van betalen van losgeld is ook een risicofactor. Ongeveer de helft van de aangevallen organisaties betaalt deze som. [46] Maar aan de andere kant betaalt bijna 20% van de organisaties drie of meer keer losgeld. [46] Uit een andere bron komen vergelijkbare cijfers naar voren, plus de toevoeging dat het in de helft van de gevallen ook nog eens dezelfde daders zijn die opnieuw toeslaan. [47] Het is aannemelijk dat zij worden gezien als partijen waar geld te halen valt. In de interviews komt een opmerkelijk gemengd beeld naar voren. Sommige experts geven aan dat het betalen van losgeld wel degelijk de kans vergroot om opnieuw slachtoffer te worden, andere betwisten dit ten zeerste.

5.3.2 Kosten voor de aanvaller

De voornaamste post die kosten verhoogt ligt uiteraard in de mate waarin organisaties zich wapenen tegen aanvallen. Hoe sterker het fort, hoe duurder het is om binnen te komen. Daarom is vooral de pakkans interessant. Dat is immers de ultieme kostenpost voor een crimineel. Deze pakkans lijkt echter vrij laag te zijn en dat komt deels doordat de daders zich vaak in landen begeven waarin zij niet vervolgd werden. [134] [135] Er wordt gesproken over een pakkans van 0,05%. [136] Recent is echter de REvil groep opgerold door de Russische veiligheidsdiensten en dit lijkt een schok voor de *community van aanvallers* te zijn geweest. [137] Ook in de Oekraïne zijn recent arrestaties geweest van leden van het eGregor kartel, al ging het hierbij om affiliates. [138] In navolging hebben drie grote groepen (Maze, Egregor en Sekhmet) recent hun afscheid aangekondigd en decryptors van vrijgegeven. [139] De inzet van affiliates kan ook gezien worden als een strategie van ransomware ontwikkelaars om buiten schot te blijven. [69]

Wellicht is dit te cynisch, maar ethisch gedrag van de daders zou ook onder kosten geschaard kunnen worden. Enkele geïnterviewde experts zijn sceptisch over de moraal van de aanvallers. Door selectief te zijn in hun gedrag, blijven ze wat meer uit de schijnwerpers**.** De tijden dat REvil toenmalig president Trump om $42 miljoen losgeld vroeg [140] zijn wellicht verleden tijd. Er kan gesteld worden dat zij, door zich voorzichtiger op te stellen, voorkomen dat ze te hard worden aangepakt.

6 Beleidsopties om risico's te verkleinen

De zesde en zeven onderzoeksvragen luiden: *Met welk instrument kunnen bestuurders in middelgrote en kleine organisaties bewust worden gemaakt van de risico's van ransomware?* en *(Hoe) kunnen de vastgelegde factoren worden gebruikt in dit instrument?*

Uit onze analyse komt naar voren dat een bewustwordingscampagne voor bestuurders van kleine en middelgrote organisaties waarschijnlijk een doelmatig en doeltreffend instrument is om de kans op en de impact van ransomware-aanvallen te verminderen. Op dit moment worden zowel het risico als de impact van deze aanvallen onderschat door bestuurders van organisaties. De ICT-ers zijn zich veel beter bewust hiervan, maar blijkbaar wordt dit onvoldoende overgebracht op de bestuurders van deze organisaties. Omdat grote organisaties hun zaken op dit gebied vaak beter op orde hebben (en omdat ze vaak in een heel specifieke context opereren) is het logisch om de focus op middelgrote en kleine organisaties te leggen. Een goede campagne zou de volgende elementen moeten bevatten:

- De campagne moet confronterende feiten bevatten, zoals de gemiddelde schade die slachtoffers ervaren.
- Bestuurders moeten worden geprikkeld om stil te staan bij hun eigen situatie. Dat kan door ze te vragen wat het effect op hun organisatie is als (1) alle gegevens openbaar worden of (2) ICT drie weken niet gebruikt kan worden of (3) losgeld betaald moet worden ter grootte van bijvoorbeeld 5 procent van de omzet.
- De campagne moet concrete handelingsperspectieven bevatten door duidelijk te maken hoe en wat een organisatie minstens op orde moet hebben om goed beschermd te zijn tegen ransomware-aanvallen . De interne risicofactoren sluiten hier goed bij aan.
- De inhoud van de campagne moet actief onder de aandacht gebracht worden en bestuurders moeten een persoonlijk gerichte boodschap ontvangen. Hiervoor zijn verschillende kanalen mogelijk, maar het lijkt zinnig om aan te sluiten bij bekende relaties van de bestuurder zodat er een betrouwbare en bekende bron wordt gehanteerd.
- Door de hoge mate van heterogeniteit van deze doelgroep lijkt een sectorale aanpak voor de hand te liggen. In combinatie met het vorige punt zouden branche- en sectororganisaties een belangrijke rol kunnen spelen.
- Tot slot kan het presenteren van een sociale norm een krachtig instrument zijn. Bestuurders moeten het gevoel krijgen dat vergelijkbare organisaties ook stappen nemen om zich te beschermen tegen ransomware.

Er zijn uiteraard ook andere mogelijkheden om gedragsverandering en bewustwording te bereiken. Zo zou een bepaald niveau van cybersecurity kunnen worden afgedwongen door klanten, leveranciers, verzekeraars of zelfs de overheid. Dit kan gelden voor zowel ICT-dienstverleners als reguliere organisaties.

6.1 Inleiding

Dit hoofdstuk draait om het bepalen van beleidsopties om risico's te verkleinen. In paragraaf 6.2 komt de meest efficiënte focus van beleid aan bod. Hier komt aan de orde waarom de focus juist zou moeten liggen op (1) bewustwording van (2) bestuurders van (3) middelgrote en kleine organisaties. In paragraaf 6.3 wordt de theorie achter bewustwordingscampagnes besproken. In paragraaf 6.4 komt de vertaalslag naar aanbevelingen voor een concrete bewustwordingscampagne met betrekking tot ransomware naar voren. Tot slot worden alternatieve aanpakken besproken.

6.2 Bepalen meest efficiënte beleidsfocus

In deze paragraaf gaan we in op de huidige risicoperceptie met betrekking tot ransomware-aanvallen . Hierbij komen we tot de conclusies dat een focus op een bewustwordingscampagne voor bestuurders van middelgrote en kleine organisaties een logische insteek is. Op deze manier kan op een efficiënte manier de weerbaarheid met betrekking tot ransomware in Nederland verhoogd worden. Dat betekent nadrukkelijk niet dat we met alleen deze maatregel het probleem volledig oplossen; deze strategie moet vooral gezien worden als "laaghangend fruit".

6.2.1 Waarom een focus op bewustwording?

In de voorgaande hoofdstukken is duidelijk geworden dat zowel de kans op ransomware-aanvallen als de impact hiervan op organisaties groot is. De risicoperceptie van bestuurders van organisaties past echter niet met dit grote risico. In een onderzoek van ABN AMRO ziet slechts zo'n 30% cybercriminaliteit als 'veel' of 'heel erg veel' risico voor de eigen organisatie. [13] Dit sluit aan bij de resultaten van het jaarlijkse cybersecurityonderzoek naar het bewustzijn van Nederlanders rondom cybersecurity. [141] Daarin wordt geconcludeerd dat Nederlanders vinden dat ze goed op de hoogte zijn van hun online veiligheid en de kans laag inschatten dat zij schade ondervinden van online risico's. Ze vinden dat zij het 'al goed genoeg' doen en maken zich beperkt zorgen. Dat laatste heeft ook te maken met prioriteit ('het is niet mijn grootste zorg'), eveneens een veelvoorkomende verklaring gegeven door ondernemers. In de interviews is ook verschillende keren aan bod gekomen dat het bewustzijn ondermaats is. Bij de validatiesessies is dit nader bevestigd. En dat terwijl veel basishygiënemaatregelen relatief snel, makkelijk en goedkoop kunnen worden genomen. Kortom, er is een hoop werk aan de winkel wat betreft bewustwording.

6.2.2 Waarom een focus op het bestuurders?

Nog geen 20% van de ICT-afnemers in het mkb is zeer bezorgd is over ransomware. [44] De partijen die ICT verzorgen voor deze organisaties (de ICT-dienstverleners) denken hier heel anders over: hiervan is bijna 85% zeer bezorgd over dit onderwerp. Op basis van de interviews trekken komen de auteurs van dit rapport eenzelfde conclusie: ICT'ers weten vaak wel degelijk dat er meer gedaan moet worden aan cybersecurity, maar bij bestuurders lijkt de urgentie niet groot genoeg. Zij onderschatten de impact en vooral de kans dat het hen overkomt. Dit heeft als gevolg dat er structureel te weinig middelen worden vrijgemaakt voor het weren van ransomware-aanvallen . Ook dit wordt bevestigd in de door de onderzoekers afgenomen interviews en bij de validatiesessies.

Het probleem ligt dus ook niet zozeer bij het kennisniveau van de ICT'er die verantwoordelijk is voor het op operationeel vlak realiseren van bescherming tegen ransomware-aanvallen . Hoewel ook hier verbeteringen mogelijk zijn, hebben zij doorgaans een redelijk beeld hoe ze een organisatie kunnen beschermen tegen ransomware-aanvallen . Veel maatregelen die in

eerdere hoofdstukken besproken worden vallen in de categorie basishygiëne cybersecurity. Daarnaast zijn er al tal van tools en afvinklijsten waaruit herleid kan worden welke acties nodig zijn voor bepaalde organisaties. Geïnterviewde experts met hand-on ervaring met het oplossen ransomware-aanvallen geven dan ook aan dat bij veel succesvolle ransomware-aanvallen er sprake was van een kwetsbaarheid die heel eenvoudig op te lossen was. Deze kwestie – bestuurders van organisaties maken te weinig middelen vrij voor cybersecurity– raakt dus eerder aan het overtuigen van de bestuurders. Met andere woorden, de ICT'er weet vaak wel dat er meer gedaan moet worden, maar krijgt de bestuurders daar niet van overtuigd.

In de interviews met experts wordt ook aangegeven dat operationele gevolgen van verhoogde veiligheid een drempel zijn voor bedrijven om hierom in te zetten. In veel gevallen betekent het namelijk dat ook de interne gebruiker te maken krijgt met extra drempels. Voor MFA moet ook de telefoon worden gebruikt om in te loggen, er moeten verschillende accounts worden gebruikt, inloggen in bepaalde (fysieke of digitale) omgevingen is niet meer mogelijk, et cetera. Een extra slot op de deur houdt de inbreker wellicht buiten, het betekent ook dat iedereen een extra sleutel moet meenemen en gebruiken.

6.2.3 Waarom een focus op middelgrote en kleine organisaties?

Na een uitvoerige deskstudie en interviewronde is het voor de onderzoekers evident om middelgrote en kleine organisaties als focusgroep te nemen. Grote organisaties hebben hun cybersecurity doorgaans redelijk goed op orde, hebben vaak een eigen IT-afdeling en dwingen soms zelfs bepaalden standaarden af bij hun ketenpartners, denk aan ASML. [5] Middelgrote en kleine organisaties besteden daarentegen hun ICT vaak uit, hebben zelf weinig cybersecuritykennis in huis en hebben een lage risicoperceptie voor wat betreft ransomware-aanvallen . [142] Uit onderzoek van Hogeschool Saxion en de Haagse Hogeschool blijkt bijvoorbeeld dat bij mkb'ers sprake is van een sterke *optimistic bias*, ofwel men is bewust van het risico, maar acht zichzelf veel minder vatbaar om slachtoffer te worden dan anderen. [143] Cybercriminaliteit wordt beschouwd als een groot maatschappelijk risico, maar niet als iets dat hen persoonlijk snel zal overkomen. Tot slot hebben grote organisaties vaker specifieke cybersecurityrisico's, terwijl de meeste middelgrote en kleine organisaties kunnen volstaan met het naleven van de basismaatregelen. [144] In de interviews is ook verschillende keren aan bod gekomen dat een logisch focuspunt ligt op middelgrote en kleine organisaties en in de validatiesessies is dit nader bevestigd.

