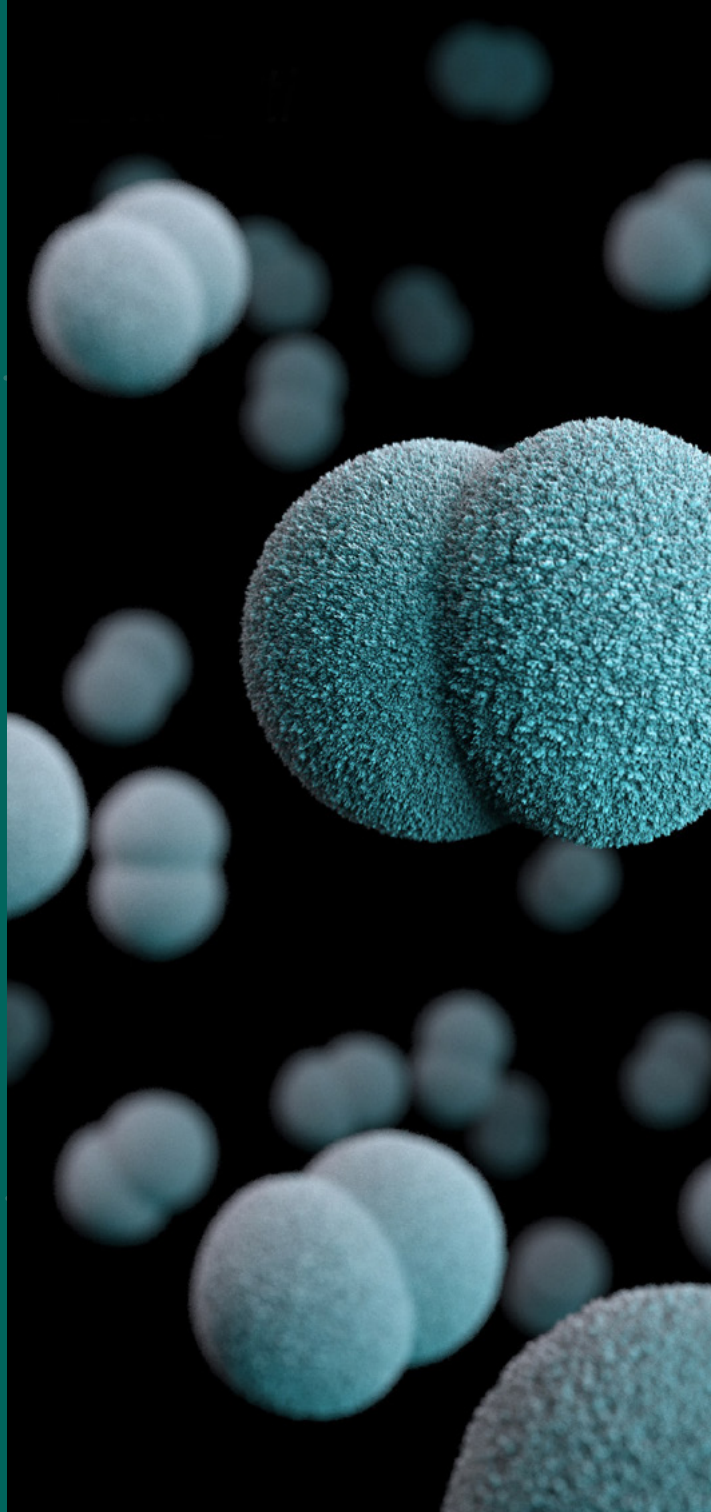
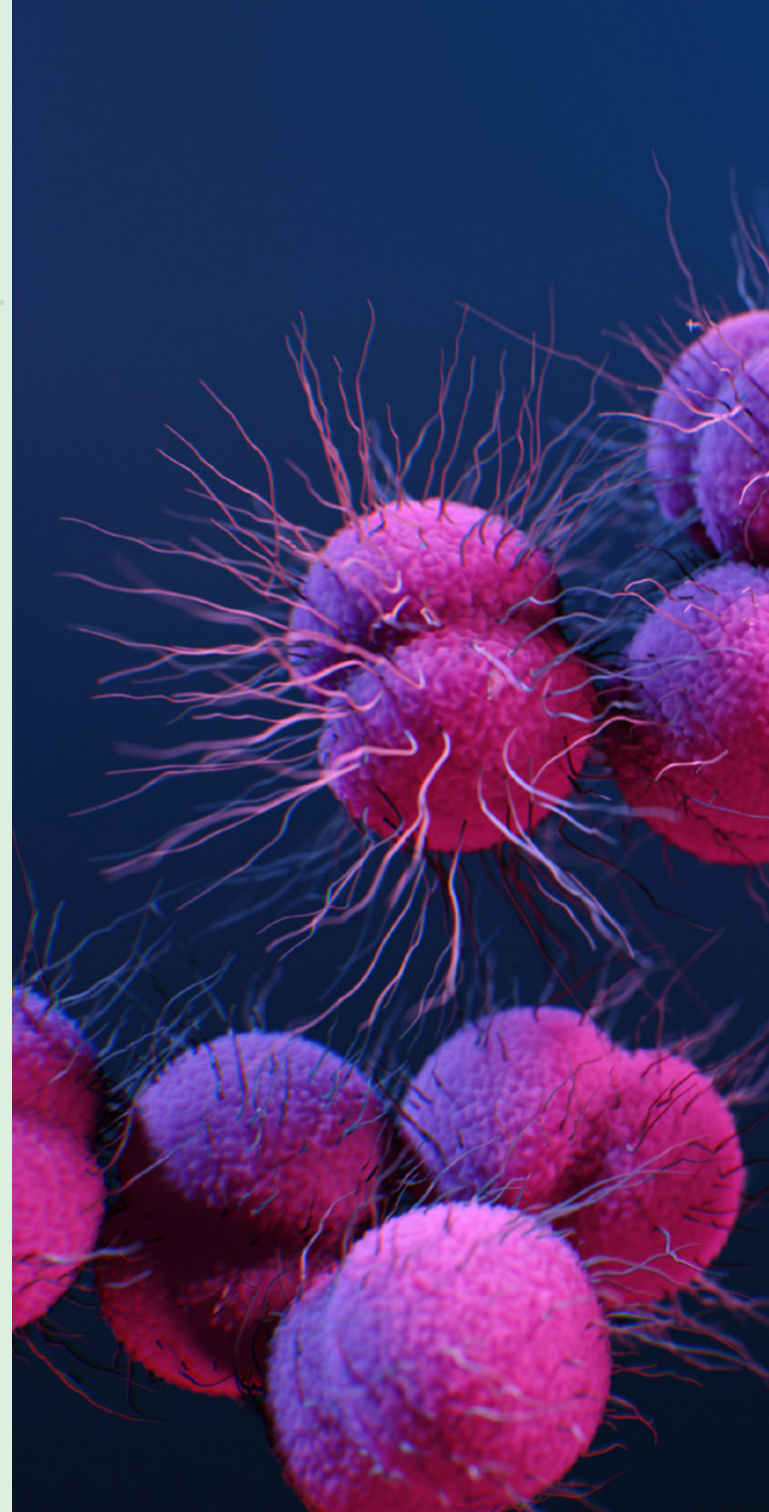
Cybersecurity Dreigingsbeeld Zorg 2021

