dialogic
innovatie • interactie

Ransomware-aanvallen op instellingen en bedrijven in Nederland

Managementsamenvatting (NL)

dr. Tessel Blom, ir. Wazir Sahebali, Kimberly Deppe MSc,
ing. Peter Romijn, Floris Donath, ir. ing. Reg Brennenraedts MBA

In opdracht van:
Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)

Publicatienummer:
2022.173-2319-MSNL

Datum:
Utrecht, 1-8-2023

Managementsamenvatting

Introductie

In opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (hierna: WODC) heeft Dialogic Innovatie en Interactie (hierna: Dialogic) een onderzoek naar ransomware-aanvallen op instellingen en bedrijven in Nederland uitgevoerd. Het WODC is op zoek naar indicatoren die de omvang en de aard van deze ransomware-aanvallen in kaart kan brengen. Op basis van deze indicatoren moet er een beeld gevormd worden van ransomware-aanvallen in de jaren 2020, 2021 en 2022. Daarnaast moeten de beperkingen van deze indicatoren en databronnen onderzocht worden. Het onderzoek beantwoordt de volgende onderzoeksvragen:

1. Met **welke indicatoren** kan inzicht worden gekregen in de mate waarin ransomware-aanvallen op instellingen en bedrijven in Nederland voorkomen en de aard en gevolgen van deze aanvallen met betrekking tot de eigenschappen van de getroffen instellingen en bedrijven, de response op de aanvallen, de geleden schade en andere gevolgen?
2. Bevatten **bestaande databronnen** gegevens die inzicht bieden in de relevante indicatoren?
3. **Welk beeld** kan aan de hand van de bestaande databronnen worden gevormd voor **de jaren 2020, 2021 en 2022** over de mate waarin ransomware-aanvallen op instellingen en bedrijven in Nederland voorkomen en de aard en gevolgen van deze aanvallen met betrekking tot de eigenschappen van de betrokken instellingen en bedrijven, de response op de aanvallen, de geleden schade en andere gevolgen?
4. **Welke beperkingen** hebben de bestaande databronnen met betrekking tot de beschikbaarheid, volledigheid en kwaliteit van data en in hoeverre gelden er andere beperkingen?
5. Op welke wijze kunnen deze beperkingen worden **verminderd of weggenomen**?

Voor de uitvoering van dit onderzoek is gebruik gemaakt van verschillende dataverzamelingsmethodes: literatuuronderzoek, interviews, analyse van politieaangifte data[1] en web scraping.

Deel 1: Theoretische achtergrond

De indicatoren van ransomware

Databronnen zullen in veel gevallen slechts inzicht kunnen geven in een bepaald aspect van een ransomware-aanval. De indicatoren, die op basis van literatuuronderzoek en interviews relevant zijn gebleken, zijn:

- **Generieke kenmerken van een ransomware-aanval**. Deze indicator beslaat de aanvaller, het doelwit, de wijze waarop toegang is verkregen en de acties die gebruikt worden om druk uit te oefenen op het slachtoffer.

[1] Verkregen binnen het PhD-onderzoek van Tom Meurs naar de aard en omvang van ransomware binnen Nederland.

- **Kenmerken van het slachtoffer**. Bij deze indicator gaat het specifiek over de kenmerken van het slachtoffer, zoals de sector, de grootte of de locatie van de organisatie.
- **Impact van een ransomware-aanval**. Deze indicator brengt de gevolgen van een ransomware-aanval voor de individuele organisatie of de maatschappij in kaart.
- **Frequentie van ransomware-aanvallen**. Bij deze indicator gaat het niet om een specifieke ransomware-aanval, maar hoe vaak bepaalde ransomware-aanvallen op bepaalde slachtoffers met een bepaalde impact plaatsvinden.

De stappen in een ransomware-aanval

De meeste databronnen kunnen slechts inzicht geven in een bepaalde stap van een ransomware-aanval. Daarmee bevatten ze alleen informatie over een bepaalde groep slachtoffers. Bij elke opeenvolgende stap in een ransomware-aanval wordt deze groep slachtoffers kleiner. In dit onderzoek verwijzen wij naar verschillende groepen onder de slachtoffers als *subsets*.