Overigens is de groep van middelgrote en kleine organisaties een grote en heterogene groep. De verschillen tussen organisaties in deze groep zijn zeer groot: Een snelgroeiend jong bedrijf op het gebied van kunstmatige intelligentie is heel anders dan een organisatie die zich met thuiszorg bezighoudt. Een kinderdagverblijf kent weer heel andere eigenschappen dan een transportbedrijf.

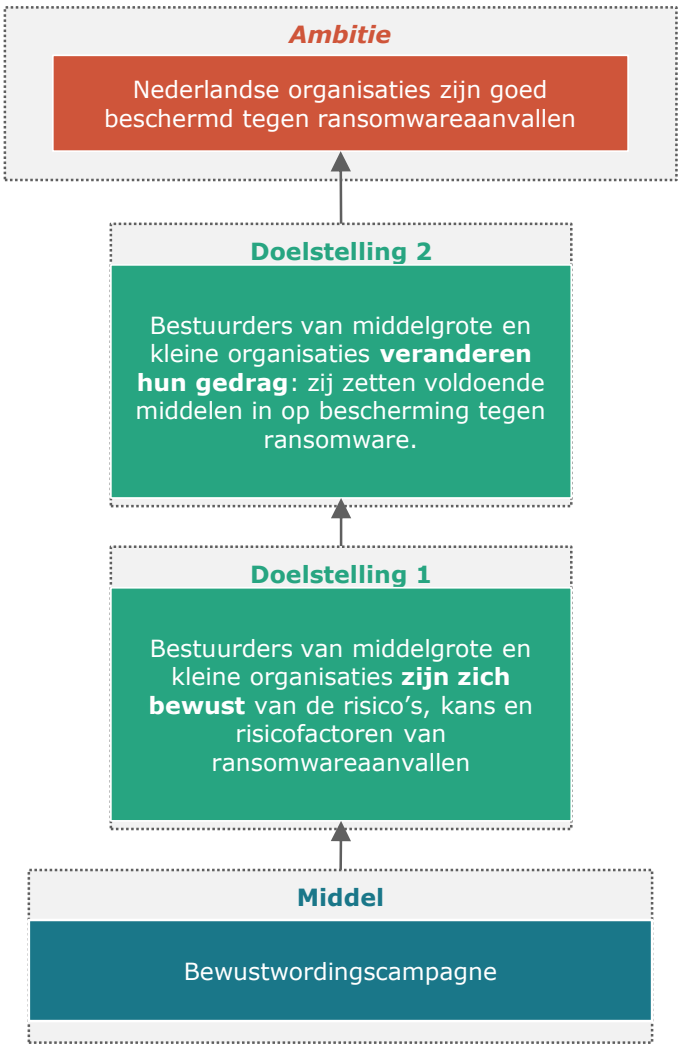
Box 15. Uitkomsten validatiesessies met betrekking tot doelgroep

In de validatiesessies is de vraag aan bod gekomen of de bewustwording van de risico's bij bestuurders van middelgrote en kleine organisaties ondermaats was. Over de hele linie werd dit beeld gedeeld. Daarnaast werden er ook enkele interessante nuanceringen en toevoegingen geplaatst. Zo wordt er aangegeven dat dit probleem ook bij grotere organisaties speelt, al lijkt er wel een positieve correlatie te zijn tussen de mate van bewustwording en de omvang van organisaties. Ook wordt aangegeven dat de mate van bewustwording toe lijkt te nemen over de tijd. Enkele jaren geleden was dit probleem nog groter. Er wordt aangegeven dat bestuurders denken dat de (veelal grotendeels

uitbestede) ICT-afdeling het onder controle heeft, maar hier geen sprake van is. Deze ICT-ers zien de risico's veelal beter, maar kunnen het blijkbaar niet goed voor het voetlicht brengen bij bestuurders. Een andere interessante observatie maakt onderscheid tussen (1) het risico op een aanval en (2) het risico van een aanval voor de organisatie. (Dit laatste noemen we in dit rapport de impact van een aanval.) Er wordt een beeld geschetst dat vooral de mogelijke impact van een aanval wordt onderschat en niet zozeer de kans op een aanval.

6.2.4 Waarom is een bewustwordingscampagne het juiste instrument?

Op basis van de hierboven gepresenteerde redeneringen is het duidelijk dat een ransomwarebewustwordingscampagne gericht op bestuurders van middelgrote en kleine organisaties een doelmatige en doeltreffende methode kan zijn om het aantal ransomware-aanvallen en impact hiervan te verminderen. Dat wil nadrukkelijk niet zeggen dat allerlei andere instrumenten (gericht op specifieke kennis voor ICT-ers, gericht op grote organisaties, et cetera) dit niet zijn en hier niet meer op ingezet zou moeten worden. Er kan echter relatief veel bereikt worden door te werken aan de bewustwording en gedragsverandering van de bestuurders in middelgrote en kleine organisaties. In onderstaand figuur is deze redenatie uitgewerkt in een doelenboom.



Figuur 10. Doelenboom ransomware instrument

6.3 De theorie achter bewustwordingscampagnes

Om mensen aan te zetten tot actie zijn verschillende factoren van belang. Risicoperceptie, respons- en zelfeffectiviteit staan aan de basis. In deze paragraaf wordt op basis van literatuuronderzoek kort enkele kernbegrippen beschreven en wordt een blik op de bekendste theorieën geworpen. Tot slot wordt een lijst van elementen gegeven waaraan risicocommunicatie zou moeten voldoen in algemene termen. In de volgende paragraaf wordt de vertaalslag naar ransomware gemaakt.

6.3.1 Risicoperceptie

Risicoperceptie is de wijze waarop mensen risico's interpreteren. [145] Het is de inschatting in hoeverre mensen een risico zien als een bedreiging voor zichzelf, hun familie, hun bezittingen en hun omgeving. Mensen maken de afweging tussen de kans op en de eventuele impact van een risico. Over het algemeen zijn mensen niet goed in het inschatten van risico's. Deze inschatting wordt beïnvloed door het intuïtieve (emotionele) systeem en het analytische (rationele) systeem van de hersenen. Het eerste systeem is snel, vaak onbewust en zorgt voor gevoelens als angst en bezorgdheid die mensen ervaren als ze bijvoorbeeld denken aan risico's. Het tweede systeem is langzamer en beredeneert risico's op basis van logica en rationaliteit. [146] Bij het verwerken van informatie kunnen beide of een van de twee systemen actief zijn. Het over- of onderschatten van risico's komt over het algemeen voort uit het intuïtieve systeem. Bij een directe confrontatie (bijv. een slang) reageert dit systeem accuraat, bij een indirecte confrontatie (bijv. statistiek die de kans geeft op het tegenkomen van een slang) is dit systeem onnauwkeuriger. Zo maken aangrijpende gebeurtenissen meer indruk (bijv. vliegtuigrampen) en lokken daardoor te veel reactie uit van het intuïtieve systeem. [147] Dit leidt tot een te hoge risicoperceptie voor dat specifieke risico. Terwijl alledaagse gevaren minder indruk maken (bijv. auto-ongelukken), waardoor hiervoor juist een te lage risicoperceptie ontstaat. Het intuïtieve systeem is tevens actiever als iemand moe is. [148] Na een lange dag is de kans daardoor ook groter dat iemand een verkeerde beoordeling maakt en bijvoorbeeld een *phishing mail* minder snel herkend. Hoe context iemands risicoperceptie beïnvloed wordt ook goed geïllustreerd in een klassiek experiment van Tversky en Kahneman, zie Box 16. Iemands risicoperceptie bepaalt (deels) hoe iemand zich gedraagt. Zowel een te hoge als te lage risicoperceptie zorgt ervoor dat mensen minder geneigd zijn om actie te ondernemen. [149] Bij een te lage risicoperceptie voelen mensen niet de noodzaak om actie te ondernemen en bij een te hoge risicoperceptie voelt het alsof het geen zin heeft om er nog iets aan te doen.

Box 16. Experiment Tversky en Kahneman (1979)

Een klassiek experiment van Tversky en Kahneman (1979) toont aan dat de inschatting van risico's relatief is; de context is belangrijk. [150] Zij schetsten een fictieve situatie met 600 eilandbewoners die getroffen zouden worden door een epidemie. Er waren twee condities; een scenario met een verliesperspectief en een scenario met een winstperspectief. Vanuit het verliesperspectief werd aangegeven dat respondenten konden kiezen voor medicijn A (leidt tot het overlijden van 400 mensen) of medicijn B (33% kans dat niemand sterft en 67% dat alle mensen sterven). De meesten (78%) kozen voor medicijn B. Vanuit het winstperspectief werd aangegeven dat respondenten konden kiezen voor medicijn A (het redden van 200 levens) of medicijn B (33% kans dat 600 mensen overleven en 67% kans dat niemand kan worden gered). Hoewel feitelijk dezelfde risico's worden gepresenteerd, koos de meerderheid nu niet voor medicijn B. Slechts 28% koos voor deze optie.

Dit experiment toot aan dat vanuit een verliesperspectief mensen meer risico nemen en vanuit een winstperspectief mensen risicomijdend zijn. Hieruit blijkt hoe belangrijk communicatie is: Wordt het onderwerp vanuit een perspectief van winst of verlies gepresenteerd? [151]

6.3.2 Respons- en zelfeffectiviteit

Het geloof dat een handeling effectief is in het verminderen van een risico of de gevolgen van het risico wordt responseffectiviteit genoemd. Bij een lage responseffectiviteit geloven mensen niet dat een handeling helpt en zullen ze minder geneigd zijn om deze handeling uit te voeren. [152] Denk hierbij bijvoorbeeld aan het dragen van een gordel in de auto. Als mensen niet overtuigd zijn dat een gordel dragen bijdraagt aan de veiligheid, dan zullen ze deze ook niet omdoen.

Het vertrouwen in eigen bekwaamheid om met succes invloed uit te oefenen op een situatie wordt zelfeffectiviteit genoemd en is een essentieel element in theorieën over gedragsverandering. Bij een lage zelfeffectiviteit geloven mensen niet dat ze in staat zijn om handelingen daadwerkelijk uit te voeren en zullen ze minder geneigd zijn om het te proberen. [152] Om het voorbeeld van de rookmelder aan te halen; als mensen niet geloven dat ze in staat zijn om een rookmelder te installeren of de kennis te vinden hoe een rookmelder geïnstalleerd kan worden, dan zal men geen rookmelder installeren ter preventie.

Beide zijn dus kernbegrippen wanneer het doel is om mensen te motiveren hun gedrag te veranderen. Hebben ze vertrouwen dat de handeling nut heeft en denken ze in staat te zijn deze uit te voeren?

6.3.3 Verklaringsmodellen uit de literatuur

Verschillende modellen zijn toonaangevend op het gebied van gedragsverandering.[14] Waar de klassieke modellen[15] intentie als centrale factor voor gedragsverandering plaatsen, leunen de nieuwere theorieën minder sterk op deze verklaring. En niet zonder reden. Een meta-analyse liet zien dat ondanks positieve intentie om condooms te gebruiken, te laten screenen op kanker of om meer te bewegen gemiddeld maar de helft van de mensen deze intentie omzette in daadwerkelijk gedrag. [153] In de jaren daarop werden delen van de klassieke theorieën verworpen en ontstonden er variaties en nieuwe theorieën over gedragsverandering. Een daarvan is de *Protection Motivation* theorie, zie de onderstaande box. Deze theorie is complexer en gaat uit van meer, zowel positieve als negatieve, invloeden op gedragsverandering. De theorie wordt nog veel gebruikt in gezondheidsonderzoek, maar heeft ook zijn weg gevonden tot andere wetenschapsvelden. De eerder uitgelegde begrippen respons- en zelfeffectiviteit zijn eveneens opgenomen in dit model. Ook het *Extended Parallel Process Model* is interessant om naar te kijken, zie de onderstaande box. Dit model is een veelgebruikt *framework* voor effectieve risicocommunicatie en besteed ook aandacht aan 'kop in het zand'-steken gedrag.

