WHITEPAPER

Data-exfiltratie bij een ransomware-aanval

Inhoud

Inleiding

Met deze whitepaper willen we de weerbaarheid van Nederlandse organisaties vergroten. Cybersecurity wordt nog vaak gezien als een 'ver van mijn bed show', waar het management zich niet in hoeft te verdiepen en 'een kostenpost in plaats van een investering'. Cybercriminaliteit treft echter steeds meer organisaties en herstellen van een cyberincident is vele malen duurder dan maatregelen die vooraf kunnen worden ingezet. Via een serie whitepapers, gericht op de doelgroep CISO en security verantwoordelijke, gaan we bewustwording, inzicht én handelingsperspectief bieden van veelvoorkomende schadelijke cyber-manifestaties.

Ransomware, ook wel gijzelsoftware genoemd, is op dit moment wereldwijd de meest voorkomende en meest lucratieve vorm van cybercriminaliteit. Aanvallen vinden op een continue basis plaats en de gevraagde losgelden lopen van enkele tonnen tot miljoenen euro's. Grofweg wordt vaak een bedrag tussen de 0,4 tot 2% van de jaarlijkse omzet als geldbedrag gevraagd. Het afpersen van organisaties levert deze criminele groeperingen dan ook honderden miljoenen op. Het veroorzaakt bij de slachtoffers grote schade, zowel psychologisch als materieel. Daarnaast levert het schade en ongemak op aan organisaties die ketenafhankelijk van het slachtoffer zijn. Daarom spreekt de Nederlandse overheid ook van ransomware als een maatschappij-ontwrichtend probleem.

Een essentieel onderdeel van een ransomware-aanval is het afpersen van het slachtoffer om deze onder druk te zetten om de gevraagde losgeldsom te betalen. Eén van de afpersingsmethoden die door cybercriminelen veelvuldig wordt ingezet is het stelen van data: de data-exfiltratie.

Doel whitepaper: inzicht in en wapenen tegen data-exfiltratie

Dit is het tweede whitepaper in deze serie. De eerste was een top-level document over ransomware dat het fenomeen, de fases van een aanval en de actoren van ransomwarebeschreef. Ook gaf het een aanzet tot de acties die kunnen worden ondernomen om uzelf te wapenen tegen ransomware.[1] Deze serie whitepapers zijn tot stand gekomen met samenwerking van het NCSC, de Nationale Politie, het Openbaar Ministerie en verschillende van onze leden met specifieke kennis en ervaring op incident respons. Met dit whitepaper willen we inzicht verschaffen zodat organisaties over specifieke onderwerpen:

- meer bewustwording krijgen;
- zich er beter tegen beveiligen;
- snel en adequaat handelen wanneer ze slachtoffer zijn.

In dit whitepaper gaan we in op data-exfiltratie bij een ransomware-aanval. We beschrijven het fenomeen data-exfiltratie, delen de kennis die bij de Politie, het NCSC en verschillende cybersecurity bedrijven aanwezig is, laten de verschillende methoden van data-exfiltratie zien en geven een aanzet tot de acties die u kunt ondernemen om zich te wapenen tegen data-exfiltratie.

FASE	IN	DOOR	UIT
OMSCHRIJVING	Alle acties tot en met het succesvol binnendringen van de omgeving	Alle acties om zich binnen de omgeving te bewegen	Alle acties om het uiteindelijke doel te bereiken
VOORBEELDEN	1. Phising 2. Configuratie-fouten 3. Kwetsbaarheden	1. Verhogen van rechten 2. Laterale bewegingen 3. Verkennen gevoelige informatie; financiën	1. Wegsluizen van informatie 2. Versleutelen van bestanden 3. Financiële afhandeling

1. https://cyberveiligheidnederland.nl/upload/userfiles/files/CVNL_Ransomware_def.pdf