Deel 2: Databronnen

In dit onderzoek zijn onderstaande databronnen geanalyseerd. Elke databron geeft inzicht in een subset van slachtoffers en een beperkte hoeveelheid indicatoren:

1. **Virusscanaanbieders** hebben vaak detectiemechanismes voor ransomware en hebben dus zicht op het aantal pogingen tot een ransomware-aanval.
2. **IT-dienstaanbieders** hebben zicht op verdachte activiteiten van de cybercrimineel wanneer deze binnen is gedrongen.
3. **Incident response bedrijven** worden door het slachtoffer ingeschakeld om de response op de ransomware-aanval te coördineren.
4. **Cybersecurity-verzekeraars** worden door het slachtoffer ingelicht bij een ransomware-aanval en zijn ook betrokken bij de afhandeling.
5. **Politieaangiftes**. Bij een ransomware-aanval kan een slachtoffer hier bij de politie aangifte van doen, maar is hier niet toe verplicht.
6. De **CBS Cybersecuritymonitor** bevraagt een selectie van Nederlandse organisaties of ze het afgelopen jaar te maken hebben gehad met een ransomware-aanval en wat daar de impact van is geweest.
7. De **media** rapporteren over bepaalde ransomware-aanvallen en hebben daarmee ook deels invloed op de impact van aanvallen op de maatschappij. Daarnaast vervullen de media een belangrijke rol als het gaat om de bewustwording van ransomware.
8. Op **websites van ransomware-groepen** wordt gedreigd met het publiceren van gestolen data van slachtoffers en wordt deze data gepubliceerd als er geen losgeld is betaald.
9. De **Autoriteit Persoonsgegevens** heeft zicht op het aantal bij de AP gemelde datalekken. Slachtoffers van een ransomware-aanval moeten, bij een vermoeden van een datalek, een melding maken bij de AP.
10. Het **cryptobetalingsverkeer** bevat losgeldbetalingen naar ransomware-groepen.
11. **No More Ransom** biedt voor bepaalde ransomware-software *decryptors* aan waarmee de versleutelde bestanden ontsleuteld kunnen worden.

Het beeld van ransomware voor de jaren 2020, 2021 en 2022

De bestaande databronnen geven geen eenduidig beeld van ransomware-aanvallen op Nederlandse bedrijven en instellingen voor de jaren 2020, 2021 en 2022. Veel databronnen zijn te generiek, waardoor het bijvoorbeeld niet mogelijk is om er specifiek informatie voor

Nederland uit te halen, of ze beslaan niet de volledige periode 2020, 2021, 2022. Daarnaast spelen er bij een aantal partijen ook commerciële belangen mee of is de informatie die partijen publiekelijk beschikbaar maken zeer beperkt. Desalniettemin schetsen we hieronder per indicator een beeld.

Generieke kenmerken van ransomware-aanvallen

Aanvaller: Het cryptobetalingsverkeer laat in de jaren 2020, 2021 en 2022 zien dat het marktaandeel van de verschillende ransomware-groepen over de tijd sterk schommelt. Het oprollen van een groep leidt vaak tot het ontstaan van nieuwe groepen met een nieuwe software. Deze diversiteit aan ransomware-groepen is ook terug te zien in de rapportages van de virusscanaanbieders, waar vele verschillende ransomware *strains* gedetecteerd worden. Analyses van de websites van ransomware-groepen laten zien dat de LockBit groep in 2021 en 2022 verantwoordelijk is voor de meeste datalekken van Nederlandse organisaties.

Doelwit: Virusscanaanbieders laten zien dat er wereldwijd een toename is van gerichte aanvallen in 2021. Ook tonen deze virusscanaanbieders dat de opkomst van Ransomware-as-a-Service met name te zien is bij consumenten, maar minder bij de grote bedrijven en MKB'ers.

Initiële toegang: Zowel de IT-dienstaanbieders als de incident response bedrijven zeggen dat e-mail de meest gebruikte methode is van initiële toegang (*phishing*), gevolgd door desktop sharing software in de jaren 2020, 2021 en 2022.

Acties om druk uit te oefenen: Er is geen bron die inzicht geeft in de verhouding tussen de verschillende acties die gebruikt kunnen worden (blokkeren, versleutelen, data exfiltratie). Wel hebben we in de interviews opgehaald dat het stelen van data steeds gangbaarder wordt (vaak zelfs zonder de bestanden te versleutelen), terwijl het blokkeren van systemen tegenwoordig minder vaak voorkomt.

Kenmerken van slachtoffer

Locatie: De websites van ransomware-groepen, waar zij slachtoffers publiceren, laten zien dat Nederland in de periode 2021 en 2022 in de lijst van gepubliceerde organisaties op plek 12 staat. Amerikaanse organisaties worden het vaakst gepubliceerd. Ook bij de IT-dienstaanbieders bevinden de meeste slachtoffers van ransomware in de Verenigde Staten.