---

[14] Disclaimer: Modellen over gedrag hebben altijd voor- en tegenstanders. Dit komt omdat gedrag nooit 1-op-1 te verklaren is. Bovendien zijn er nog vele andere modellen te vinden over gedragsverandering, die nuttig hadden geweest om hier te benoemen. Er is gekozen om de drie modellen te beschrijven die volgende de onderzoekers het beste passen in de context.

[15] Zoals het *Transtheoretical model of behavior change*, de *Rational Choice Theory* en de *Theory of planned behavior*.

Box 17. Verklaringsmodellen

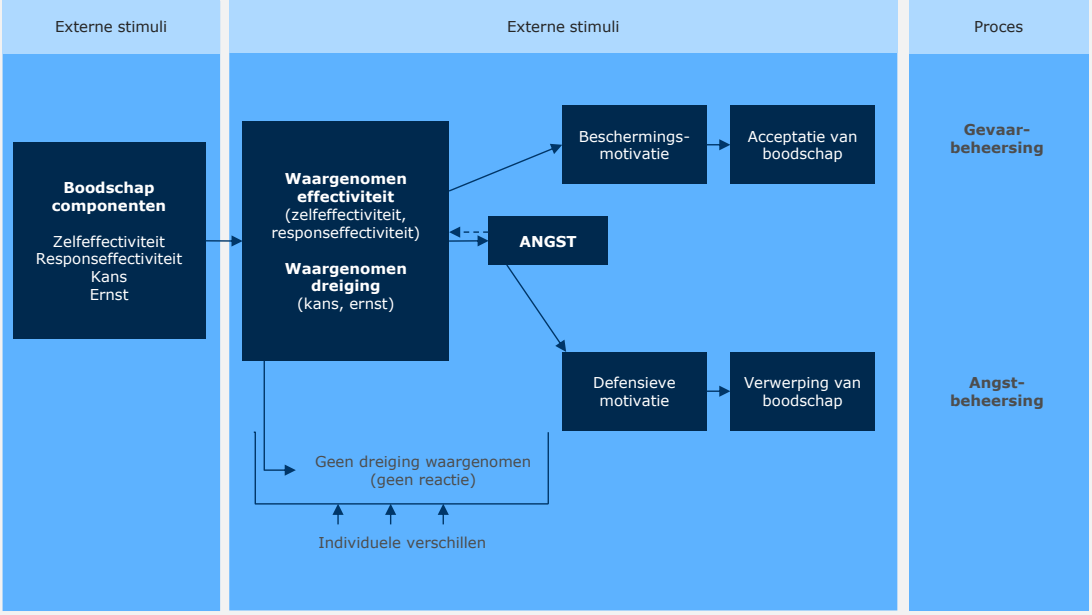
Protection Motivation Theory

De *Protection Motivation Theory* (PMT) gaat over hoe mensen omgaan met en beslissingen nemen in tijden van schadelijke of stressvolle gebeurtenissen. [154] Het legt uit en voorspelt wat mensen motiveert om hun gedrag te veranderen en zich te beschermen tegen waargenomen bedreigingen. Het gaat uit van twee cognitieve processen: 1) Bedreigingsbeoordeling (*threat appraisal*) gaat over hoe bedreigd iemand zich voelt door een risico. Het wordt afgeleid aan de hand van de ervaren kwetsbaarheid, de ervaren ernst van het risico en beloningen die het gedrag opleveren. 2) *Coping* beoordeling (*coping appraisal*) gaat over de evaluatie van factoren die zorgen voor een actie. Dit is een optelsom van de responseffectiviteit (*respons efficacy)*, zelfeffectiviteit (*self-efficacy)* en responskosten (de kosten die verbonden zijn met de uitvoering van een actie). De theorie gaat ervan uit dat een actie voortkomt uit het geloof dat er een ernstige bedreiging is die zich waarschijnlijk zal voordoen en dat door een bepaalde actie te nemen deze bedreiging effectief verminderd kan worden. De persoon moet daarnaast geloven dat hij/zij in staat is om het gedrag uit te voeren.

De bovenstaande afbeelding is een bewerking van een afbeelding uit een publicatie van [154].

Extended Parallel Process Model

Dit model is een veelgebruikt *framework* voor effectieve risicocommunicatie. Het Extended Parallel Proces Model stelt dat de ontvanger van de risicoboodschap eerst de ernst van het gevaar inschat evenals zijn persoonlijke kwetsbaarheid daarvoor. Als er geen relevante dreiging is, vindt er geen verdere verwerking plaats en negeert de persoon de boodschap. Als de persoon wel een relevante dreiging ziet, wordt deze bang en probeert hij de effectiviteit van de aanbeveling in te schatten (werkt de aanbeveling en kan ik de aanbeveling adequaat toepassen?). Als de persoon meent dat de aanbeveling effectief is én hij dit kan toepassen dan zal hij de aanbeveling gaan uitvoeren om de dreiging tegen te gaan. Als de persoon echter twijfelt aan de effectiviteit van de aanbeveling of twijfelt of hij het op de juiste wijze kan uitvoeren en volhouden, dan zal hij de aanbeveling niet uitvoeren. Hij zal zijn (cognitieve) inspanningen vooral gaan richten op het verminderen van angstgevoelens en doet dit door de boodschap te ontkennen of te vermijden. De EPPM stelt verder dat persoonlijkheidsverschillen zowel de perceptie van dreiging als de perceptie van eigen effectiviteit kan beïnvloeden.



De bovenstaande afbeelding is een bewerking van een afbeelding uit een publicatie van [152].

6.3.4 Risicocommunicatie en gedragsverandering

Risicocommunicatie is de voorlichting en communicatie over een mogelijke ramp, crisis of risico. [147] Risicocommunicatie wordt door de Rijksoverheid gedaan via campagnes, zie de box aan het eind van deze pararaaf voor enkele voorbeelden. Het is een uitdaging om risico-informatie te verstrekken die vragen beantwoordt, aansluit bij de kennis die er al is, en die zorgen goed verwoordt. [155] Om gedragsverandering te bewerkstelligen, is het van groot belang om in deze communicatie concrete handelingsperspectieven op te nemen. Een effectieve strategie is bijvoorbeeld laten zien hoe mensen het aanbevolen gedrag goed kunnen uitvoeren. [156] Dit heeft invloed op de respons- en zelfeffectiviteit van mensen.

Vaak is het nodig om daarbij eerst in te spelen op de risicoperceptie van mensen. Hoe beter mensen een risico kunnen inschatten en inzien wat de risico's van bepaald gedrag zijn, hoe groter de kans is dat zij verstandig gedrag laten zien. Denk bijvoorbeeld aan appen in de auto of stoppen met roken. Het analytische systeem in de hersenen moet worden aangesproken om kennis over te brengen en het nut van beschermende maatregelen in te zien, en het intuïtieve systeem is nodig om mensen aan te zetten tot bepaald gedrag. [147] Hierbij is het goed om te beseffen dat gedragsintentie niet altijd leidt tot gewenst gedrag. De context waarin gedrag plaats vindt, bijvoorbeeld locatie, gezelschap en gelegenheid, beïnvloeden wel degelijk. [157] Mensen zijn moe, hebben gedronken, worden omgepraat, zijn afgeleid en kunnen dan (tijdelijk) geen motivatie meer hebben om bepaald gedrag te laten zien. Bovendien worden keuzes doorgaans gemaakt op basis van impuls of gewoonte, zeker als een sterke overtuiging ontbreekt.

Daarnaast is de sociale norm van belang. Daarmee kan worden ingespeeld op het gevoel tot conformisme. Mensen zijn geneigd om in bepaalde situaties hun gedrag te conformeren aan dat van anderen en wel om twee redenen: omdat mensen niet weten wat het juiste gedrag is en daarvoor ter informatie naar anderen kijken, of omdat ze graag bij anderen willen horen en daarom hun gedrag willen aanpassen. [157] Conformisme als beïnvloedingsmechanisme werkt goed bij onzekerheid (niet zeker weten welk gedrag goed is) en gelijksoortigheid (*peers*). Het communiceren van een descriptieve norm (het gedrag van *peers* laten zien) of

injunctieve norm (het gedrag dat *peers* zouden moeten laten zien) stimuleert conformisme naar het gecommuniceerde gedrag.

Binnen de overheid is er steeds meer aandacht voor gedragseffecten via campagnes. [157] Campagnes hadden vaak als hoofddoel het vergroten van kennis of draagvlak, maar er vindt sinds een jaar of tien een verschuiving plaats om de focus van campagnes op gedragsverandering te leggen. In theorie wordt er dan bij de opstart van campagnes meer structureel nagedacht over gedragsanalyses en dient er bij het formuleren van doelstellingen van een campagne rekening gehouden te worden met de potentie voor gedragsverandering. Uit een meta-analyse blijkt dat preventiecampagnes aanzienlijk minder effectief zijn dan naleving- of handhavingscampagnes (bijv. alcohol in het verkeer). [158] Respectievelijk vertonen gemiddeld 3% tegenover 17% van de mensen het gewenste gedrag. Daarnaast blijkt dat het succes van een campagne afhankelijk is van of het gericht is op een eenmalige gedragsverandering (bijv. donorregistratie) of gewoontegedrag (bijv. nooit meer alcohol drinken achter het stuur). [159] Eenmalig gedrag teweegbrengen is makkelijker dan structureel gedrag bij mensen te veranderen. Het ontwikkelen van effectieve risicocommunicatie gericht op preventie en gewoontegedrag is dus niet eenvoudig.

In een wat ouder, maar nog steeds relevant onderzoek naar Postbus51-campagnes is gekeken naar welke beïnvloedingsmechanismen gebruikt worden en langs welke route in de hersenen de informatieverwerking plaats vindt (centraal, intuïtief of analytisch). [157] De meest gebruikte beïnvloedingsmechanismen in 2010 en 2011 waren het bieden van concreet handelingsperspectief, het tonen van gedrag van anderen en (ondersteunend) het gebruik van *fear appeal* (oproepen van angst) en humor. Bewustwording is ook een van de ingezette beïnvloedingsmechanismes. Vaak wordt deze in combinatie met concreet handelingsperspectief ingezet. Het ongewenste gedrag wordt aangegeven en een alternatief, gewenst gedrag wordt geboden. Dit blijkt een redelijk succesvolle combinatie, met name in veiligheidscampagnes.

Box 18. Succesvolle en minder succesvolle overheidscampagnes

Voorbeeld van een succesvolle overheidscampagne

De BOB-campagne loopt in Nederland sinds 2001 (het oorspronkelijke idee voor de campagne is van het Belgisch Instituut voor de Verkeersveiligheid) en is inmiddels uitgegroeid tot een bekend begrip. [160] Hier wordt gebruik gemaakt van altercasting, er wordt een rol bedacht waar bepaald gedrag aan wordt gekoppeld. Dat maakt het makkelijker voor mensen om een bepaalde rol te accepteren en om alcohol te laten staan.

De BOB-campagne is in 2020 geëvalueerd. [161] Er worden positieve korte en lange termijneffecten geconstateerd. Zo wordt de campagne goed herkend en zijn steeds meer automobilisten van plan om tegen anderen te zeggen dat zij de BOB zijn. De campagne wordt door automobilisten daarnaast bovengemiddeld gewaardeerd met een cijfer 7,7. Kortom, deze campagne is erin geslaagd haar boodschap over te brengen.