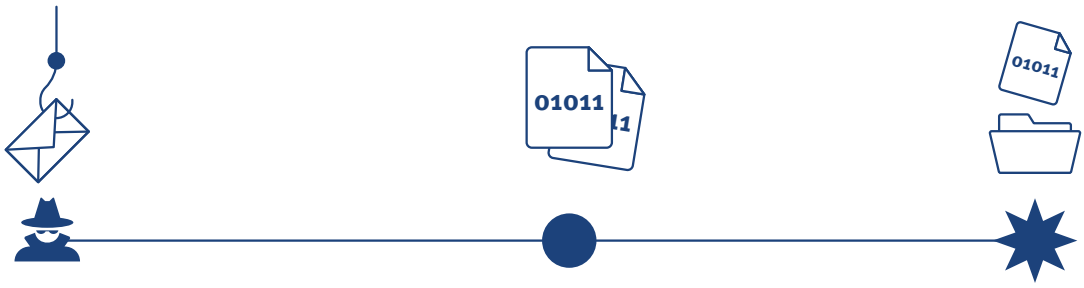
Wat is data-exfiltratie en hoe is het ontstaan?

Data-exfiltratie is een proces tijdens een ransomware-aanval waarbij data wordt gestolen en eventueel openbaar gepubliceerd als het slachtoffer niet betaald. Het doel van aanvallers is dus om druk uit te oefenen op het slachtoffer. Voor het gemak verstaan we onder data-exfiltratie alle stappen van dataverzameling op het netwerk van het slachtoffer, het exfiltreren van die data en publiceren van deze data.

Slachtoffers lijken sneller bereidt te betalen omdat de gestolen data gevoelige (persoons-)gegevens van werknemers en/of klanten kan bevatten. Daarnaast is er angst voor reputatieschade of het verlies van (eigen) intellectuele eigendom aan derden. Een bijkomend voordeel voor aanvallers: soms is de schade van datapublicatie zo groot dat slachtoffers van een ransomware-aanval zelfs betalen als ze de versleutelde bestanden kunnen herstellen met een back-up. Dit maakt het doen van data-exfiltratie aantrekkelijk voor criminelen bij een aanval met digitale afpersing, zoals ransomware.

Organisaties die baat hebben bij het beschermen van (persoons)gegevens zijn extra gevoelig voor data-exfiltratie en afpersing. Denk hierbij aan overheidsorganisaties, de zorgsector, maar ook de (financiële) dienstverlening. Nederlandse voorbeelden waar data-exfiltratie als drukmiddel is ingezet zijn: Gemeente Buren en ROC Mondriaan.

Data-exfiltratie bij een ransomware-aanval ziet er schematisch zo uit:



Voorbereiding

- Data zoeken
- Data verzamelen
- Doelserver en service instellen

Data exfiltreren

- Data exfiltreren
- Verplaatsen en kopieren

Dreigen datapublicatie

- Dreigen slachtoffer
- Datapublicatie

De methodes van data-exfiltratie

Data-exfiltratie is een relatief nieuw fenomeen bij een ransomware-aanval. Rond 2019 worden andere vormen van cybercriminaliteit 'toegevoegd' aan een ransomware-aanval. Dit om de kans te vergroten dat het slachtoffer daadwerkelijk losgeld betaalt. Data-exfiltratie, DDoS-aanvallen[2] en chantage van medewerkers en klanten werden onderdeel van de aanval. Van deze aanvallen komt vooral data-exfiltratie voor bij ransomware-aanvallen.

Wanneer de aanvallers toegang hebben tot het netwerk van het slachtoffer dan zijn er verschillende stappen te onderscheiden die nodig zijn om te komen tot data-exfiltratie:

STAP 1.
Vinden van gevoelige gegevens die gebruikt kunnen worden om slachtoffers onder druk te zetten te betalen. Aanvallers zoeken hierbij naar documenten met woorden als 'financieel', 'vertrouwelijk', 'paspoort' en 'verzekering'. ZIE FIGUUR 1.

STAP 2.
Gereedmaken voor exfiltratie: verpakken van de gevoelige gegevens door de aanvallers om detectie tijdens het exfiltreren te voorkomen. Dit kan gedaan worden met bijvoorbeeld de software 7Zip. De criminelen hebben hier een voorkeur om legitieme tools te gebruiken om detectie te voorkomen. Een ander voorbeeld is Cobalt Strike.[3]

STAP 3.
Het voorbereiden van (externe) servers om de gegevens naar toe te exfiltreren. De aanvaller kan ofwel hun eigen servers gebruiken om de gegevens naar toe te exfiltreren. Deze servers staan, volgens informatie van de Nederlandse politie en incidentresponspartijen bij de volgende services: Mega, Pcloud, Dropbox, Sendspace, Onedrive, GitHub en Google Drive.