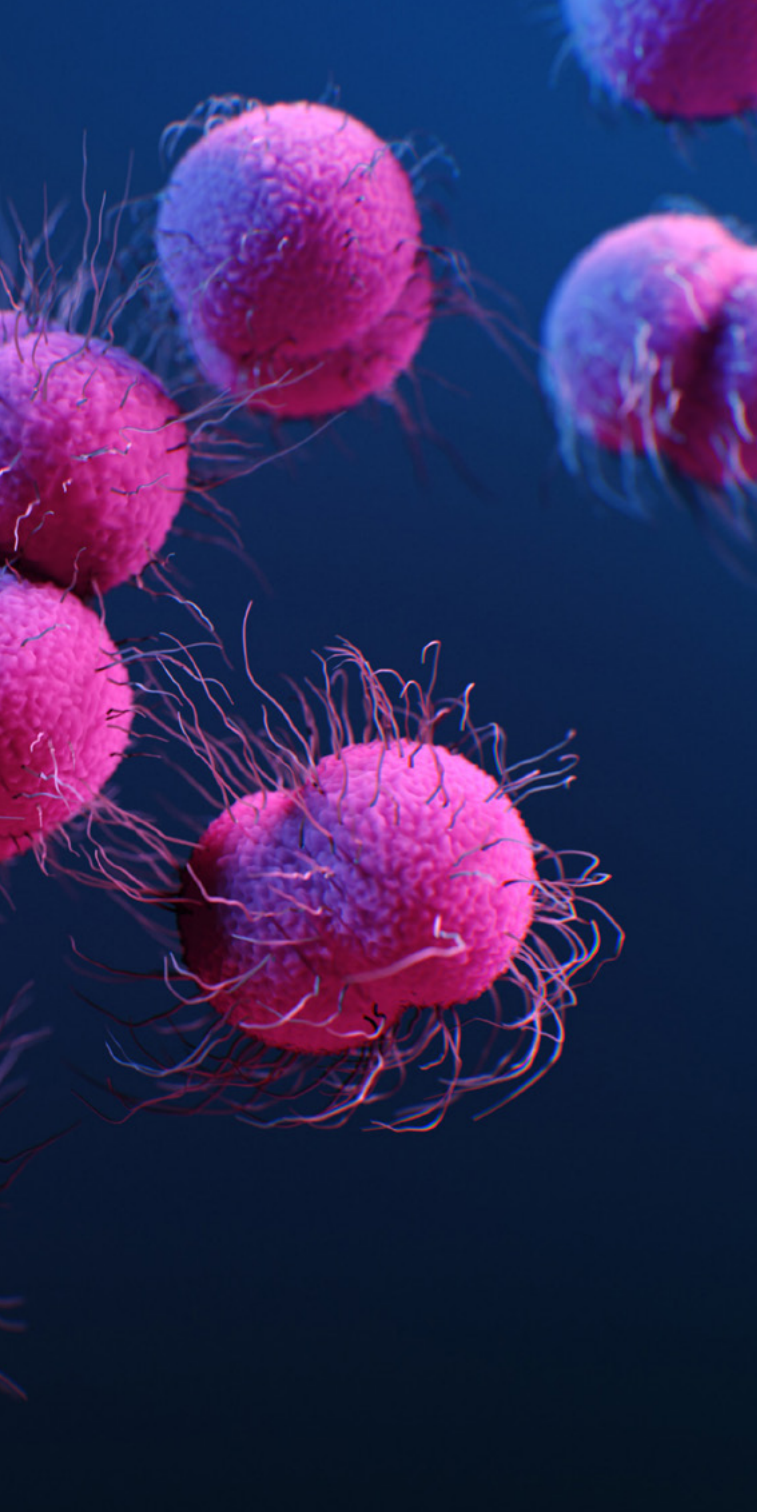
COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

CERT



De missie van Z-CERT is het versterken van de digitale veiligheid van de zorgsector





Inhoud

Colofon

Stichting Z-CERT is hét expertisecentrum op het gebied van cybersecurity in de zorg. Samen met de bij ons aangesloten zorginstellingen, het Nationaal Cyber Security Centrum (NCSC), Health-ISAC (Information Sharing and Analysis Center), brancheorganisaties, leveranciers en andere Computer Emergency Respons Teams (CERTs) vormen we een professioneel netwerk. Met elkaar pakken we cyber-uitdagingen aan, zoals ransomware, phishing, datalekken en hacken.