Voorbeeld van een minder succesvolle overheidscampagne

Borden met social media-iconen en een oproep om deze alleen te checken op een parkeerplaats. Dit lijkt op het eerste gezicht een goede campagne, maar geeft een verkeerd beeld af. Dit heeft te maken met *priming*: als je iets ziet wordt het concept actiever in je hoofd. Het onderbewustzijn wordt geprikkeld om juist wél aan deze zaken te denken en er potentieel zelfs mee bezig te gaan. [160]

6.3.5 Waar moet goede risicocommunicatie aan voldoen?

Er is een aantal belangrijke elementen waar succesvolle risicocommunicatie aan moet voldoen, volgens de hierboven beschreven theorie. Een overzicht van deze elementen is te zien in Tabel 6.

Tabel 6. Samenvatting van de elementen die van volgens de literatuur van belang zijn bij risicocommunicatie

Relevant element	Type	Concrete eis aan risicocommunicatie
Sociale norm	Contextueel	Een duidelijke sociale norm moet worden gepresenteerd in de boodschap. Op die manier kan worden ingespeeld op de menselijke neiging tot conformisme.
Vertrouwen afzender	Contextueel	De bron van een risicoboodschap heeft invloed op hoe de boodschap ontvangen wordt. Het is belangrijk dat de informatie van een betrouwbare en bekende bron komt.
Confronterende feiten	Inhoudelijk	Confronterende feiten zijn nodig om de ontvanger met zijn of haar neus op de feiten te drukken en helpt om de aandacht te vangen en te stimuleren om meer over het onderwerp te weten te komen.
Stilstaan bij eigen situatie	Inhoudelijk	Door de ontvanger van de boodschap stil te laten staan bij zijn of haar eigen situatie, dwing je als het ware een moment van zelfreflectie af waarbij de eigen beleving wordt afgetoetst tegen de risicoboodschap.
Handelingsperspectief bieden	Inhoudelijk	Bij goede risicocommunicatie zijn handelingsperspectieven onmisbaar. Nadat men is overtuigd zijn of haar gedrag te moeten aanpassen, moet ook duidelijk aangegeven worden hoe dat dan kan. Wanneer dit ontbreekt zal de eerdere boodschap worden ontkend of vermeden (verminderen angstgevoelens door 'kop in het zand' te steken).
Verhalen en illustraties	Inhoudelijk	Levendige verhalen over *peers* verhogen de persoonlijke risico-inschatting en maken dat de boodschap beter blijft hangen. Goede risicocommunicatie moet dus verhalen en/of illustraties bevatten.

In de volgende paragraaf worden deze elementen meegenomen en verder uitgewerkt in een concrete ontwerpcampagne voor ransomware.

6.4 Ontwerp van een ransomware-campagne

In de vorige paragraaf is de theorie achter goede bewustwordingscampagnes behandeld. In deze paragraaf wordt deze kennis toegepast op ransomware. Vanuit sociaalpsychologisch perspectief wordt beargumenteerd welke elementen een bewustwordingscampagne moet hebben om succesvol te zijn. Hierbij wordt geput uit de theorie zoals aangehaald in de vorige paragraaf. Dit is aangevuld met de uitkomsten van interviews waarbij we onze voorlopige uitkomsten hebben getoetst middels validatiesessies. We baseren ons dus op de modellen die eerder in dit hoofdstuk zijn gepresenteerd en hebben slechts een beperkte toetsing van deze modellen uitgevoerd. De onderstaande aanpak moet dus gezien worden als een

inventarisatie van mogelijk werkzame elementen op basis van de theorie. Wellicht dat in vervolgonderzoek het onderstaande ontwerp sterker kan worden getoetst.

Zoals in paragraaf 6.2 is besproken, richten deze bewustwordingscampagne zich direct tot bestuurders van middelgrote en kleine organisaties. Dit is de **doelgroep** en dit zijn de personen in de organisatie die de ernst van de situatie moeten gaan inzien en uiteindelijk actie moeten gaan ondernemen. ICT'ers zijn vaak al op de hoogte van de risico's, maar blijken zij tot op heden toch niet voldoende in staat om bestuurders hiervan te overtuigen.

Tot slot merken wij nog op dat de theorie die we hierboven hebben behandeld slaat op de risicoperceptie van individuen. Op managementniveau spelen naar verwachting ook nog andere factoren een rol dan enkel de eigen waarneming van de bestuurder. Wellicht in deze specifieke context communicatie vanuit partners (zoals aandeelhouders, financiers, leveranciers, klanten, et cetera) ook een belangrijke rol spelen. Deze overweging zou eveneens getoetst kunnen worden in eventueel vervolgonderzoek.

De ransomware-campagne zou de volgende elementen moeten bevatten (**inhoud**):

Confronterende feiten

De campagne moet **confronterende feiten** bevatten. Dat kan door een concreet beeld te schetsen van de gevolgen voor vergelijkbare organisaties die eerder slachtoffer zijn geworden van een ransomware-aanval. Bijvoorbeeld: "Bedrijf X uit dezelfde sector als uw bedrijf is slachtoffer geworden van een ransomware-aanval. Er werd €750.000 in bitcoin geëist. Het bedrijf heeft ervoor gekozen niet te betalen. Een groot deel van de data is verloren gegaan en er is nog steeds een risico op publicatie van de data. Het bedrijf is drie weken dicht geweest, maar de totale hersteltijd is vermoedelijk 2 jaar. De totale kosten van de aanval worden op 4 miljoen euro geschat. Het bedrijf staat nu op de rand van faillissement."[16] Door dit verhalend te vertellen (liefst met afbeeldingen), wordt ook voldaan aan het element **verhalen en illustraties**. Bepaalde illustraties beklijven goed, zoals het visualiseren van een pensioenregeling met een zak geld of het vertalen van risico's in de vorm van haaien, zoals op de volgende pagina gebeurt. Levendige verhalen over *peers* verhogen de persoonlijke risico-inschatting ('het kan mij dus ook overkomen').

Er kan ook (aanvullend) worden gekozen voor het presenteren van enkele feiten. Eerder in dit onderzoek werden verschillende losgeldbedragen genoemd. Aanvullend hierop zien we voor Nederland dat een geslaagde ransomware-aanval een Nederlands bedrijf gemiddeld 96.000 euro kost en dat 53% van de slachtoffers het losgeldbedrag betaalt. [162] Daarnaast zijn er natuurlijk nog de indirecte kosten, zoals aansprakelijkheid (o.a. boetes van de Autoriteit Persoonsgegevens), kosten voor de inzet van externe cybersecurityspecialisten, reputatieschade, etc. Zie voor een volledig overzicht van de kosten Figuur 1. Een voorbeeld van een campagne die op deze punten inspeelt is zichtbaar in Figuur 11. Deze infographic is specifiek gericht op zorgorganisaties. De confronterende feiten zijn dan ook gericht op deze sector. Verder is de afbeelding verhalend ingestoken en is direct duidelijk welke consequenties een aanval heeft. Een ander voorbeeld is een campagne van de Zweedse internet security organisatie (SSF) over de kwaliteit van wachtwoorden. In Abri's hingen posters met de meest gebruikte wachtwoorden in Zweden, zoals "*Your password is shit (Shit is the 16th most common internet password used in Sweden.)*" [163] Een ander voorbeeld komt van Hiscox een verzekeraar (van cybersecurityrisico's). Zij maakten in London binnen

[16] Hoewel dit voorbeeld overduidelijk confronterend is, is het te overwegen om een ander voorbeeld te kiezen. Dit zou immers geïnterpreteerd kunnen worden als een aanmoediging om vooral losgeld te betalen. Vanuit een breder perspectief zou het uiteraard het best zijn als niemand ooit losgeld zou betalen, dan zou de business case van criminelen die ransomware inzetten snel onderuit gaan.

één dag een nepwinkel van fietsproducent Brompton (genaamd 3rompton) waar alleen maar illegale goederen verkocht werden. Een clip hiervan is op internet te vinden. [164] SecureOps heeft in 2021 een ransomware infographic gemaakt voor verspreiding, waarbij veel van de eerdergenoemde voorwaarden (o.a. confronterende feiten, verhalen en illustraties en handelingsperspectief) worden aangestipt, zie Figuur 12. Voor alle hier genoemde voorbeelden moeten we echter ook aangeven dat deze -voor zover wij weten- niet op doeltreffendheid geëvalueerd zijn.

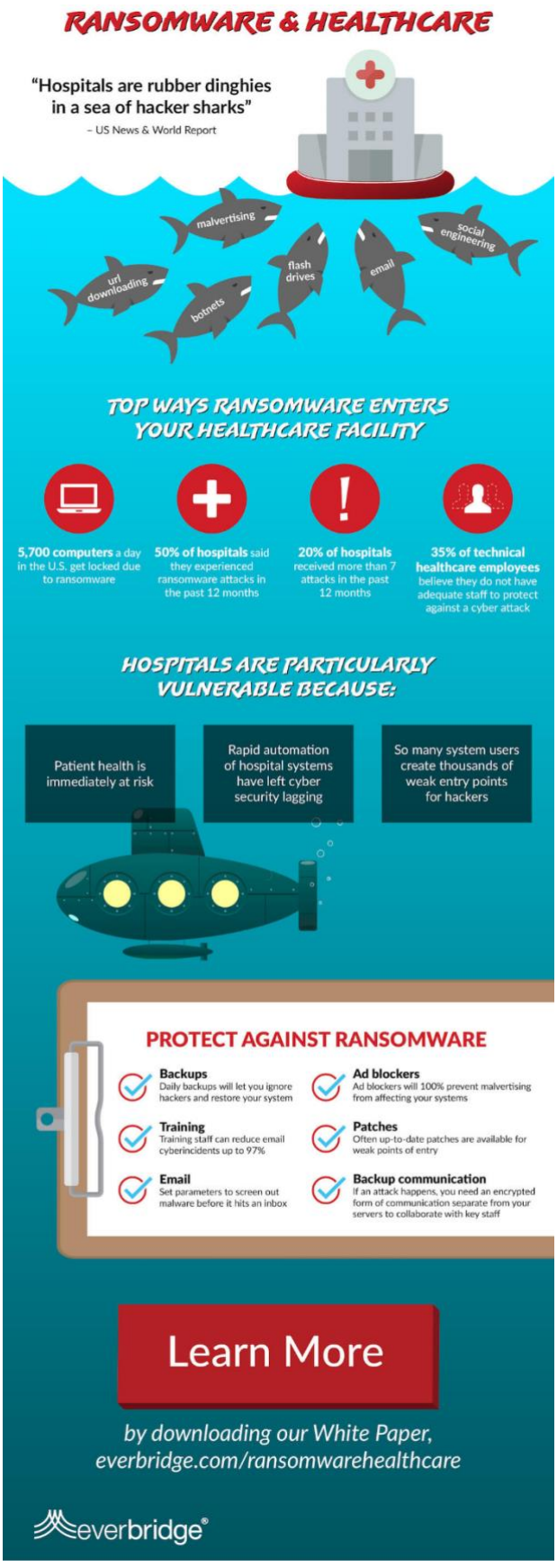
Reflectie op eigen situatie

Bestuurders moeten stilstaan bij hun eigen situatie. Dat kan door ze een aantal vragen te stellen geredeneerd vanuit de risico's:

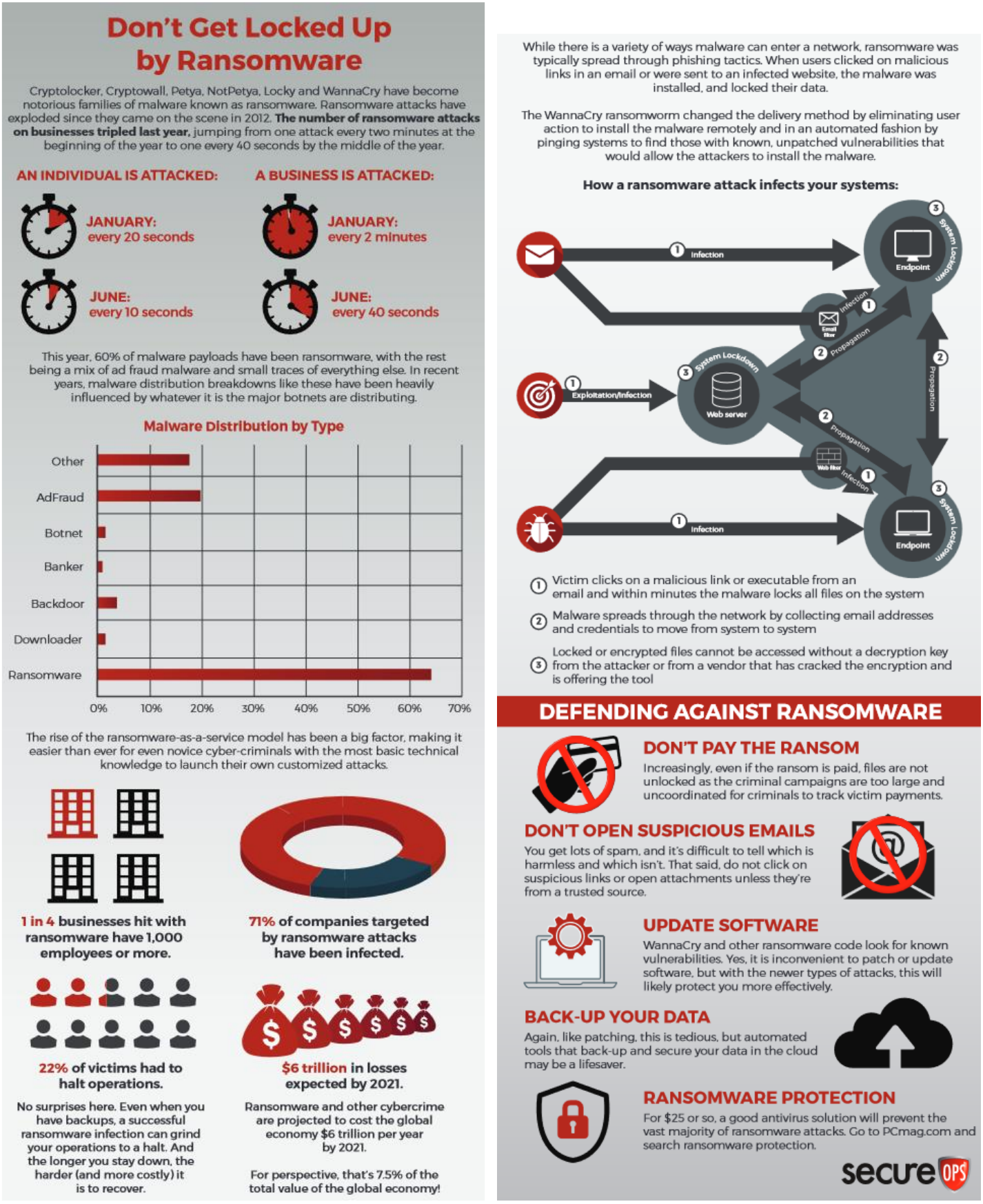
- *Wat is de impact op de organisatie als alle gegevens openbaar worden?*
- *Wat is de impact op de organisatie als ICT drie weken niet gebruikt kan worden?*
- *Wat is de impact op de organisatie als losgeld betaald moet worden ter grootte van 5 procent van de omzet?*

Uit de interviews met cybersecurityspecialisten komt naar voren dat vooral de businesscasebenadering aan lijkt te slaan bij middelgrote en kleine bedrijven. Het is uiteraard ook niet zo vreemd dat bestuurders van deze organisaties redeneren vanuit business cases. Hoewel cybersecurity in organisaties vaak enkel gezien wordt als kostenpost, zouden ook de secundaire voordelen van goede cybersecurity moeten worden meegenomen: een goede audit heeft meerwaarde voor de organisatie, er wordt direct voldaan aan dataprotectie, goede reputatie naar klanten toe en korting op eventuele cyberpolissen. Volgens enkele geïnterviewde cybersecurityexperts is er een ongeschreven vuistregel die voor veel typen en grootten van organisaties opgaat: de kosten voor goede cybersecurity is vaak het dubbele van wat nu wordt betaald.[17] Kortom: als de kwestie van ransomware-aanvallen inzichtelijk wordt gemaakt in termen van een business case, kunnen bestuurders een weloverwogen beslissing maken. En als die business case illustreert hoe een investering van €1 een aanval kan stoppen die de organisatie € 10 zou kosten, zijn bestuurders van bedrijven vaak snel overtuigd. Op internet zijn verschillende voorbeelden te vinden hoe zo een business case te maken. Hoewel de benadering van business cases goed zal aanslaan bij middelgrote en kleine bedrijven, zal dit voor middelgrote en kleine organisaties die geen winstoogmerk hebben (bijvoorbeeld in de zorg of het onderwijs) genuanceerder liggen. Wellicht werkt het bij deze organisaties beter om te verwijzen naar de belangen van hun cliënten (bijvoorbeeld patiënten en leerlingen).

[17] Bij deze uitspraak is het wellicht goed om te beseffen dat veel van deze experts een belang hebben: veel worden ingehuurd worden om deze diensten te leveren.



Figuur 11. Ransomware campagne specifiek gericht op de zorgsector [165]



Figuur 12. Voorbeeld van ransomware campagne. [166] De originele langgerekte afbeelding is hier in twee delen (links en rechts) geknipt om deze beter te kunnen visualiseren.

Bieden van concrete handelingsperspectieven

De campagne moet concrete handelingsperspectieven bevatten door duidelijk te maken hoe en wat een organisatie minstens op orde moet hebben om goed beschermd te zijn tegen ransomware-aanvallen . Men moet weten welke acties ondernomen kunnen worden, hoe deze ondernomen moeten worden en wat het nut ervan is (respons- en zelfeffectiviteit). Voor ICT'ers bestaan er tal van checklists en tools om dit te bepalen (zie bijvoorbeeld Tabel 3). Voor bestuurders zijn er enkele behapbare adviezen: (1) Ga het gesprek aan met de ICT'er(s) of ICT-dienstverlener. Laat een inschatting maken van de risico's; (2) Zet het onderwerp op de agenda van het Management Team; (3) Laat eventueel extra testen doen door een cybersecurityspecialist of laat een businesscase opstellen.

Ook concrete handelingsperspectieven kunnen opgenomen worden in een campagne, of er kan verwezen worden naar waar deze te vinden zijn. Voor een voorbeeld, zie ook Figuur 11.

Vorm en context

Wat betreft vorm en context is de eerste voorwaarde voor een succesvolle bewustwordingscampagne dat mensen de informatie **daadwerkelijk tot zich nemen**. Dat betekent dat het weinig nut heeft om de informatie op een website te plaatsen waar de doelgroep normaal gesproken ook niet op kijkt. De inhoud moet dus actief onder de aandacht gebracht worden. De huidige werkwijze van het NCSC is het publiceren van kennisproducten via een PDF op hun website. Daarbij gaat NCSC uit van een gemotiveerd publiek met pleiters en falers. [12] De pleiter is degene die de *factsheet* downloadt en aan de faler opstuurt om haar argumenten kracht bij te zetten. De faler is de formeel verantwoordelijke die faalt vanuit een cybersecurityperspectief: wat hij doet of nalaat maakt de organisatie onveiliger. Dat sluit aan bij de analyse van dit onderzoek, echter zouden de onderzoekers aanbevelen het succes van een advies niet af te laten hangen van gemotiveerde pleiters. De pleiter is in deze zin de overheid die gericht de bestuurders van kleine en middelgrote organisaties wil overtuigen om meer tegen ransomware te doen. De ICT'er als pleiter binnen de organisatie is tot dusver blijkbaar vaak onsuccesvol geweest.

Persoonlijke gerichte boodschap

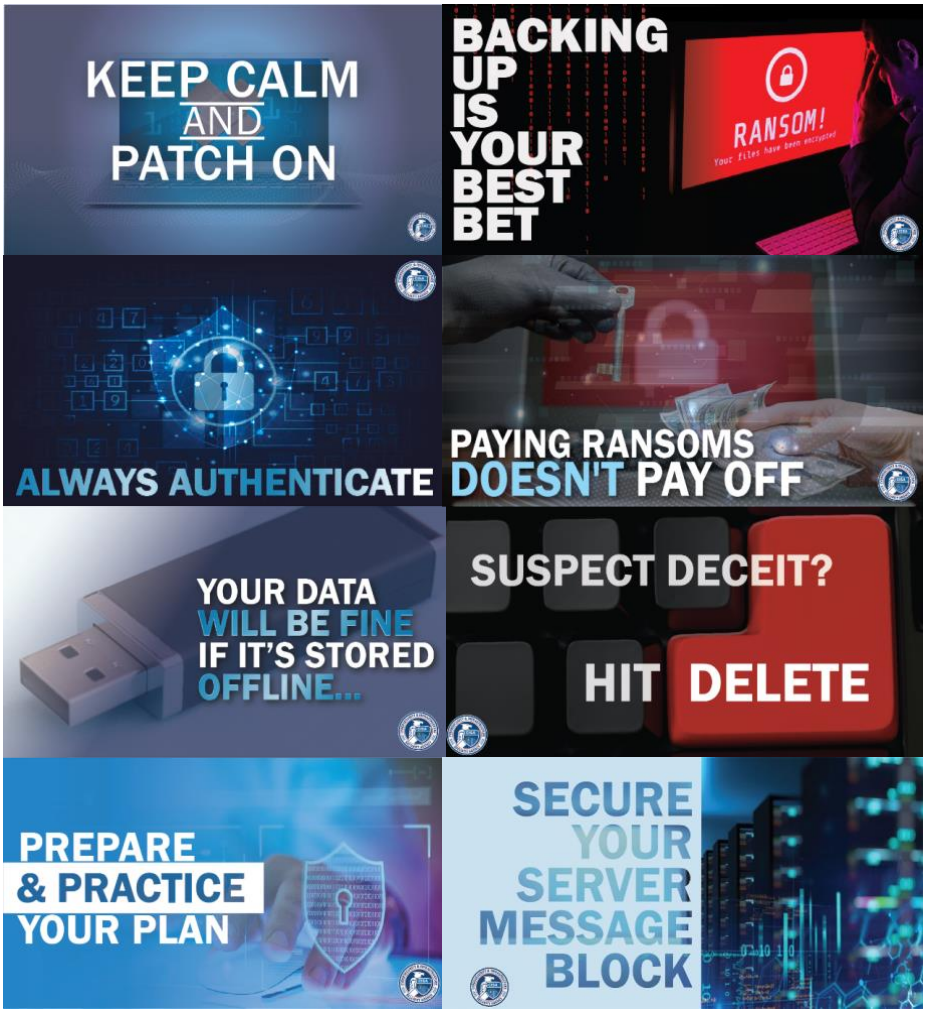
Het belang van een persoonlijk gerichte boodschap moet benadrukt worden. Het gaat om een relatief kleine doelgroep (enkel de bestuurders van midden en kleine organisaties), maar het benaderen hiervan kan lastig zijn. Hun gegevens zijn weliswaar bekend (denk aan inschrijvingen bij de KvK), maar het is de vraag of zij een brief die aan hun organisatie gericht is, ook daadwerkelijk (met interesse) gaan lezen.

Daarbij speelt uiteraard ook de vraag wie deze brief verstuurd heeft. Vanuit de theorie is het van belang dat het een **betrouwbare en bekende afzender** betreft. We zouden ook kunnen redeneren vanuit de actoren waarmee deze bestuurders contact heeft en waar zij vertrouwen in hebben. Wellicht is het een beter idee om deze actoren te gebruiken om de gewenste boodschap naar deze bestuurders te brengen. Voorbeelden van deze actoren zijn: KvK, accountant, verzekeringsmaatschappij (of tussenpersoon), externe ICT-leverancier, bank, toeleveranciers, brancheorganisaties en klanten. Daarbij zou onderscheid moeten worden gemaakt tussen verschillende soorten bestuurders. Bestuurders in het primair onderwijs zouden anders moeten worden benaderd dan eigenaren van een autobedrijf. Wellicht zou de eerste groep het beste via het Ministerie van OCW of Kennisnet worden benaderd, wellicht zou de tweede het beste via de BOVAG worden benaderd. [18] Het

[18] Merk op dat de BOVAG samen met MKB-Nederland wel al een digitale campagne heeft voor digitale veiligheid. Voor Kennisnet geldt hetzelfde.

persoonlijk benaderen is echter wel relevant. Door hen persoonlijk aan te schrijven, is de kans groter dat zij de inhoud daadwerkelijk lezen.