STAP 4.
Gebruiken van tools om de gegevens van het slachtoffer te exfiltreren naar de gekozen doelserver of -service. Tools van derden om gegevens naar webservices te uploaden zijn onder meer megasync, rclone, filezilla, stealbit, windows secury copy, ngrok.

STAP 5.
Verplaatsen en kopiëren van de geëxfiltreerde gegevens naar verschillende servers om de sporen tegen de wetshandhaving te verdoezelen en het risico van bevriezing van de gegevens door opsporingsdiensten te verkleinen.

STAP 6.
Het dreigen naar het slachtoffer om de geëxfiltreerde gegevens openbaar te maken wanneer er niet wordt betaald binnen een bepaalde tijd.

STAP 7.
Het openbaar toegankelijk maken van de bestanden van het slachtoffer wanneer er niet wordt betaald. Dit gebeurt via een blog, ook wel leakpage genoemd, een speciale website op het darkweb. Vaak wordt eerst een deel van de gegevens publiekelijk gepubliceerd (sample data) op het 'gewone' internet. Slachtoffers hebben daarna nog enige tijd om te beslissen om te betalen, voordat de gegevens volledig publiekelijk worden gedeeld of worden verkocht op het darkweb. Een andere methode is dat de gegevens van het slachtoffer gratis worden aangeboden op de leakpage van een cybercriminele organisatie. Verschillende cybersecuritybedrijven melden dat er soms extra druk op het slachtoffer wordt gezet door informatie over de publicatie van gegevens op de leakpage onder de aandacht te brengen bij werknemers en klanten. Soms wordt de data ook verkocht aan andere criminelen of aan concurrerende bedrijven. Dit gebeurt wanneer het slachtoffer besluit om niet te betalen. Tot nu toe is er geen bewijs dat dit op grote schaal gebeurt.

[2] Ddos (Distributed Denial of Service). Aanval door een verzameling computers of andere apparaten die tegelijk proberen om een computer(netwerk) of dienstverlening uit te schakelen. Vaak gaat de aanval via een botnet. Uit: https://cyberveilignederland.nl/woordenboek

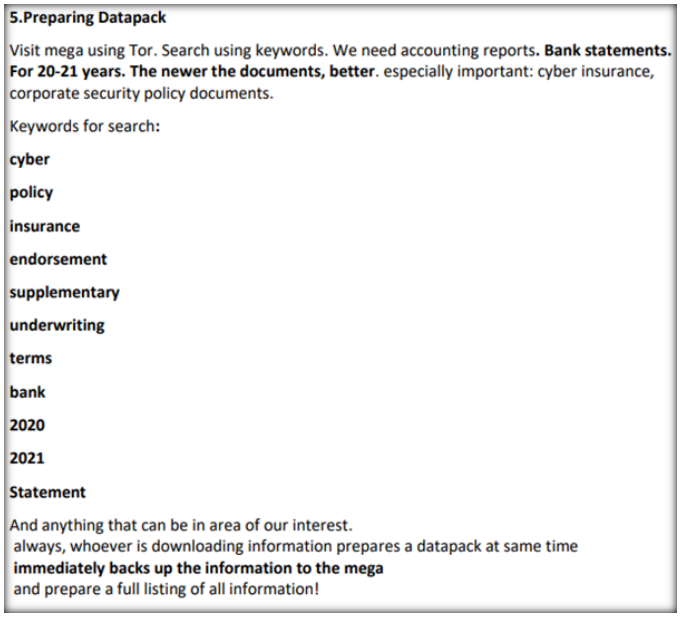
[3] Strategic Cyber LLC. (2022, May). Cobalt Strike User Manual.