Z-CERT is in 2017 opgericht op initiatief van de Nederlandse Vereniging van Ziekenhuizen (NVZ), Nederlandse Federatie van Universitair Medische Centra (NFU) en de Nederlandse GGZ. Z-CERT is een stichting en heeft geen winstoogmerk.

In dit Cyberdreigingsbeeld voor de Zorg 2021 beschrijven we de belangrijkste gevaren voor de Nederlandse zorgsector. We putten hierbij uit meldingen van deelnemers, informatie van (inter)nationale partners en kennisinstituten, eigen bevindingen, interviews met deskundigen, literatuuronderzoek, een enquête onder zorginstellingen en research van (open) bronnen.

Het dreigingsbeeld is opgebouwd uit columns, thema's en mogelijke gevaren. Bij de hoofdstukken delen we onze ervaringen en tips in de hoop dat deze de lezer inspireren, bewust maken en aanzetten tot het nemen van maatregelen.

Voorwoord

Voor u ligt het tweede cyberdreigingsbeeld voor de zorg. Niet alleen bevat deze editie meer dreigingsinformatie en meer incidenten dan de vorige uitgave, maar ook meer statistieken en tips. Dat betekent ook meer tekst en bladzijden, dus ga er goed voor zitten.

Ik ben er bijzonder trots op dat voor deze editie bijna honderd instellingen uit de geestelijke gezondheidszorg, ziekenhuizen, verzorgings- en revalidatiecentra hun incidentdata in detail met ons wilden delen. Zoals iedereen zal beamen, is informatiedeling een belangrijk onderdeel in de strijd tegen cybercrime. Wij hopen dat deze transparantie over cybersecurity-incidenten doorzet de komende jaren.

Vele tientallen deelnemers en meerdere leveranciers hebben openheid van zaken gegeven in een online-enquête en tijdens interviews met onze security-analisten. De zorg-CISO's (Chief Information Security Officers) deelden informatie over incidenten, beveiligingsmaatregelen en incident respons. Waardevolle informatie waarmee we een accuraat en actueel beeld kunnen schetsen.

Naast onze deelnemers hebben we een aantal belangrijke spelers uit de zorg gevraagd hun visie te geven op cybersecurity. Mijn dank gaat dan ook uit naar de CISO van 's Heerenloo, Daan Brinkhuis en tot slot de Chief Financial Officer (CFO) van het Radboudumc, Mark Janssen. Hun persoonlijke ervaringen maken het dreigingsbeeld compleet en geven meer duiding aan alle cijfers.

Naast de dreigingen valt er namelijk ook genoeg positief nieuws te melden. Zo maken steeds meer zorginstellingen werk van cybersecurity en informatiebeveiliging. Geen dag te laat, want de dreiging van ransomware is groter dan ooit. In 2020 lazen we nog berichten dat cybercriminelen de zorg zouden ontzien in verband met de pandemie, maar daar hebben we in 2021 helaas weinig van gemerkt. In oktober 2021 hebben we op onze website (www.z-cert.nl) een teller gelanceerd. Die geeft aan hoeveel ransomware-incidenten binnen de zorg hebben plaatsgevonden, in Nederland en in Europa.

> **"Steeds meer zorginstellingen maken werk van cybersecurity en informatiebeveiliging."**

Elke aanval is er natuurlijk één te veel. Daarom blijven we strijden tegen cybercrime door het delen van de dreigingsinformatie. Dat doen we elke dag via het ZorgDetectieNetwerk en onze kennisproducten, en vandaag ook via dit Cyberdreigingsbeeld voor de zorg 2021.

Wim Hafkamp
directeur Z-CERT

“ Ransomware is de grootste digitale dreiging voor de zorgsector. ”

06

dreiging

Ransomware

Ransomware of gijzelsoftware is een door hackers gebruikt chantagemiddel. Het is de grootste digitale dreiging voor de zorgsector, zo blijkt.

Incidenten in de Nederlandse en Europese zorgsector

De dreiging met ransomware is in 2021 gegroeid. Het aantal ransomware-incidenten in de Europese zorgsector steeg explosief. Kwamen er in 2020 nog één of enkele incidenten per kwartaal in de publiciteit, in 2021 waren dat er vijf tot zes per kwartaal. In 2021 zijn, voor zover bekend bij Z-CERT, 31 zorginstellingen in Europa getroffen door ransomware, dat werkte door naar in totaal 116 zorglocaties.

Ook in Nederland steeg het aantal ransomware-aanvallen. Voor zover bekend bij Z-CERT zijn in Nederland in 2021 vijf zorginstellingen geraakt. Dat is vier meer dan in 2020. Hierbij ging het om instellingen in de ouderenzorg, thuiszorg, gespecialiseerde zorg en twee categorale zorginstellingen. Bij twee incidenten bleef de schade beperkt door tijdig ingrijpen.

Ransomware-incidenten bij leveranciers

De meeste ransomware-incidenten met doorwerking naar de zorg, vonden plaats bij leveranciers. Uit onderzoek van Z-CERT blijkt dat zestien Nederlandse zorginstellingen in 2021 hinder hebben ondervonden van ransomware-incidenten bij een leverancier en in één geval bij een subleverancier. Van de zestien kregen vijf instellingen zelfs met meerdere incidenten te maken. De incidenten leidden tot datalekken, vertragingen in leveringen, stagnatie van onderhoud, maar ook ernstige verstoringen van operationele processen. Vaak was er sprake van een domino-effect en was er daardoor impact op meerdere zorginstellingen (*kader 1*).