Sector: De industriële en financiële sectoren worden wereldwijd volgens de incident response bedrijven het vaakst getroffen. Uit de CBS cybersecuritymonitor komen ook de sectoren *industrie* en *financiële dienstverlening* naar voren als meest getroffen. De meeste politieaangiftes van ransomware komen uit de handelssector. Deze bronnen houden andere sectorverdelingen aan, maar wijzen wel met name naar organisaties in de industrie. Ten opzichte van 2020 was er in 2021 een verdubbeling van het aantal aangiftes uit de ICT-sector. Deze toename van aanvallen op de ICT-sector wordt ook beaamd door de Autoriteit Persoonsgegevens, die in 2021 de aanvallen op IT-leveranciers uitlichtten.

Grootte: De CBS Cybersecuritymonitor laat zien dat hoe groter de organisatie is (c.q. hoe meer werkzame personen), hoe groter de kans is dat de organisatie te maken heeft gehad met een ransomware-aanval. Ook de Autoriteit Persoonsgegevens zegt in 2020 voornamelijk meldingen van datalekken te hebben gehad van grotere organisaties die over veel persoonsgegevens beschikken. Leden van het Verbond van Verzekeraars geven daarentegen aan dat zij zien dat met name de kleinere MKB bedrijven door een afhankelijkheid van een enkel systeem en lage bewustwording slachtoffer worden van ransomware.

Impact van ransomware-aanvallen

Losgeld: Incident response bedrijven geven aan dat het aandeel van de aanvallen waarin tot het betalen van losgeld wordt overgegaan over de jaren 2020, 2021, 2022 flink is gedaald. Ook het cryptobetalingsverkeer laat zien dat er ten opzichte van 2020 en 2021 een omslag is geweest in 2022, waarbij alle slachtoffers samen veel minder losgeld betaald hebben. In de periode van juni 2022 tot juni 2023 zijn er daarnaast 32% van de gepubliceerde organisaties van de website van LockBit verwijderd. Organisaties worden vaak van de website verwijderd als ze losgeld betaald hebben. Dat impliceert dat ongeveer een derde van de LockBit slachtoffers die gepubliceerd zijn alsnog betaald hebben. Hier zat slechts één Nederlandse organisatie tussen. Tegenover de daling in de betalingsbereidheid staat wel een stijging in het gemiddeld betaalde losgeldbedrag in die periode. Uit politieaangiftes blijkt dat de gevraagde losgeldbedragen bij Nederlandse slachtoffers in de handel- en ICT-sector gemiddeld boven de miljoen euro uitkomen. Het betaalde losgeldbedrag bedraagt voor kleine bedrijven een groter percentage van de totale omzet dan voor grotere bedrijven (CBS Cybersecuritymonitor).

Kosten: Naast het betalen van losgeld kunnen ransomware-aanvallen ook andere kosten met zich meebrengen, zoals bijvoorbeeld de verstoring van de bedrijfscontinuïteit, het verlies van klanten door reputatieschade, het herstellen van de IT-systemen of het inschakelen van een incident response bedrijf. De politieaangiftes laten zien dat het gevraagde losgeldbedrag in veel gevallen disproportioneel hoog is en dat de geleden financiële schade door een ransomware-aanval uiteindelijk vaak lager ligt.

Frequentie van ransomware-aanvallen

Volgens rapportages van de verzekeraars (op basis van enquêtes) is 26% van de Nederlandse bedrijven in 2022 getroffen door ransomware. In 2021 en 2022 zijn er respectievelijk 107 en 110 aangiftes van ransomware binnengekomen bij de politie. De politie vermoedt dat slechts 2% tot 4% van de slachtoffers aangifte doet. Dat dit percentage laag is komt ook naar voren uit de CBS Cybersecuritymonitor, waar slechts 13% van de bedrijven aangeeft hulp te hebben gezocht bij de politie. Van de organisaties die bevraagd zijn in de cybersecuritymonitor van het CBS zegt slechts 1% een ransomware-aanval te hebben gehad in 2021. Analyses van berichtgeving in de media suggereert dat ransomware met name een 2021 een groot thema was.