Data van incidentresponspartijen

Niet alle slachtoffers van een ransomware-aanval stappen naar de politie om aangifte te doen. Daarom is het ook belangrijk om deze informatie op te vragen bij incidentresponsbedrijven (IR-bedrijven). Verschillende leden van Cyberveilig Nederland hebben hun informatie gedeeld voor dit Whitepaper. De data gaat over de periode 2019-juli 2022. Hieruit blijkt dat de beslissing om al dan niet te betalen verband hield met data-exfiltratie. Twee IR-bedrijven meldden dat data-exfiltratie leidden tot een hogere betalingsbereidheid. Sommige IR-bedrijven melden echter dat betalingsbereidheid alleen afhangt van de beschikbaarheid van goede back-ups. Dit is ook in lijn met onderzoek dat momenteel plaatsvindt aan de Universiteit Twente.[5]

DE BELANGRIJKSTE CONSTATERINGEN ZIJN:

- Ransomware-varianten die vaak data-exfiltratie inzetten: Quantum, Blackcat, Conti, Suncrypt, Clop, Ragnar Locker, Hive en Vice Society. Groepen die tot op heden geen data-exfiltratie gebruiken zijn Phobos/Dharma. Karakurt[6] exfiltreert alleen gegevens;
- Rclone en Megasync zijn de meest gebruikte tooling voor exfiltratie;
- Data-exfiltratie vindt vaak plaats via FTP-servers of malware die ook gebruikt wordt voor data-exfiltratie, zoals Cobalt Strike en/of Qbot.



5.Preparing Datapack

Visit mega using Tor. Search using keywords. We need accounting reports. **Bank statements. For 20-21 years. The newer the documents, better**. especially important: cyber insurance, corporate security policy documents.

Keywords for search:

cyber

policy

insurance

endorsement

supplementary

underwriting

terms

bank

2020

2021

Statement

And anything that can be in area of our interest.
always, whoever is downloading information prepares a datapack at same time
immediately backs up the information to the mega
and prepare a full listing of all information!

Figuur 1. Een handleiding hoe een ransomware-aanval met data-exfiltratie uitgevoerd moet worden door Conti-affiliates is gelekt in 2021. Hier staat omschreven hoe gezocht moet worden naar gevoelige documenten op het netwerk van het slachtoffer, die geëxfiltreerd worden.

[5] T. Meurs, M. Junger, S. Abhishta, and E. Tews (2022). Ransomware: How attacker's effort, victim characteristics and context influence ransom equested, payment and financial loss. In 2022 APWG Symposium on Electronic Crime Research (eCrime). IEEE.

[6] Deze groep is waarschijnlijk een afgeleide van de Conti-groep. Zie hiervoor: https://mobile.twitter.com/contileaks. Bekeken op 31 juli 2022.

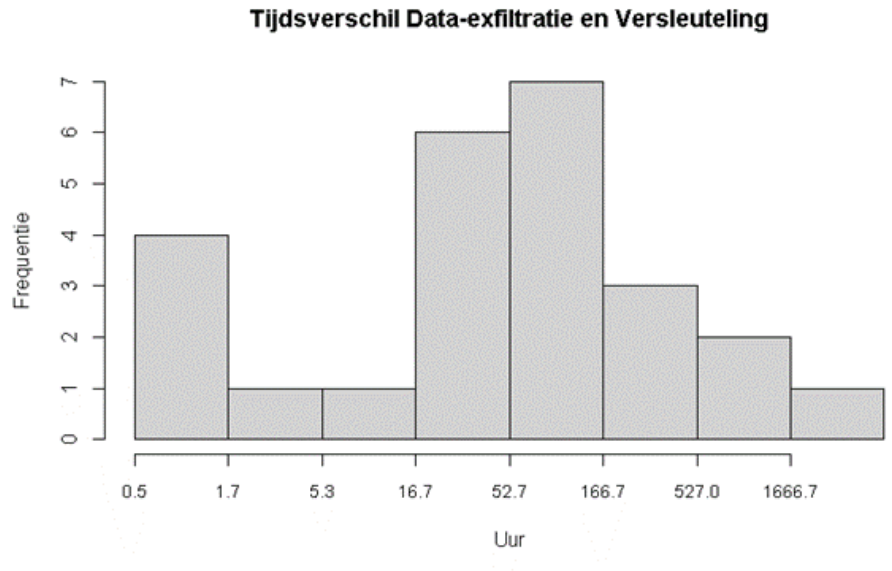
Data-exfiltratie in Nederland (2019-2022)