> **“De meeste ransomware-incidenten vonden plaats bij leveranciers.”**

Z-CERT stelt vast dat dit domino-effect ook speelt op kleinere schaal bij zorgorganisaties met meerdere locaties (zogenaamde zorggroepen) met een gedeelde IT-afdeling. Bij een besmetting met ransomware ondervinden alle locaties hinder. In Europa waren er in 2021 vier voorbeelden van, waarbij er impact was op meer dan honderd zorglocaties (*kader 2*).

Kader 1: Voorbeelden van leveranciers in de zorgsector die in 2021 werden geraakt door ransomware, waarbij het incident impact had op meerdere zorglocaties in Nederland.

Organisatie	Impact
ERP-clouddienst	Twee zorginstellingen hadden enkele dagen geen toegang tot het ERP-systeem (Enterprise Resource Planning). Hierdoor moesten bestellingen via een omweg worden gedaan. Ook kon het voorraadbeheer en de logistieke afhandeling niet worden ingezien.
Subverwerker van een data-analysebedrijf	Patiëntendata van vier laboratoria waren ontoegankelijk.
Leverancier medische apparaten	Leverancier kon bepaalde onderhoudstaken niet uitvoeren doordat het ziekenhuis uit voorzorg de VPN-verbinding dichtzette.
Organisatie voor professionele ontwikkeling	Niet-gevoelige data van meer dan twintig zorgorganisatie werden versleuteld.
Toeleverancier kantoorartikelen	Nihil, alleen vertragingen van leveringen.
Ziekenhuizen en GGZ-instellingen	Verschillende leveranciers en zorginstellingen namen met spoed preventieve maatregelen, omdat er een kwetsbaarheid was in Kaseya VSA die op grote schaal werd misbruikt door een ransomware-groep.

Kader 2: Voorbeelden in 2021 van ransomware-incidenten in de Europese zorgsector met impact op meerdere zorginstellingen.

Organisatie	Land	Impact
SRH-Holding (ziekenhuizen en revalidatieklinieken)	Duitsland	Elf vestigingen waren meerdere weken offline [1].
Pallas Kliniken (schoonheidsklinieken)	Zwitserland	Twintig klinieken werden getroffen, bijna twee weken diverse verstoringen [2].
La Fondation Santé des Étudiants (jeugdzorg en GGZ)	Frankrijk	Dertien klinieken werden getroffen [3].
ASL Roma 3 (gezondheidscentra en ziekenhuizen)	Italië	In totaal werden 46 vestigingen getroffen.

Impact van ransomware op een organisatie

De headlines in het nieuws zeggen veel over de impact van een ransomware-aanval: “Revalidatieklinieken en ziekenhuizen terug naar pen en papier” [1], “Ambulances moesten uitwijken naar een ander ziekenhuis” [4],”De eerste hulp bijna twee weken dicht na aanval” [4], en “GGZ-instelling stelt 35.000 cliënten op de hoogte dat persoonlijke data is gelekt” [5]. Het zijn allemaal gevolgen van ransomware-incidenten waarbij toegang werd verkregen tot cruciale systemen en zorgprocessen werden verstoord of data werd gestolen. Cybercriminelen sturen hier bewust op aan, hoe groter de ontwrichting, hoe groter de kans op betaling.

Losgeld gebaseerd op bedrijfsomzet

Cybercriminelen eisten van hun slachtoffers gemiddeld in Q3 2021 bijna 140.000 dollar losgeld [6]. Het gevraagde bedrag hangt uiteindelijk af van de bedrijfsomzet. De cybercriminelen proberen op basis van deze informatie te schatten hoeveel losgeld zij denken te kunnen eisen. Om hun eisen kracht bij te zetten, is het inmiddels gemeengoed geworden dat de criminelen dreigen om buitgemaakte data te lekken of te verkopen. Ook wordt het slachtoffer met naam en toenaam gepubliceerd op een publiek toegankelijke website waarbij in sommige gevallen zelfs de pers of samenwerkingspartners worden ingelicht [8]. Dit alles om extra druk uit te oefenen.

Hoge herstelkosten

Los van de betaling, zijn er ook nog de herstelkosten. Een ransomware-incident kan zoveel schade veroorzaken dat (een deel van) de IT-infrastructuur opnieuw moet worden opgebouwd. Nederlandse organisaties waren gemiddeld 2,3 miljoen euro kwijt om te herstellen van een ransomware-incident [7]. Bij dat bedrag zijn betaling, downtime, personeelskosten, gederfde inkomsten (lost opportunity) en materiaalkosten meegerekend.

Niet alle data wordt hersteld

De gemiddelde duur van de verstoringen is 22 dagen [6]. Daarnaast gaat er veel tijd zitten in het informeren van patiënten en cliënten waarvan mogelijk data is gelekt. Ook als het losgeld is betaald, bestaat de kans dat niet alle data kan worden hersteld [9]. Uit onderzoek onder ransomware-incidenten uit de zorg, bleek dat bij de slachtoffers gemiddeld 69 procent van de data kon worden hersteld na het betalen van de losprijs [9]. Een cyberverzekering neemt misschien een deel van het financiële risico voor zijn rekening, maar de risico’s op langdurige verstoringen en dataverlies blijven. Daarnaast houdt betaling het verdienmodel van de crimineel in stand.