Een ander voordeel van gerichte communicatie of *tailoring* is dat het in potentie effectiviteit (want persoonlijk) kan verenigen met efficiency (want interpersoonlijk contact is niet nodig). Er kan dan een onderscheid worden gemaakt naar verschillende typen organisaties. Dat maakt het delen van voorbeelden van *peers* ook een stuk effectiever (zoals hierboven is geïllustreerd). Op basis van het voorgaande is het wellicht een optie om een *white label*[19] *campagne* te ontwikkelen. Verschillende intermediaire partijen die we hierboven benoemd hebben, kunnen dit gebruiken om zelf eenvoudig een campagne voor hun achterban te ontwikkelen. Op die manier is de communicatie afkomstig van een bekende en betrouwbare afzender en kan de inhoud worden aangepast aan de specifieke doelgroep. In deze lijn zien we dat het Amerikaanse Cybersecurity & Infrastructure Security Agency (CISA) een aantal afbeeldingen heeft gemaakt die door haar partners kunnen worden ingezet in campagnes, zie Figuur 13.



Figuur 13. Compilatie van afbeeldingen uit een Ransomware Toolkit voor partners van het Amerikaanse Cybersecurity & Infrastructure Security Agency. [167]

[19] *White label* diensten of diensten worden geproduceerd door een partij, maar door een andere partij op de markt gezet alsof deze hiervan de producent is. In de supermarkt zijn talloze van deze producten te vinden. Maar ook als het gaat om ICT-diensten wordt dit model geregeld toegepast.

Het presenteren van een **sociale norm** kan een krachtig instrument zijn. Door bestuurders het gevoel te geven dat vergelijkbare organisaties ook stappen nemen om zich te beschermen tegen ransomware, wordt ingespeeld op hun gevoel tot conformisme. Een concrete sociale norm kan zijn: "60% van de bedrijven uit uw sector heeft het afgelopen jaar meer geïnvesteerd in cybersecurity. Ga met deze bedrijven in gesprek via het volgende platform [samenwerkingsverband of CERT]".

Box 19. Uitkomsten validatiesessies met betrekking tot campagne

In de validatiesessies is de vraag aan bod gekomen of een bewustwordingscampagne gericht bestuurders van middelgrote en kleine organisaties een goed beleidsinstrument zou zijn. Aangezien over de hele linie het beeld werd gedeeld dat deze groep zich te weinig bewust is van de risico's, wordt aangegeven dat dit inderdaad een goed instrument is. De discussies gingen daarom veel meer over de wijze waarop dit zou moeten worden vormgegeven. In de sessies is bewust initieel als een open vraag gesteld zonder dat de respondent werd gestuurd in een bepaalde richting. In de daaropvolgende discussie zijn de ideeën die in deze paragraaf worden genoemd ook getoetst. Er zijn drie aspecten die heel duidelijk naar voren komen:

1. Het gebruiken van concrete cases van ransomware-aanvallen uit de specifieke sector waarin de bestuurder opereert wordt sterk aangeraden. Hierbij zou de focus niet zozeer moeten liggen op de technische aspecten van de aanval, maar de impact ervan op de getroffen organisatie. Bestuurders zijn gevoelig voor kosten, impact op imago, gegevenslekken, verstoring van de continuïteit.
2. Branche- of sectororganisaties lijken een heel logische partij om de boodschap goed te verspreiden. Deze bestuurders zijn een lastig te bereiken groep, maar deze organisaties genieten het vertrouwen en kunnen de boodschap in de juiste sectorale context plaatsen.
3. Er is een beeld dat een deel van deze bestuurders niet de financiële slagkracht heeft om grote maatregelen te treffen. De focus zou dus moeten liggen op relatief eenvoudige en kostenefficiënte maatregelen. Denk aan het maken van een eenvoudig incident response plan en het op orde brengen van de basishygiëne.

Over het kanaal dat gebruikt moet worden om deze boodschappen te communiceren is duidelijk geen consensus bij de deelnemers aan de validatiesessies. De meningen variëren van een campagne die volledig gericht is op online of exact het tegenovergesteld. Sommige respondenten zijn van mening dat bestuurders juist persoonlijk moeten worden aangesproken, anderen zijn van mening dat het juist indirect (en via de ICT-ers) zou moeten. De auteurs van dit rapport hebben het vermoeden dat de grote heterogeniteit in de doelgroep (bestuurders van middelgrote en kleine organisaties) er toe kan leiden dat voor verschillende soorten bestuurders, verschillende kanalen het meest geschikt zijn.

6.5 Alternatieve aanpak

Om gedragsverandering en bewustwording (zie Figuur 10) te bereiken, zijn overigens diverse routes mogelijk. Een veel bepleite route is het afdwingen van een bepaald niveau van cybersecurity door bedrijven te verplichten te voldoen aan de standaarden van CIS.[20] De overheid of verzekeraar kan in dit geval de afdwinger zijn. De standaarden kunnen gelden voor de ICT-dienstverleners (waaraan het mkb vaak uitbesteedt) of direct aan het mkb zelf

[20] De Center for Internet Security (CIS) standaarden zijn gericht op hoe de industrie zijn infrastructuur dient in te richten. Enkele incident response bedrijven hanteren CIS level 1, banken hanteren CIS level 3).

(door iedereen die diensten levert aan de overheid te verplichten hieraan te voldoen). In de Nationale Cybersecurity Agenda wordt overigens al gesproken over een bredere toepassing van internationale standaarden. [168] In feite is het doel een cultuurverandering te bewerkstellingen, en hoe mooi dat ook zou zijn, dat lukt niet met één brief. Dat vraagt om een combinatie van verschillende methoden én om opvolging.

Box 20. Uitkomsten validatiesessies met betrekking tot een alternatieve aanpak

In de validatiesessies is een open vraag gesteld welke andere beleidsopties er zijn om Nederland meer weerbaar te maken tegen ransomware-aanvallen . Er is één antwoord dat meerdere keren gegeven werd en er echt uitspringt. Er zou moeten worden ingezet op het in meer of mindere mate hacken van middelgrote en kleine organisaties zodat aan hen kan worden aangetoond hoe eenvoudig het is om binnen te komen. Hierbij kan gebruik gemaakt worden van middelen die gebruikt worden voor het verkrijgen van initiële toegang, zie hoofdstuk 3. De verwachting is dat bestuurders hiervan schrikken en maatregelen gaan nemen. Aan de andere kant zijn er ook vragen of dit mogelijke beleidsinstrument (1) wel ethisch verantwoord is, (2) juridisch toegestaan is en (3) geen additionele risico's creëert.

Een ander antwoord dat werd gegeven, en dat ook in de reguliere interviews in verschillende vormen terugkwam, was het inzetten op het verbeteren van de kwaliteit van ICT-dienstverleners. Er is een beeld dat te veel van deze partijen onvoldoende bescherming geven aan hun klanten. Dat komt deels doordat bestuurders van middelgrote en kleine organisaties vaak sterk gericht zijn op het verlagen van de kosten van de inkoop van ICT. Aanbevelingen van hun ICT-dienstverlener over het verhogen van cyberweerbaarheid worden dan gezien als verkooppraatje. Aan de andere kant zijn er ook (veelal kleine) ICT-dienstverleners die simpelweg niet de capaciteiten hebben om voldoende weerbaarheid te bieden.

6.6 Mogelijke vervolgstappen

In dit hoofdstuk gaven wij, op basis van theorie, een voorzet voor het ontwerp van een ransomware-campagne. Die opzet is nog niet getoetst. Daarnaast slaat de theorie vooral op de risicoperceptie van individuen en weten we niet precies of en welke andere factoren een rol spelen op managementniveau. Daarvoor zou ook de managementliteratuur geraadpleegd moeten worden, iets wat buiten de scope van dit onderzoek viel. Een logische vervolgstap zou zijn om middels vervolgonderzoek een effectiviteitsbepaling uit te voeren. Slechts een deel van de uitgevoerde campagnes in het algemeen wordt geëvalueerd en met sterk wisselende resultaten. Zo blijkt dat meer kennis niet automatisch zorgt voor veiliger gedrag. [169] Soms worden neveneffecten gevonden die juist niet bijdragen aan het doel van de campagne. Uit een recente meta-analyse van bewustwordingscampagnes gericht op online criminaliteit blijkt bijvoorbeeld dat er substantiële verschillen in de omvang van de effecten gevonden worden. [170]

Daarnaast rest het ons nog op te merken dat de in dit rapport genoemde maatregelen ook helpen tegen andere vormen van cybercriminaliteit en dat daarmee het nut van dit onderzoek ook breder gezien kan worden. We hebben hier bepaalde keuzes gemaakt met betrekking tot de doelgroep voor de ransomware-campagne (focus op bestuurders en middelgrote en kleine organisaties), maar er zijn uiteraard meer doelgroepen relevant. Vermoedelijk zijn dezelfde principes dan van toepassing, maar ook dat zou onderwerp kunnen zijn van eventueel vervolgonderzoek.

Verwijzingen

[1] Emisoft, (2020). *Ransomware statistics for 2020: Year in summary* [blog.emsisoft.com]

[2] NCSC, (2020). *Ransomware. Maatregelen voor het voorkomen, beperken en herstellen van een ransomware-aanval* [www.ncsc.nl] Den Haag: NCSC.

[3] Verizon, (2021). *Data Breach Investigations Report* [www.verizon.com]

[4] WEF, (2022). *Global Cybersecurity Outlook 2022. Insight report* [www3.weforum.org] Geneva: World Economic Forum.

[5] NCTV, (2021). *Cybersecuritybeeld Nederland 2021* [www.nctv.nl] Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

[6] NOS Nieuws, (2021). *Kritiek op Rusland vanwege ransomware-aanvallen: 'Criminelen kunnen hun gang gaan'* [nos.nl]

[7] Digital Trust Center (2022). *Basisscan Cyberweerbaarheid - Digital Trust Center* [basisscan.digitaltrustcenter.nl]

[8] Foresite (2022). *Ransomware Risk Assessment* [foresite.com]

[9] Kroll (2022). *Ransomware Preparedness Assessment* [www.kroll.com]

[10] Bankers Electronic Crimes Task Force, State Bank Regulators, and the United States Secret Service, (2020). *Ransomware Self-Assessment Tool* [www.csbs.org]

[11] CISA, (2022). *Cyber Security Evaluation Tool (CSET®)* [www.cisa.gov]

[12] NCSC (2022). *Kennisproducten met impact: de wereld veranderen met een pdf* [www.ncsc.nl]

[13] ABN-AMRO, (2022). *Cyberdreiging zet ondernemers aan tot maatregelen* [www.abnamro.nl]

[14] Politie.nl, (2022). *Het dataportaal van de politie* [data.politie.nl]

[15] ENISA, (2021). *ENISA Threat Landscape 2021* [www.enisa.europa.eu]

[16] Trend Micro, (2021). *Ransomware Double Extortion and Beyond: REvil, Clop, and Conti* [www.trendmicro.com]

[17] Palo Alto Networks, (2021). *Extortion Payments Hit New Records as Ransomware Crisis Intensifies* [www.paloaltonetworks.com]

[18] Coveware, (2022). *Law enforcement pressure forces ransomware groups to refine tactics in Q4 2021* [www.coveware.com]

[19] Sophos, (2021). *The State of Ransomware 2021* [secure2.sophos.com] A Sophos Whitepaper..