Politie data

In de periode 2019- juli 2022 zijn 353 ransomware-aanvallen gemeld bij de Nederlandse politie. Hiervan bleek bij 51 gevallen daadwerkelijk data geëxfiltreerd van het slachtoffer. In 73 gevallen kon vastgesteld worden dat zeer waarschijnlijk geen data was geëxfiltreerd. Voor de overige 188 bekende aanvallen is geen informatie over data-exfiltratie beschikbaar.
Verder blijkt uit de gegevens van de Nederlandse Politie dat 21,9% van de slachtoffers betaalde wanneer er data-exfiltratie was, terwijl 27,5% van de slachtoffers betaalde wanneer er geen data-exfiltratie was. Dit lijkt tegenstrijdig, maar het kan op verschillende manieren uitgelegd worden: 1) slachtoffers met data-exfiltratie die hebben betaald zijn mogelijk minder geneigd om naar de politie te gaan, dus ontbreken ze in deze dataset. 2) slachtoffers die betaalden, willen de politie niet vertellen dat ze betaald hebben. 3) de steekproefomvang is klein, waardoor de analyse minder betrouwbaar is.

UIT INFORMATIE VAN DE POLITIE BLIJKT VERDER DAT:

- Mega (50%) het vaakst werd gebruikt om gegevens naar te exfiltreren;
- Rclone (60%) het meest als tooling werd gebruikt om dit te doen;
- Bij data-exfiltratie is gemiddeld 2,917,109 euro losgeld gevraagd en zonder data-exfiltratie gemiddeld 753,342 euro Met andere worden: data-exfiltratie lijkt samen te hangen met meer gevraagd losgeld dan bij een ransomware-aanval dan wanneer (waarschijnlijk) geen data was geëxfiltreerd;
- De bandbreedte van de geëxfiltreerde gegevens tussen de 60 GB en 730 GB lag;
- De bandbreedte tussen het moment van data-exfiltratie en versleuteling verschilt per ransomware-groepering. Hierbij lijkt wel te gelden: hoe professioneler de groepering hoe minder tijd tussen exfiltratie en versleuteling. (zie figuur 2).
- In deze dataset zijn geen gegevens van aanvallen waarbij er data-exfiltratie heeft plaatsgevonden maar geen versleuteling.



FIGUUR 2. Tijd tussen data-exfiltratie en versleuteling. Gemiddeld rond de 40 uur. Deze informatie kan gebruikt worden bij het monitoren van eigen netwerken.

4. Standaardafwijking met data-exfiltratie is 4,937,751 euro en zonder data-exfiltratie 2,727,347 euro.

Wat te doen tegen data-exfiltratie?

Data-exfiltratie tijdens een ransomware-aanval kan veel impact hebben op een bedrijf, naast de impact die de ransomware-aanval zelf al heeft. Zelfs na betaling kan niet uitgesloten worden dat die is buitgemaakt ergens wordt opgeslagen door de criminelen, om eventueel later nog te gebruiken. Daarom is het belangrijk om verschillende (voorzorgs-)maatregelen te nemen. Deze kunnen worden onderverdeeld in algemene maatregelen en maatregelen specifiek gericht op het voorkomen van data-exfiltratie. In het vorige whitepaper zijn we al ingegaan op generieke maatregelen.[7] Verder is het goed om te benoemen dat incidentresponsepartijen hun best doen om de impact van de data-exfiltratie te minimaliseren. Zo monitoren ze voor de klant of en wanneer de data gepubliceerd wordt. Ook kunnen ze bijvoorbeeld contact opnemen met platformen waar data opgeslagen wordt om gestolen data te laten verwijderen, zoals bij de abusedesk van Mega.

Specifieke maatregelen om data-exfiltratie te detecteren, te voorkomen en/of de impact van data-exfiltratie te verkleinen zijn:

MONITORING EIGEN NETWERK.

Het gebruik van uitgebreide detectie en respons (XDR) toepassingen om het gedrag van de actor te detecteren. Aangezien data-exfiltratie voor veel netwerkverkeer zorgt, kan bij goeie monitoring data-exfiltratie in een vroeg stadium onderkend worden.