Cyberweerbaarheid tegen ransomware-aanvallen

Het verbeteren van de cyberweerbaarheid tegen ransomware-groepen is voor zowel grote als kleine organisaties belangrijk. De meeste ransomware-aanvallen waren in Q3 2021 bij organisaties tussen de 11 en 1.000 werknemers. Zij incasseerden in het derde kwartaal van 2021 78,3 procent van de ransomware-incidenten [6]. Een groot deel van de ransomware-aanvallen is niet doelgericht [10]. Dit heeft als voordeel dat de initiële aanvalsmethoden vaak te voorspellen zijn. Z-CERT constateert dat bij veel van de ransomware-incidenten drie methoden worden gebruikt om binnen te dringen [6]:

1. Verleiden van gebruikers om kwaadaardige software (malware) op te starten.
2. Inloggen op RDP (mogelijkheid binnen Windows om op afstand computer over te nemen) met gestolen of geraden inloggegevens.
3. Aantasten van systemen door misbruik te maken van kwetsbaarheden in de software.

Methode 1: Verleiden van gebruikers om kwaadaardige software (malware) op te starten

Het is niet ongebruikelijk dat een middelgrote zorginstelling tussen de 75 en 200 besmette mails per maand ontvangt. Niet altijd wordt de malware gedetecteerd door de mailgateway, web proxy of virusscanner. Bij uitvraag bij 92 deelnemers werden 37 malware besmettingen gemeld verdeeld over zestien instellingen. Een deel van deze malware wordt ook gebruikt door ransomware-groepen. Zorginstellingen nemen daarom vaak aanvullende maatregelen om de uitvoering van malware te voorkomen. Om vast te stellen hoever we in de zorg op dit gebied zijn, hebben we een enquête gehouden:

Top 3 aanvullende securitymaatregelen
Van de ondervraagde zorginstellingen, heeft ...

1. 64 procent applicatie-whitelisting/allow-listing toegepast op gebruikerscomputers.
2. 59 procent het gebruik van Office-macro's gereguleerd.
3. 47 procent een Endpoint Detection and Response (EDR) oplossing draaien.

Dit zijn positieve cijfers voor de zorg, maar er is meer winst te behalen. Alleen vertrouwen op de spamfilter, web proxy, sandboxing of virusscanner blijkt gezien de hoeveelheid incidenten lang niet altijd voldoende. Het hebben van een Endpoint Detection and Response oplossing helpt om een hacker te detecteren die niet wordt gezien door de antivirusoplossing. EDR helpt ook om snel maatregelen te treffen in geval van infectie.

Methode 2: Misbruiken van oplossing om op afstand computer over te nemen

Systeembeheerders gebruiken vaak een oplossing om op afstand beheer-activiteiten uit te voeren, RDP genoemd. Helaas hebben kwaadwillenden dit door en proberen ze op deze systemen op grote schaal gebruikersnamen en wachtwoorden uit. Als een systeembeheerder een eenvoudig te raden wachtwoord gebruikt, wordt de server gecompromitteerd. Z-CERT zag dat in 2021 RDP-inloggegevens van zorginstellingen werden verhandeld op het dark web.

Van de ransomware-incidenten in 2021 had 40 procent voorkomen kunnen worden als de RDP niet was ontsloten via internet [6].

Het is daarom belangrijk om regelmatig te controleren of de RDP-oplossing niet 'per ongeluk' door iemand is aangezet. Een open verbinding in combinatie met een slecht wachtwoord zet de deur wagenwijd open voor criminelen. Z-CERT zag het afgelopen jaar daar gelukkig weinig voorbeelden van in de zorg.

Methode 3: Misbruiken kwetsbare systemen

Zo'n 15 procent van de ransomware-incidenten vindt zijn oorsprong in het misbruiken van kwetsbaarheden [6]. Veel van die misbruikte kwetsbaarheden zijn bekend en hadden verholpen (gepatched) kunnen zijn. [11].

Z-CERT ziet dat vooral kleinere zorginstellingen kwetsbare systemen lang ongepatched laten.
Dat creëert een groot risico, omdat de kans op misbruik toeneemt in de tijd. In 2021 werd het een aantal keer spannend, omdat er actief kwetsbaarheden in de mailoplossing van Microsoft (Exchange) misbruikt werden door ransomware-groepen.

Gelukkig scant 64 procent van de ondervraagde zorginstellingen de buitenkant van hun IT-infrastructuur op kwetsbaarheden en afwijkingen. Fouten die dan worden gemaakt bij patchen en systemen die per abuis niet zijn gepatched, komen zo bovendrijven. De ervaring is dat veel zorginstellingen snel patchen en snel adequaat reageren op dreigingsinformatie.

Zero-day kwetsbaarheden

Sommige ransomware-groepen gebruikten in 2021 een 'zero-day exploit'. [12] [13] [14]. Een exploit is een stuk software waarmee je een kwetsbaarheid kan misbruiken en zo bijvoorbeeld een systeem kan overnemen.

Bij een zero-day is er al een exploit die wordt gebruikt door hackers. De softwareleverancier heeft alleen nog geen updates ter beschikking gesteld en weet in veel gevallen zelfs niet dat de kwetsbaarheid bestaat. Dat maakt iedereen die het product gebruikt, kwetsbaar voor een aanval.

> **"Een exploit is een stuk software waarmee je een kwestbaarheid kan misbruiken en zo bijvoorbeeld een systeem kan overnemen."**

Het percentage zero-days dat door ransomware-groepen wordt gebruikt, is relatief klein. De dreiging werd in 2021 voor de zorgsector concreet toen een ransomware-groep een zero-day exploit misbruikte voor een kwetsbaarheid in het product Kaseya VSA (zie pagina 13, kader Kaseya).