[20] Grustniy, L. (2021). *The ransomware saga* [www.kaspersky.com]

[21] Fortinet, (2021). *The 2021 Ransomware Survey Report* [www.fortinet.com]

[22] VPNGids, (2021). *CD PROJEKT bevestigt dat gestolen data op internet rondgaat* [www.vpngids.nl]

[23] IGN Benelux, (2021). *Gestolen CD Projekt Red files zouden verkocht zijn na veiling op het dark web* [nl.ign.com]

[24] CSO, (2021). *The 15 biggest data breaches of the 21st century* [www.csoonline.com]

[25] Raconteur, (2016). *How a data breach battered Yahoo!'s reputation* [www.raconteur.net]

[26] Wired, (2015). *Hackers Finally Post Stolen Ashley Madison Data* [www.wired.com]

[27] Quekel, S. (2021). *Megaclaim in de maak: stichting eist miljarden van ministerie om datalek GGD* [www.ad.nl] Algemeen Dagblad.

[28] EDPB, (2021). *Guidelines on Examples regarding Data Breach Notification* [edpb.europa.eu]

[29] Techzine, (2020). *Nieuwe ransomware dreigt met GDPR-overtreding* [www.techzine.nl]

[30] esentire, (2021). *Grief Ransomware Gang Claims 41 New Victims, Targeting Manufacturers; Municipalities; & Service Companies in U.K. & Europe* [www.esentire.com]

[31] Reuters, (2019). *Yahoo strikes $117.5 million data breach settlement after earlier accord rejected* [www.reuters.com]

[32] Chainalysis, (2021). *Ransomware 2021: Critical Mid-year Update [REPORT PREVIEW]* [blog.chainalysis.com]

[33] Toulas, B. (2022). *Ransom payments fall as fewer victims choose to pay hackers* [www.bleepingcomputer.com]

[34] Coveware (2022). *Quarterly Report. Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022* [www.coveware.com]

[35] Techtarget, (2021). *Ransomware* [www.techtarget.com]

[36] Bank info security, (2021). *Ransomware: Average Ransom Payment Drops to $137,000* [www.bankinfosecurity.com]

[37] Dailycoin, (2020). *Ransomware Attacks and Payments Are Rising* [dailycoin.com]

[38] NetDiligence (2021). *Ransomware 2021 Spotlight Report* [netdiligence.com]

[39] World Economic Forum, (221). *5 urgent actions in the fightback against ransomware* [www.weforum.org]

[40] Allianz, (2021). *Ransomware - Risks and Resilience* [www.agcs.allianz.com]

[41] Business insider, (2021). *One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a cyberattack* [www.businessinsider.com]

[42] Paquet-Clouston, M., Haslhofer, B., and Dupont, B. (2019). *Ransomware Payments in the Bitcoin Ecosystem* [doi.org] Journal of Cybersecurity, Volume 5, Issue 1, 2019, tyz003.

[43] FOX-IT, (2020). *Spoedondersteuning project Fontana* [www.maastrichtuniversity.nl]

[44] Datto, (2020). *Global State of the Channel Ransomware Report* [www.datto.com]

[45] security.nl, (2021). *VDL Groep maand na cyberaanval volledig hersteld dankzij back-ups* [www.security.nl]

[46] Hiscox (2021). *Hiscox Cyber Readiness Report 2021* [www.hiscoxgroup.com]

[47] Cybereason, (2021). *Ransomware: The thru cost to business* [www.cybereason.com]

[48] NCTV, (2021). *Cybersecuritybeeld Nederland* [www.nctv.nl]

[49] Financieel Dagblad, (2021). *ASML geeft zijn leveranciers bijles over het weren van hackers* [fd.nl]

[50] RTLNieuws, (2021). *Geen kaas: hoe een hack zorgt voor lege schappen in de AH* [www.rtlnieuws.nl]

[51] MIT Technology Review, (2021). *The Colonial pipeline ransomware hackers had a secret weapon: self-promoting cybersecurity firms* [www.technologyreview.com]

[52] Tweakers.net, (2017). *Systemen van containerconcern Maersk zijn getroffen door ransomware* [tweakers.net]

[53] Bleeping computer, (2022). *FBI: BlackByte ransomware breached US critical infrastructure* [www.bleepingcomputer.com]

[54] VPNGids, (2021). *De 10 grootste cyberaanvallen van 2021* [www.vpngids.nl]

[55] Computable, (2014). *Indirecte aanval via stepping stones in opmars* [www.computable.nl]

[56] Hassan, N. (2019). *Ransomware Revealed. A Beginner's Guide to Protecting and Recovering from Ransomware Attacks* [link.springer.com] Springer Nature Switzerland AG.

[57] Cyber Security Raad, (2021). *Integrale aanpak Cyberweerbaarheid. Een integrale aanpak om de open, vrije en welvarende Nederlandse samenleving structureel cyberweerbaar te maken en (digitale) kansen te verzilveren* [www.rijksoverheid.nl] Den Haag,

[58] Greenberg, A. (2020). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*Random House Usa Inc.

[59] Vos, A. (2020). *Cyberwar als het ultieme machtsvertoon* [] Financieel Dagblad.

[60] Greenert, J.W. (2013). *Kill Chain Approach* [web.archive.org]

[61] Muckin, M., and Fitch, S. (2019). *A Threat-Driven Approach to Cyber Security* [www.lockheedmartin.com] Lockhead Martin White paper.

[62] Exabeam, (2016). *Threat research report. The anatomy of a ransomware attack* [www.exabeam.com]

[63] Lazarovitz, L. (2017). *Ransomware Analysis – Executions Flow and Kill Chain* [www.isaca.org]

[64] Microsoft, (2020). *Ransomware groups continue to target healthcare, critical services; here's how to reduce risk* [www.microsoft.com]

[65] McAfee, (2021). *Threat Report 06.21* [www.mcafee.com]

[66] Tweakers.net, (2022). *Community-interview met SchizoDuckie* [tweakers.net]

[67] NCSC, (2021). *Log4shell – Wat is het, hoe lossen we het op en waarom hebben organisaties er last van?* [www.ncsc.nl]

[68] Microsoft, (2022). *Remote Desktop Protocol Remote Code Execution Vulnerability* [msrc.microsoft.com]

[69] Coveware, (2022). *Ransomware as a Service Innovation Curve* [www.coveware.com]

[70] Hiscox, (2020). *Data exfiltration during ransomware attacks* [www.hiscox.co.uk] London,

[71] Trend Micro, (2021). *LockBit Resurfaces With Version 2.0 Ransomware Detections in Chile, Italy, Taiwan, UK* [www.trendmicro.com]

[72] Meskauskas, T. (2022). *LockBit ransomware verwijderingsinstructies* [www.pcrisk.nl]

[73] Github, (2017). *wanakiwi* [github.com]

[74] Tajalizadehkhoob, S., Asghari, H., Ganan, C., and Eeten , M.v. (2014). *Why them? Extracting intelligence about target selection from Zeus financial malware* [repository.tudelft.nl] Proceedings of the 13th Annual Workshop on the Economics of Information Security, WEIS 2014, State College (USA), June 23-24, 2014,

[75] Tajalizadehkhoob, S., Goethem, T.v., Korczyński, M., Noroozian, A., Böhme, R., Moore, T., Joosen, W., and Eeten, M.v. (2017). *Herding Vulnerable Cats: A Statistical Approach to Disentangle Joint Responsibility for Web Security in Shared Hosting* [www.researchgate.net] ACM CCS'17.

[76] Nieuwsuur, (2021). *Zo voert de digitale mafia een hack-aanval uit.* [www.youtube.com]

[77] Northwave, (2021). *Inside the world of ransomware, Part 1/3: dissecting the attack* [northwave-security.com]

[78] Bleeping computer, (2021). *Hacking gang creates fake firm to hire pentesters for ransomware attacks* [www.bleepingcomputer.com]

[79] Smilyanets, D. (2022). *An ALPHV (BlackCat) representative discusses the group's plans for a ransomware 'meta-universe'* [therecord.media]

[80] Samani, R. (2021). *Ransomware: Relationship breakdowns have never been so satisfying* [www.helpnetsecurity.com]

[81] Coveware, (2021). *What We Can Learn From Ransomware Actor "Security Reports"* [www.coveware.com]

[82] Smilyanets, D. (2022). *An ALPHV (BlackCat) representative discusses the group's plans for a ransomware 'meta-universe'* [therecord.media]

[83] Clueley, G. (2022). *Ransomware demands acts of kindness to get your files back* [www.tripwire.com]

[84] Abrams, L. (2020). *Ransomware Gangs to Stop Attacking Health Orgs During Pandemic* [www.bleepingcomputer.com]

[85] Ryan, M. (2021). *Ransomware Revolution: The Rise of a Prodigious Cyber Threat. (Advances in Information Security, 85)* [www.amazon.com] Springer.

[86] VPNGids, (2022). *Wat is ransomware?* [www.vpngids.nl]

[87] Cimpanu, C. (2022). *Conti ransomware gang chats leaked by pro-Ukraine member* [therecord.media]

[88] RTLNieuws, (2022). *Cyberaanvallen op Oekraïne in volle gang: malware verspreid die computers sloopt* [www.rtlnieuws.nl]

[89] IEEE, (2013). *The Real Story of Stuxnet. How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program* [spectrum.ieee.org]

[90] Wired, (2010). *Guilty Plea in 'Anonymous' DDoS Scientology Attack* [www.wired.com]

[91] AD, (2016). *20 jaar cel voor hacker met IS-sympathieën* [www.ad.nl]

[92] ABC News, (2011). *Top Hacker Suspect Arrested After Attacks on Sony, Sega, Citibank, CIA* [abcnews.go.com]

[93] Threatpost, (2021). *Office 365 Cyberattack Lands Disgruntled IT Contractor in Jail* [threatpost.com]

[94] Consumerist, (2014). *Teens Hack ATM, Then Show Bank How Easily They Did It* [consumerist.com]

[95] Helpsystems, (2019). *Diversionary tactics: The use of ransomware as misdirection* [www.helpsystems.com]

[96] Ernst & Young, (2021). *How to protect your organization from ransomware* [assets.ey.com]

[97] SHI, (2020). *12 ways to protect your organization from ransomware* [blog.shi.com]

[98] ExtremeNetworks, (2017). *7 Steps for Protecting Your Organization from Ransomware* [cloud.kapostcontent.net]

[99] Security intelligence, (2019). *10 Reasons Your Organization Is Potentially at Risk of a Ransomware Attack* [securityintelligence.com]

[100] Microsoft, (2021). *Protect your organization from ransomware* [download.microsoft.com]

[101] CIS, (2021). *Ransomware: Facts, Threats, and Countermeasures* [www.cisecurity.org]

[102] No More Ransom, (2021). *Hoe voorkom ik een ransomware-aanval?* [www.nomoreransom.org]

[103] digitaldefense, (2021). *Top 3 Attack Vectors Ransomware Loves to Exploit* [www.digitaldefense.com]

[104] Digital Trust Center, (2021). *Ransomware* [www.digitaltrustcenter.nl]

[105] IT Governance USA, (2021). *Ransomware Prevention: 5 Tips To Protect Against Ransomware* [www.itgovernanceusa.com]

[106]Kaspersky, (2022). *Laat je niet chanteren.* [www.kaspersky.nl]

[107]KvK, (2021). *Wat kun je doen tegen ransomware? 6 tips* [www.kvk.nl]

[108]Microsoft, (2013). *Ransomware: Ways to Protect Yourself & Your Business* [www.microsoft.com]

[109]Microsoft, (2021). *3 steps to prevent and recover from ransomware* [www.microsoft.com]

[110]National Cyber Security Centre, (2021). *Mitigating malware and ransomware attacks* [www.ncsc.gov.uk]

[111]Nationaal Cyber Security Centrum, (2022). *Basismaatregelen cybersecurity* [www.ncsc.nl]

[112]Nortec, (2022). *The #1 Risk Factor for Ransomware* [www.nortec.com]