Beperkingen

Geen enkele databron in dit onderzoeksrapport is vrij van beperkingen. Een eerste beperking is de beschikbaarheid van (relevante) data. Een aantal databronnen (zoals de virusscanaanbieders, IT-dienstaanbieders, incident response bedrijven en de cybersecurity-verzekeraars) hebben commerciële belangen. Zij publiceren mede daarom geen ruwe data, maar alleen rapportages. Deze rapportages bevatten vaak figuren en conclusies waarvan de oorsprong lastig te achterhalen is, maar die wel een verhaal vertellen dat de noodzaak van deze partijen onderschrijft. Doordat het ook onduidelijk is op basis van welke data of klantsegment de figuren zijn gemaakt, kunnen de resultaten uit de verschillende databronnen ook niet worden gecombineerd. Daarnaast zijn er partijen als het NCSC en de Autoriteit Persoonsgegevens die momenteel niet aan datadeling doen (de AP geeft echter wel aan hiermee bezig te zijn). Een tweede beperking, die voor de meeste databronnen geldt, is dat de databronnen niet specifiek zijn toegespitst op Nederlandse bedrijven en instellingen. De focus van veel databronnen ligt op Noord-Amerika of is wereldwijd. De enige databronnen zich specifiek focussen op Nederland zijn de politieaangiftes, de datalekmeldingen bij de Autoriteit Persoonsgegevens en de uitkomsten van de CBS Cybersecuritymonitor.

Daarnaast is geen enkele databron volledig. Eerder bespraken we al dat databronnen slechts inzicht kunnen geven in een subset van slachtoffers, maar ook daarin zijn ze vaak niet volledig. Zo doen lang niet alle slachtoffers aangifte van een ransomware-aanval of belanden alle slachtoffers van data-exfiltratie op de websites van ransomware-groepen.

Tenslotte is de kwaliteit van de data in sommige gevallen niet toereikend voor het in kaart brengen van ransomware-aanvallen op Nederlandse bedrijven en instellingen. Het steekproefsgewijs bevragen van Nederlandse organisaties over hun ervaringen met ransomware zou een goed beeld moeten kunnen geven van de problematiek. Echter verschilt het percentage tussen de verschillende enquêtes wel heel erg sterk. Uit de enquêtes van de banken en verzekeraars lijkt de frequentie van ransomware overschat te worden, terwijl deze in de CBS Cybersecuritymonitor juist onderschat lijkt te worden. Het probleem bij de banken en verzekeraars ligt waarschijnlijk in de gekozen steekproef (waar disproportioneel veel slachtoffers inzitten), terwijl die bij de CBS Cybersecuritymonitor mogelijk in de vraagstelling ligt. De meeste resultaten uit de rapportages van commerciële partijen voldoen ook niet aan de standaarden van reproduceerbaarheid, waardoor de kwaliteit van de resultaten niet vast te stellen is.

Aanbevelingen

Een centraal punt waar verschillende instanties hun data (geanonimiseerd en/of geaggregeerd) aan kunnen rapporteren zou enkele beperkingen van databronnen (die nu alleen rapportages uitbrengen) weg kunnen nemen. Incident response bedrijven, die zijn benaderd en in Nederland opereren, zeggen dat ze incidenten melden aan het NCSC. Daarnaast beschikt de Autoriteit Persoonsgegevens over meldingen van datalekken en kunnen slachtoffers in het meldproces aangeven dat het over een ransomware-aanval gaat. Zowel het NCSC als de AP delen deze data nu niet (ook niet met elkaar). Ook zou dit centrale punt bij bijvoorbeeld de virusscanbedrijven specifiek data over Nederlandse klanten uit kunnen vragen en de indexeerwebsites van ransomware-groepen kunnen monitoren voor Nederlandse slachtoffers.

Uit een vooronderzoek bleek al dat CBS-wet grondslag biedt voor verplichte data levering door overheidsorganisaties aan het CBS. Het CBS zou, in ieder geval voor overheidsorganisaties, kunnen fungeren als een centraal punt voor data van ransomware-aanvallen. Deze verplichting geldt niet voor commerciële partijen, zoals de verzekeraars, de virusscanaanbieders en de IT-dienstaanbieders. De overheid moet onderzoeken onder welke voorwaarden deze partijen bereid zijn data te delen over aanvallen op Nederlandse organisaties.

Daarnaast zouden slachtoffers meer gestimuleerd moeten worden om aangifte te doen bij de politie. De informatie die uit politieaangiftes komt is zeer rijk, maar helaas doet maar een klein percentage van de slachtoffers aangifte. Mogelijk zouden de verzekeraars hier een rol in kunnen spelen door een aangifte als voorwaarde te stellen voor het uitkeren van het schadebedrag (zoals bijvoorbeeld ook het geval is bij diefstal).