De budgetten waarmee ransomware-groepen tegenwoordig werken, maakt het voor hen ook mogelijk om zero-day exploits te kopen op het dark web of zelf exploits te ontwikkelen [15]. De verwachting is dat het gebruik van zero-day exploits door ransomware-groepen aanhoudt of verder toeneemt.

De toekomst

In 2021 versterkten politie en overheden op internationaal niveau de samenwerking tegen cybercrime. Criminelen werden opgepakt [16] [17] [18], infrastructuur van ransomware-groepen en partners werd onschadelijk gemaakt [19] [20] en geld werd in beslag genomen [17] [21]. In oktober 2021 maakten dertig regeringsleiders afspraken over het actief bestrijden van ransomware-groepen [22]. Z-CERT verwacht daarom dat de aandacht

voor ransomware-groepen vanuit opsporings- en inlichtingendiensten komende jaren verder toeneemt.

Maar zolang er veel geld kan worden verdiend met cybercrime, verwacht Z-CERT niet dat de dreiging afneemt. Naar aanleiding van de acties van onder meer de Amerikaanse regering beloofden sommige ransomware-groepen geen zorginstellingen meer aan te vallen [21]. Dat zijn mooie voornemens, waardoor Z-CERT alleen niet wordt gerustgesteld. De goud-koorts onder ransomware-groepen is namelijk zo hevig dat de zorg nog altijd prominent in de ransomware-statistieken terugkomt [6] [7].

Advies
in dit dreigingsbeeld hebben we een top 10 opgenomen met maatregelen die in de praktijk de meeste aanvallen door ransom-ware-groepen tegenhouden en de netwerkinfiltratie bemoeilijken [26]. Daarnaast is het goed om over de hele breedte te kijken welke maatregelen er nodig zijn. Er zijn verschillende whitepapers beschikbaar die u hiermee verder kunnen helpen [27] [28].
Wat verder opvalt in 2021 is dat ransomware-groepen steeds sneller tot hun doel komen als ze eenmaal een netwerk zijn binnengedrongen. Het is daarom belangrijk om met uw technische staf na te gaan of uw netwerk makkelijk te infiltreren is. Controleer ook of het voor hackers eenvoudig is om wachtwoorden en andere authenticatieobjecten of rechten te stelen en te misbruiken. De maatregelen die u vervolgens neemt, zijn vaak kosteloos.

Wel vergt het nemen van de juiste maatregelen kennis en begrip van de methoden die hackers gebruiken. Als u dat duidelijk heeft, kunt u de aanvallers raken waar het hen het meest pijn doet [29]. Zo vergroot u de kans dat de aanvaller afhaakt of wordt gedetecteerd.

Voorbeelden van praktische gidsen die u helpen netwerkinfiltratie te bemoeilijken:

- **Windows Credential Theft Mitigation Guide Abstract [30]**
- **Ransomware Protection and Containment Strategies [31]**
- **Restricting SMB-based lateral movement in a Windows environment [32]**

Ransomware as a Service (RaaS)

Anatomie van een ransomware-groep

Ransomware-groepen hanteren verschillende organisatiestructuren en modellen. De dominantste op dit moment is het Ransomware as a Service model (RaaS). In dit model werken individuen en groepen mensen samen. Ze delen de opbrengsten met elkaar. Hoe werkt RaaS?

Efficiënter zonder randzaken

Een hacker of groep hackers verbindt zich als een 'affiliate' aan een cybercrime groep die 'Ransomware as a Service' aanbiedt; de ransomware-operator. Deze professionele dienstverlener neemt een hacker allerlei zaken uit handen om zo de overhead te verminderen. Denk aan het ontwikkelen en onderhouden van de ransomware-software, financiële zaken, IT-infra-structuur, helpdeskactiviteiten en het bijhouden van een datalekwebsite. Alles wordt voor de hacker geregeld. Als ze erin slagen om een slachtoffer losprijs te laten betalen, mogen ze zelf vaak tussen de 75 tot 90 procent houden. De rest gaat naar de ransomware-dienstverlener [23]. In dit model hoeft de hacker zich niet bezig te houden met randzaken, waardoor hij een stuk effectiever wordt.

Korter aanwezig in netwerk

In 2021 is de effectiviteit van ransomware-operaties toegenomen.
Bij 50 procent van de ransomware-incidenten waren de hackers slechts vijf dagen of minder in het netwerk aanwezig [8]. Soms werden ze snel gedetecteerd, maar een andere mogelijke reden van de korte verblijfsduur, is dat hackers meer gebruikmaken van 'Initial Access Brokers' (IAB). Dit zijn hackersgroepen die maar één doel hebben: toegang krijgen tot het netwerk van een organisatie. Die toegang verkopen ze vervolgens, als een gespreid bedje, door aan andere cybercriminelen. Soms werken deze IAB's exclusief voor een ransomware-operator of bieden ze accounts met hoge rechten aan op het dark web. Een andere oorzaak waardoor hackers steeds sneller worden, is dat ransomware-operators actief investeren in functionaliteiten in hun software om bepaalde taken te automatiseren [24] [25].