[113]TechRepublic, (2021). *9 tips to protect your organization against ransomware* [www.techrepublic.com]

[114]KPN, (2020). *Ransomware: wat is het en hoe kun je het voorkomen?* [www.kpn.com]

[115]AIG (2022). *Vragenformulier ransomware (aanvullend)* [www.aiginsurance.nl]

[116]Allianz (2022). *Binnen 10 minuten uw cyberrisico's in beeld* [cyberrisicoscan.allianz.nl]

[117]AON (2022). *Direct van start: Voorbereiden op een cyberincident* [www.aon.com]

[118]Barracuda, (2022). *Ransomware protection checklist* [assets.barracuda.com]

[119]Interpolis, (2022). *Cyberscan* [www.interpolis.nl]

[120]Turien&Co, (2022). *Voorwaarden en documenten* [turien.nl]

[121]Statcounter, (2022). *Desktop Windows Version Market Share Netherlands* [gs.statcounter.com]

[122]Microsoft, (2022). *Ondersteuning voor Windows XP is beëindigd* [support.microsoft.com]

[123]Coalition (2021). *Cyber Insurance Claims Report* [info.coalitioninc.com]

[124]Techradar, (2021). *Is Microsoft Defender good enough for your PC – or do you need a better free antivirus?* [www.techradar.com]

[125]Adroit Market Research, (2019). *Global Multi-Factor Authentication Market Size by Model (Two-Factor Authentication, Three-Factor Authentication, Four-Factor Authentication, and Five-Factor Authentication), by Application (Government, Healthcare, Banking, BFSI, Retail and E-commerce, and* [www.adroitmarketresearch.com]

[126]Trend Micro, (2022). *What Are the Different Types of Phishing?* [www.trendmicro.com]

[127]ZDNet, (2004). *How does 'Sender Policy Framework' work?* [www.zdnet.com]

[128]NCSC, (2015). *Factsheet Bescherm domeinnamen tegen phishing* [www.ncsc.nl]

[129]DTC, (2022). *Een back-up strategie opstellen* [www.digitaltrustcenter.nl]

[130]Marsh (2021). *The Changing Face of Cyber Claims 2021* [www.marsh.com]

[131]Coveware, (2021). *Ransomware attackers down shift to 'Mid-Game' hunting in Q3 2021* [www.coveware.com]

[132]Tweakers.net, (2020). *Hoe ransomware veranderd is. Van foto's versleutelen naar miljardenindustrie* [tweakers.net]

[133]CBS, (2022). *Bedrijven; bedrijfsgrootte en rechtsvorm* [opendata.cbs.nl]

[134]zdnet, (2019). *Ransomware: Big paydays and little chance of getting caught means boom time for crooks* [www.zdnet.com]

[135]NPR, (2021). *In The Ransomware Battle, Cybercriminals Have The Upper Hand* [www.npr.org]

[136]WEF, (2019). *Fighting cybercrime – what happens to the law when the law cannot be enforced?* [www.weforum.org]

[137]BBC, (2022). *REvil ransomware gang arrested in Russia* [www.bbc.com]

[138]ZDNet, (2022). *Egregor ransomware operators arrested in Ukraine* [www.zdnet.com]

[139]ZDNet, (2022). *Decryptor released for Maze, Egregor, and Sekhmet ransomware strains* [www.zdnet.com]

[140]Forbes, (2020). *Hackers Claim To Have Trump's Dirty Laundry And Demand $42 Million To Keep Quiet* [www.forbes.com]

[141]Motivaction, (2020). *Veilig Online 2020* [www.adformatie.nl]

[142]TNS, (2016). *Cybersecurity awareness en skills in Nederland* [www.vandoorne.com]

[143]Hogeschool Saxion , and De Haagse Hogeschool , (2020). *Cyberweerbaarheid. Risicobewustzijn en zelfbeschermend gedrag rondom cybercriminaliteit onder jongeren en mkb'ers.* [www.saxion.nl]

[144]Rathenau, (2018). *Een nooit gelopen race* [www.rathenau.nl]

[145]Paton, D. (2003). *Disaster preparedness: A social-cognitive perspective.* [www.researchgate.net]

[146]Slovic, P., Finucane, M., Peters, E., and MacGregor, D. (2004). *Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. Risk analysis, 24(2), 311-322.* [pubmed.ncbi.nlm.nih.gov]

[147]Instituut Fysieke Veiligheid , (2019). *Gedrag beïnvloeden met risico-communicatie.* [nipv.nl]

[148]Cuccibu, (2022). *Bewustwordingscampagnes en gedragsverandering* [cuccibu.nl]

[149]Ruitenberg, A., and Helsloot, I. (2004). *Zelfredzaamheid van burgers bij rampen en zware ongevallen* [crisislab.nl]

[150]Kahneman, D., and Tversky, A. (1979). *Prospect Theory: An Analysis of Decision under Risk in Econometrica, Vol. 47, No. 2. (Mar., 1979), pp. 263-292,* [www.jstor.org]

[151]Kahneman, D., and Tversky, A. (1979). *On the interpretation of intuitive probability: A reply to Jonathan Cohen. Cognition, 7(4), 409–411.* [doi.org]

[152]Witte, K. (1992). *Putting the fear back into fear appeals: The extended parallel process model. Communications Monographs, 59(4), 329-349.* [doi.org]

[153]Sheeran, P. (2011). *Intention—Behavior Relations: A Conceptual and Empirical Review* [www.tandfonline.com]

[154]Haugabook, (2022). *Protection Motivation Theory* [www.communicationtheory.org]

[155]Claassen, L., and Kerckhoffs, T. (2018). *Publieksperceptie van Stralingsrisico's:* [rivm.openrepository.com]

[156]Ruiter, R., Kessels, L., Peters, G., and Kok, G. (2014). *Sixty years of fear appeal research: Current state of the evidence* [onlinelibrary.wiley.com]

[157]Renes, R., Putte, van de, B., Breukelen, van, R., Loef, J., Otte, M., and Wennekers, C. (2011). *Gedragsverandering via campagnes* [www.communicatierijk.nl]

[158]Snyder, L., and Hamilton, M. (2002). *A Meta-Analysis of U.S. Health Campaign Effects on Behavior: Emphasize Enforcement, Exposure, and New Information, and Beware the Secular Trend* [www.taylorfrancis.com]

[159]Wakefield, M., Loken, B., and Hornik, R. (2010). *Use of mass media campaigns to change health behaviour. The Lancet Volume 376, ISSUE 9748, P1261-1271, October 09, 2010* [doi.org]

[160]Mullink, J. (2019). *Campagnes voor gedragsverandering: missers & successen* [www.frankwatching.com]

[161]DVJ, (2021). *Campagne-effectonderzoek BOB 2020* [www.rijksoverheid.nl]

[162]Financieel Dagblad, (2022). *Oeps, door jouw fout ligt het bedrijfsnetwerk plat* [fd.nl]

[163]AdAge, (2021). *These provocative billboards tell Swedes that their passwords are literally 'shit'* [adage.com]

[164]Famous Campaigns, (2019). *Bike shop 'hacked' to illustrate the impact of a cyber attack* [www.famouscampaigns.com]

[165]Everbridge, (2022). *Ransomware Infographic: The Risks are High for Healthcare Organizations* [www.everbridge.com]

[166]SecureOPS, (2021). *Don't Get Locked Up by Ransomware* [www.secureops.com]

[167]CISA, (2022). *Ransomware Campaign Toolkit* [www.cisa.gov]

[168]Dialogic, (2021). *Evaluatie van de opbouw en meetbaarheid van de Nederlandse Cybersecurity Agenda* [www.dialogic.nl]

[169]Kleij, van der, R., Weijer, van de, S., Leukfeldt, R., and Hoff-de Goede, van 't, S. (2019). *Hoe veilig gedragen wij ons online?* [repository.wodc.nl]

[170]Bullée, J., and Junger, M. (2020). *How effective are social engineering interventions? A meta-analysis* [dx.doi.org]

[171]Acronis, (2020). *Ransomware leaking more data than many data breaches* [www.acronis.com]

[172]AD, (Met Black Friday en kerst voor de deur staat MediaMarkt voor loodzware keus: criminelen betalen of forse schade lijden). *2021* [www.ad.nl]

[173]Tweakers, (2020). *Ransomware-aanval op Duits ziekenhuis leidde mogelijk tot dood patiënte* [tweakers.net]

[174]Bekkers, L., Kleij, van der, R., and Leukfeldt, R. (2021). *Cyber-ketenweerbaarheid. Een verkennend onderzoek naar dreigingen, kwetsbaarheden en geleerde lessen* [www.dehaagsehogeschool.nl] Den Haag: De Haagse Hogeschool.

[175]National Institute of Standards and Technology, (2021). *Cybersecurity Framework Profile for Ransomware Risk Management. Draft NISTIR 8374.* [doi.org] U.S. Department of Commerce..

[176]Onderwijsinspectie, (2020). *Cyberaanval Universiteit Maastricht* [www.onderwijsinspectie.nl] Utrecht,

[177]Wagen, W.v. d., van 't Zand-Kurtovic, E., Matthijsse, S., and Fischer, T. (2019). *Cyberdaders: uniek profiel, unieke aanpak? Een onderzoek naar kenmerken van en passende interventies voor daders van cybercriminaliteit in enge zin.* [repository.wodc.nl] Den Haag: Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC).

[178]CyberVeilig Nederland, (2021). *Whitepaper Ransomware* [cyberveilignederland.nl]

[179]Politie.nl, . *Het dataportaal van de politie* [data.politie.nl]

[180]NOS, (2021). *NCTV: ransomware is bedreiging voor nationale veiligheid* [nos.nl]

Bijlage 1. Overzicht interviewrespondenten

Naam	Organisatie
Archana Ramkhelawan	Gemeente Rotterdam
Arwi van der Sluijs	NFIR
Christiaan Ottow	Northwave
Dave Woutersen	NCSC
David Lacroix	Hof van Twente
Erwin Hasenpflug	Digital Trust Center
Esther Baars	OM parket Rotterdam
Frank Plattel	ROS
Harrie Bolt	Commitment
Inge van der Beijl	Northwave
Jacques Beursgens	Universiteit van Maastricht
Joep van Sambeek	Onafhankelijk IT adviseur
John Fokker	McAfee
Joost Raeven	DGRR
Koen Augustijn	Universiteit van Maastricht
Laura de Korte	DGRR
Lodewijk van Zwieten	OM
Lodi Hensen	Tesorion
Marc van der Ham	OM landelijk parket
Marcel Mevissen	NWO
Marijn Schuurbiers	Politie
Matthijs Jaspers	Politie
Melvin Koelewijn	SURFcert
Michel van Eeten	TUDelft, cyber security raad
Michel Verhagen	Digital Trust Center
Nick van der Laan	NWO
Peter Lahousse	Cybercrime info.nl
Pim Takkenberg	Northwave
Sander van der Made	Politie
Tugce Serinkan	Verbond van Verzekeraars, Platform Cyber
Wouter Arts	ROS
Wouter Wissink	Verbond van Verzekeraars, Platform Cyber

Bijlage 2. Overzicht respondenten validatiesessies

Naam	Organisatie	Contact via
Arwi van der Sluijs	NFIR	CVN
Christiaan Ottow	Northwave	CVN
Gerard Brooijmans	Caci	DTC
Hans van Doorn	SelectIT	DTC
Inge van der Beijl	Northwave	CVN
Lodi Hensen	Tesorion	CVN
Mark van Dijk	12GO Biking	DTC
Mikell Becker	Sense-Comm Technology	DTC
Peter Bin	SecurityHive	DTC
Pim Takkenberg	Northwave	CVN
Roel Villerius	PCI	DTC
Ron Janson	Slachtofferhulp Nederland	DTC

Contact:
Dialogic innovatie & interactie
Hooghiemstraplein 33-36
3514 AX Utrecht
Tel. +31 (0)30 215 05 80
www.dialogic.nl