LOG-RETENTIE.

Sommige criminelen verwijderen de logs na een aanval. Een manier om dit te voorkomen is het maken van back-ups van de logs. Anders is het vaak moeilijk vast te stellen of er data is geexfiltreerd. In de praktijk zien we vaak dat criminelen tijdens onderhandelingen claimen dat data is geexfiltreerd, om zo meer losgeld te kunnen vragen. Het is daarom belangrijk om te kunnen vaststellen of data-exfiltratie heeft plaatsgevonden.

KANARIE-BESTANDEN.

Een mogelijkheid om preventief data-exfiltratie te voorkomen zijn het plaatsen van kanarie-bestanden. Een kanarie-bestand is een nepdocument tussen de echte documenten die een signaal geeft als er ongeautoriseerd data wordt gekopieerd, gemodificeerd of verplaatst. Met een kanarie-bestand valt de detectie van data-exfiltratie enorm te verbeteren.

GEGEVENSBEDROG.

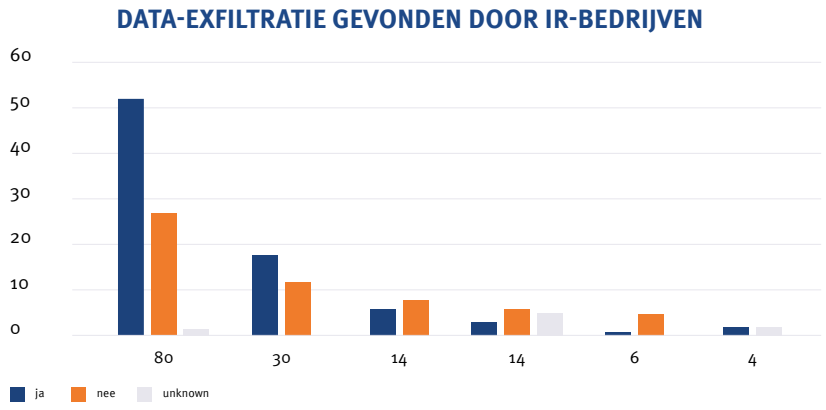
Het zou mogelijk zijn om in eigen data grote hoeveelheden nepgegevens te zetten, zodat criminelen onbelangrijke data exfiltreren. Hoewel nepgegevens of het verbergen van belangrijke data op zich niet voldoende is om data-exfiltratie te voorkomen maak je het voor aanvallers wel moeilijker. Niet alleen moeten de criminelen meer gegevens exfiltreren, waardoor er meer tijd is om de waarschuwingssoftware te laten werken, ook is de marktwaarde van de data belangrijk. Wanneer de data een mix van valse en echte informatie/ data bevat, daalt de marktprijs van de gestolen data.

STANDAARD INTERNETTOEGANG SERVERS BLOKKEREN.

Veel servers hebben vrijwel nooit internet toegang nodig en kunnen zodoende geblokkeerd worden (en eventueel beperkt met een firewall schedule opengezet worden). Het maakt data-exfiltratie niet onmogelijk, maar wel minder makkelijk omdat het extra tijd geeft om (bijvoorbeeld) de transfer van de fileshare server naar het werkstation waarvan exfiltratie kan plaats vinden te detecteren.

BACK-UPS.

Bewaren van een offline of immutable back-ups volgens het 3-2-1 principe: 3 back-ups, op 2 locaties, waarvan 1 offline (buiten het netwerk). Een immutable back-up is een back-up die niet aangepast kan worden, zowel niet door eigen personeel als door aanvallers. Dit is vooral belangrijk tegen ransomware-aanvallen in zijn algemeen, minder voor data-exfiltratie specifiek.



Figuur 3. Ransomware-aanvallen met data-exfiltratie gevonden door 6 IR-bedrijven. Op de X-as het totale aantal ransomware-aanvallen. Frequentie op de Y-as.

[7] https://cyberveilignederland.nl/upload/userfiles/files/CVNL_Ransomware_def.pdf

Melden van data-exfiltratie bij een overheidsinstantie

BENT U SLACHTOFFER GEWORDEN VAN RANSOMWARE?