Kaseya is een beheer- en monitoringtool die door IT-providers gebruikt wordt om servers en gebruikercomputers van klanten te beheren. De ransomware groep REvil slaagde erin tegen de 60 van deze IT-providers te compromitteren door gebruik te maken van een toen nog niet publiek gemaakte kwetsbaarheid (zero-day) in de Kaseya software. De criminelen versleutelden de systemen van hun klanten wat gevolgen had voor bijna 1500 organisaties. Ondanks dat Kaseya software ook wordt gebruikt door leveranciers van de zorgsector in Nederland werden er geen Nederlandse zorginstel-lingen geraakt door deze aanval. Kaseya had kunnen uitlopen op een ramp. De enige reden waarom dit niet is gebeurd, is omdat de Nederlandse leveranciers voor de zorg Kaseya niet aan het internet ontsloten hadden waardoor de criminelen de kwetsbaarheid niet konden misbruiken [74].

thema

Het risico van de cloud

Overwegingen bij leveranciersmanagement van SaaS-leveranciers

De Geestelijke Gezondheidszorg (GGZ) en in mindere mate de ziekenhuizen maken een beweging naar de cloud. Verpleeg- en Verzorgingshuizen en Thuiszorg (VVT), Jeugdzorg, Gehandicaptenzorg en categorale instellingen lijken dezelfde lijn te volgen als de GGZ. In de public cloud bestaan nieuwe risico's. Veel infrastructuur, managementinterfaces en applicaties waren vroeger alleen toegankelijk vanaf het eigen netwerk. Met de cloud zijn zij nu vaak via het internet te benaderen, voor iedereen die dat wil.

Voorbeelden van risico's die vooral spelen in de cloud (Software as a Service - SaaS en Platform as a Service - PaaS):

1. Publiekelijk toegankelijke infrastructuur en applicaties worden dag en nacht gescand door kwaadwillenden op kwetsbaarheden, misconfiguraties en gebruik van zwakke wachtwoorden. Servers die een bekende kwetsbaarheid bevatten, worden veelal binnen 24 uur gecompromitteerd, soms zelfs binnen enkele minuten [33]. Vaak hebben SaaS-leveranciers hun infrastructuur verborgen achter een Firewall of Load Balancer. Soms zijn ook servers en remote managementdiensten toegankelijk via het internet. Dit is een risico.

2. De infrastructuur en applicaties die voor iedereen toegankelijk zijn in de cloud zijn kwetsbaar voor DDoS-aanvallen.

3. In sommige gevallen host een clouddienst meerdere klanten op dezelfde achterliggende infrastructuur. Daardoor kan het voorkomen dat data en applicaties onvoldoende van elkaar zijn gescheiden. In geval van een kwetsbaarheid of misconfiguratie kan data van andere klanten worden ingezien.

Bij veel leveranciers zijn dit soort risico's afgedekt. Bij de partijen die bijvoorbeeld van oorsprong softwareontwikkelaars waren en minder hun focus hadden op infrastructuur en de beveiliging daarvan, kunnen hier wel hiaten ontstaan. Z-CERT constateerde bij sommige leveranciers remote managementtools zonder multifactorauthenticatie of verouderde software. In het licht van het huidige dreigingsbeeld en de verantwoordelijkheid voor meerdere zorginstellingen, is dit onacceptabel.

Wanneer een zorginstelling overstapt naar de cloud, krijgt die ook te maken met de dreigingen die gericht zijn op Internet Service Providers. De DDoS-dreiging op zorginstellingen zelf is relatief klein (zie hoofdstuk

over DDoS), maar bij overstap op de public cloud wordt deze dreiging veel groter. Ook cybercriminelen weten de weg naar de cloud te vinden en weten dat ze door het raken van IT-providers met meerdere klanten, veel geld kunnen verdienen. Het ransomware-incident bij een ERP-leverancier en een analysebedrijf voor patiënt- en cliëntdata waren daar in 2021 een voorbeeld van (zie hoofdstuk over ransomware).

Uitdagingen in de cloud: leveranciersmanagment

Zorginstellingen blijven verantwoordelijk voor de beveiliging van hun data, ook al staat deze bij een leverancier. De NEN-7510 schrijft voor dat zorginstellingen hun leveranciers met regelmaat moeten monitoren, beoordelen en auditen (beheersmaatregel A.15.2.1). Veel zorginstellingen zien dit als een uitdaging en zien hier ruimte voor verbeteringen (zie ook de column van Daan Brinkhuis in dit dreigingsbeeld). Zij gaan het gesprek aan met leveranciers over dreigingen en maken afspraken over bijvoorbeeld offline back-ups. De helft van de bevraagde zorginstellingen doet dit al. Ook verlangen zij rapportages met de juiste scope en diepgang. Als de zorg dit soort zaken consequent uitvraagt, verhoogt dit de weerbaarheid en herstelvermogen van leveranciers.

Een effect van goede afspraken maken, was in 2021 te zien bij de Kaseya-hack (zie hoofdstuk over ransomware). Leveranciers hebben een ramp voorkomen door de beheertool van Kaseya niet aan het internet te ontsluiten. Hadden ze dat wel gedaan, dan waren vele kritieke systemen in zowel ziekenhuizen, GGZ en gehandicaptenzorg hard geraakt, inclusief het Elektronisch Patiënten Dossier in een ziekenhuis en het Elektronisch Cliënten Dossier in een GGZ-instelling.

Te weinig capaciteit

Een risico bij de wettelijke verplichting op controle van leveranciers is dat sommige CISO's aangeven te weinig tijd te hebben om dit onderdeel van de NEN-7510 naar behoren uit te voeren. Vanuit de organisatie moet een CISO hier genoeg ondersteuning bij krijgen. Meer cloud betekent, meer leveranciersmanagement, en dat houdt meer werkdruk in. Z-CERT beoordeelt dit als een risico. Een CISO van een zorginstelling moet een vinger aan de pols kunnen houden bij leveranciers en kunnen bijsturen zodra risicotoleranties worden overschreden.