Tenslotte zou de CBS Cybersecuritymonitor uitgebreid en aangepast kunnen worden. De vraagstelling, en dan met name de gegeven voorbeelden, zijn nu erg beperkend. Ze richten zich bijvoorbeeld uitsluitend op *locker* ransomware (terwijl dat weinig meer voorkomt) en vragen niks over versleuteling van documenten of data-exfiltratie. Ook lijken sommige resultaten te impliceren dat niet de juiste persoon binnen een organisatie de vragenlijst heeft ingevuld. Het uitvragen van het kennisniveau van de respondent zou een juiste interpretatie van de resultaten bevorderen. Ook zou een grotere steekproef gewenst zijn, zodat alle subcategorieën (verschillende vormen van ransomware, losgeldbedragen, wel of niet betaald, gemaakte kosten, maar ook bedrijfssector en -grootte) groot genoeg zijn. Slachtoffers van ransomware zijn mogelijk eerder geneigd deel te nemen aan een enquête over ransomware, dus het zal geen representatief beeld geven van de frequentie van ransomware op

Nederlandse instellingen, maar het zou de verhoudingen binnen de groep slachtoffers wel beter in kaart kunnen brengen.

Voor het vormen van een betrouwbaar beeld aan de hand van bestaande databronnen doen wij op basis van bovenstaande vier concrete aanbevelingen:

1. Onderzoek hoe de barrières voor het delen van data over ransomware slachtoffers, zoals de privacy wetgeving, kunnen worden weggenomen (bijvoorbeeld door anonimisering of aggregatie). Stimuleer vervolgens datadeling van overheidsorganisaties als het NCSC, de Autoriteit Persoonsgegevens en de Politie met een centraal punt als het CBS. Artikel 33 van de CBS-wet biedt grondslag voor verplichte datalevering door overheidsorganisaties aan het CBS. Het combineren (en indien mogelijk koppelen) van data over ransomware van (in ieder geval) de overheidsorganisaties is een belangrijke eerste stap naar het vormen van een beeld van de ransomware problematiek.
2. De overheid moet onderzoeken onder welke voorwaarden commerciële partijen zoals de virusscanaanbieders, IT-dienstaanbieders en de verzekeraars bereid zijn data te delen over aanvallen op Nederlandse organisaties. Dit gebeurt idealiter met hetzelfde centrale punt als waarmee de overheidsorganisaties communiceren. Deze commerciële partijen bezitten informatie die overheidsorganisaties niet kunnen vergaren, maar delen deze data niet en rapporteren hier ook niet of nauwelijks over. Daarnaast zijn de rapportages van deze commerciële partijen opgesteld uit eigen belang en vertellen vaak een eenzijdig verhaal dat erop gericht is meer klanten aan te trekken.
3. Onderzoek op welke manier de aangiftebereidheid onder slachtoffers van ransomware verhoogd kan worden. Er zou bijvoorbeeld onderzocht kunnen worden of verzekeraars hier een rol in kunnen spelen door een aangifte als voorwaarde te stellen voor het uitkeren van het schadebedrag (zoals bijvoorbeeld ook het geval is bij diefstal). Politieaangiftes zijn een zeer rijke bron van informatie als het gaat over de kenmerken van het slachtoffer en de impact van de ransomware-aanval, maar momenteel doet slechts een fractie van de slachtoffers aangifte. Daarnaast worden overkoepelende trends uit de aangiftes over de kenmerken van aanvallen gebruikt door het ransomware *taskforce* om de cybercriminelen op te sporen en uit te schakelen.
4. Benut landelijke enquêtes of monitors als de CBS Cybersecuritymonitor beter door de steekproef te vergroten en de vraagstelling met betrekking tot ransomware uit te breiden en te verbeteren. Het landelijk bevragen van organisaties is een goede methode voor het in kaart brengen van de frequentie van ransomware-aanvallen, de kenmerken van de aanvallen en slachtoffers en de impact van ransomware-aanvallen. De huidige resultaten doen echter vermoeden dat het aantal bevraagde organisaties dat in het afgelopen jaar daadwerkelijk slachtoffer was van ransomware erg klein was. Hierdoor kan op basis van deze resultaten geen betrouwbaar beeld gevormd worden van ransomware-aanvallen op Nederlandse bedrijven. Wanneer een organisatie benaderd wordt voor het invullen van de enquête en aangeeft te maken te hebben gehad met een ransomware-aanval, zouden de kenmerken van de aanval, de kenmerken van het slachtoffer en de impact van de ransomware-aanval in detail en voor zover bekend uitgevraagd moeten worden.