Een incidentresponsdienstverlener kan u helpen om de impact en duur van het incident zo veel mogelijk te verkleinen. Ook heeft het NCSC een handig Incidentresponsplan Ransomware opgesteld.[8] Wanneer u onderdeel uitmaakt van de Rijksoverheid of valt onder de vitale infrastructuur kunt u ook bij het NCSC terecht bij een ransomware-aanval. Ten slotte, het is verplicht de Autoriteit Persoonsgegevens te informeren wanneer er sprake is van data-exfiltratie, waarbij persoonsgegevens zijn betrokken.[9]

De Nederlandse overheid adviseert altijd om niet te betalen als u slachtoffer bent geworden van een ransomware-aanval. Hoewel de politie adviseert om niet te betalen, begrijpen ze wel dat de beslissing erg ingewikkeld kan zijn. Informeer in ieder geval altijd de Nederlandse politie. Er zijn, naast het doen van aangifte, ook andere manieren om de relevante informatie bij de politie te krijgen. Uw incidentresponspartij kan u hierin adviseren. Mogelijk kan de politie een onderzoek starten. In sommige gevallen kan na betaling het geld teruggevorderd worden. Dit was bijvoorbeeld gelukt na de ransomware-aanval op de Universiteit Maastricht. Geldsporen zijn vaak de enige manier om criminelen op te sporen. Zo hebben het OM en de politie juridische mogelijkheden om in een strafzaak bitcoins te bevriezen. Hierdoor kan het losgeld terug worden gekregen. Zo werd in december 2019 de Universiteit Maastricht aangevallen. Na 3 jaar hard werken heeft de Nederlandse politie de bitcoins in beslag genomen en aan de Universiteit Maastricht teruggegeven.[10]

TOT SLOT: VOORKOMEN IS BETER DAN GENEZEN.

Op de website van het Nationaal Cybersecurity Centrum staan belangrijke maatregelen genoemd die elke organisatie minimaal zou moeten nemen om digitaal weerbaar te zijn tegen een ransomware-aanval.[11] Daarnaast adviseren we om genomen maatregelen te oefenen of te testen zodat u bent voorbereid op een incident. In de praktijk merken we dat bedrijven die een draaiboek hebben gemaakt tegen cyberaanvallen en deze hebben geoefend, sneller en adequater handelen bij een cyberincident. Vaak verlaagt dit de impact van een cyberincident enorm. De Cybersecurity Alliantie heeft een Handreiking Cyberoefenen gemaakt hoe cyberincidenten geoefend kunnen worden.[12] Cybersecurity bedrijven kunnen u helpen met het nemen van cyberweerbaarheidsmaatregelen, maar kunnen ook een incidentresponsplan (helpen) opstellen.

8. https://www.ncsc.nl/documenten/publicaties/2022/juni/3/incidentresponsplan-ransomware
9. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken
10. https://nos.nl/artikel/2434926-universiteit-maastricht-krijgt-losgeld-voor-hack-terug-met-flinke-winst
11. https://www.ncsc.nl/onderwerpen/basismaatregelen
12. https://www.cybersecurityalliantie.nl/producten-tools/handreiking-cyberoefenen

Colofon

Auteurs;

Tom Meurs[13]
Liesbeth Holterman[14]

Jaar van uitgave;
2023

Vormgeving en lay-out;
Cooler Media BV

Dit is een gezamenlijke uitgave van Cyberveilig Nederland, het NCSC, de Politie, het Openbaar Ministerie, Data Expert, Fox-IT, Deloitte, Tesorion, Kennedy Van der Laan, Computest, Northwave, Trellix en NFIR . De inhoud van deze uitgave is met grote zorg samengesteld. Toch kan er onverhoopt een fout of onvolledigheid in zijn geslopen. De betrokken partijen kunnen daarvoor niet aansprakelijk worden gesteld.

Contactgegevens
E-mail: info@cyberveilignederland.nl
Telefoon: 088 - 118 25 10

13. PhD-onderzoeker aan de Universiteit van Twente en de Nederlandse Politie.
14. Strategisch adviseur Cyberveilig Nederland