> **"Z-CERT ontwikkelt kennisproducten om de gehele keten van zorginstellingen en leveranciers cyberweerbaarder te maken."**

Samenwerking

Z-CERT besteedt in 2022 meer aandacht aan de controletaak van zorginstellingen op leveranciers. Samen met de zorgsector ontwikkelt Z-CERT kennisproducten en ontplooit daarnaast andere initiatieven om de gehele keten van zorginstellingen en leveranciers cyberweerbaarder te maken.

column

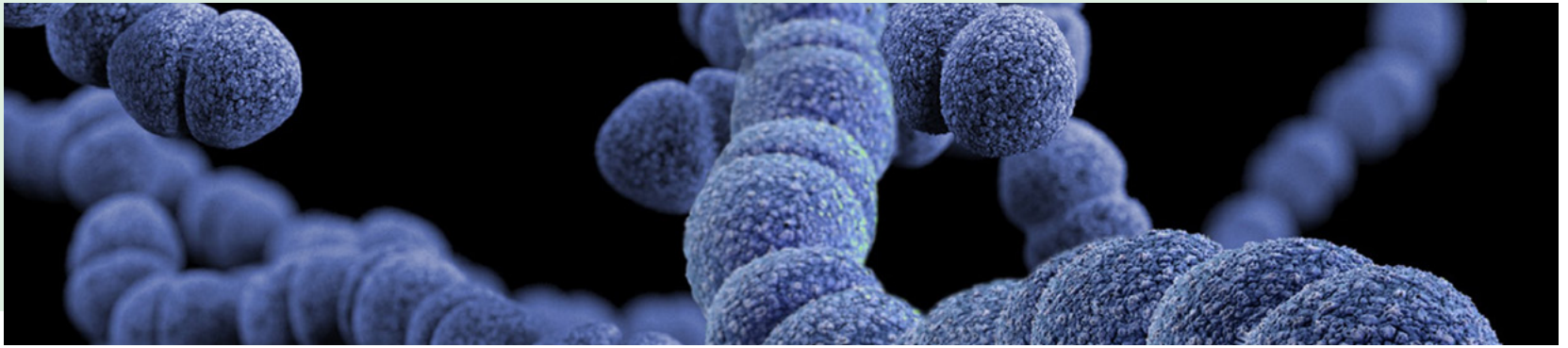
‘Wij blijven verantwoordelijk voor de veiligheid van de gegevens van onze cliënten.’

Daan Brinkhuis, CISO bij ‘s Heeren Loo

Bent u nog lekker relaxed als u dit dreigingsbeeld leest? Zodra ik nadenk over de impact van een geslaagde aanval met gijzelsoftware, voel ik als CISO de zweetdruppeltjes op mijn voorhoofd verschijnen. Terwijl we in de zorg bij ’s Heeren Loo proberen om stress en agressie bij onze cliënten te meten, te voorspellen en te verminderen, voel ik fysiek de relatie tussen het lezen over cyberdreigingen en stress.

Verantwoordelijkheid en vertrouwen

We hebben bij ’s Heeren Loo met een ‘SaaS-tenzij’-strategie veel applicaties naar de cloud gemigreerd. Onder andere ons Elektronisch Cliënten Dossier, onze human resource-applicatie en de financiële software. We zijn hier gepast trots op; in de wolken zelfs. Tegelijkertijd merken we dat het ook in de cloud kan regenen, donderen en bliksemen. Want wij blijven verantwoordelijk voor de veiligheid van de gegevens van onze cliënten. Wij ervaren de overlast als onze IT de processen niet kan ondersteunen. Natuurlijk hebben we vertrouwen dat onze SaaS-leveranciers, met meer securityspecialisten dan wij, onze omgevingen goed beveiligen. Toch merk ik dus die zweetdruppeltjes als ik over cyberdreigingen nadenk. Met een SaaS-dienst besteed je blijkbaar niet alle zorgen uit.



Mijn onrustige gevoel vermindert als ik verder nadenk. We hebben immers goede contracten afgesloten! Een goed SaaS-contract vereist meer afspraken dan een traditionele overeenkomst waarbij u de software zelf beheert. Juist op het gebied van beveiliging. Eigenlijk hebben we dat best netjes voor elkaar. Toch ben ik niet helemaal gerust …

Leveranciersbeoordeling

Onze NEN7510-certificering helpt om de onrust verder te bedwingen. "Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen", aldus de NEN7510. Natuurlijk is dat extra belangrijk bij SaaS-leveranciers. We beoordelen de certificering en ISAE-verklaring van leveranciers, inclusief de scope. We gaan na of partijen wat betreft beveiliging hun afspraken nakomen en of ze proactief informeren over kwetsbaarheden. We evalueren beveiligingsincidenten. Mijn hartslag zakt wat verder, maar nog niet genoeg om echt te kunnen ontspannen.

Samen verbeteren

We voeren periodiek gesprekken met onze belangrijkste SaaS-leveranciers. Die gaan vooral over de traditionele onderwerpen op het gebied van Service Level Agreement. Heeft de helpdesk snel genoeg geantwoord? Was de beschikbaarheid volgens afspraak? Opeens is daar het eureka-moment: dit soort gesprekken moeten we uitbreiden! Niet uit wantrouwen, maar om elkaar scherp te houden en samen te verbeteren. We kunnen leveranciers vragen hoe de back-ups bestand zijn tegen versleuteling door gijzelsoftware. Calamiteitenplannen moeten we op elkaar afstemmen.

De meeste adviezen en whitepapers van Z-CERT zijn goede gespreksonderwerpen. Daarmee draagt Z-CERT dus bij aan stressreductie in de zorg. We hebben vertrouwen in onze leveranciers, goede contracten en redelijke leveranciersbeoordelingen. We gaan de contacten met onze SaaS-leveranciers uitbreiden en beter benutten. Juist op technisch vlak. De tijd zal leren of het voldoende is. Garanties zijn er helaas niet. En mijn hartslag? Die kan nog steeds flink hoog zijn. Tijdens het sporten natuurlijk, maar ook uit enthousiasme om verder te verbeteren. Veel gezonder dan stress!

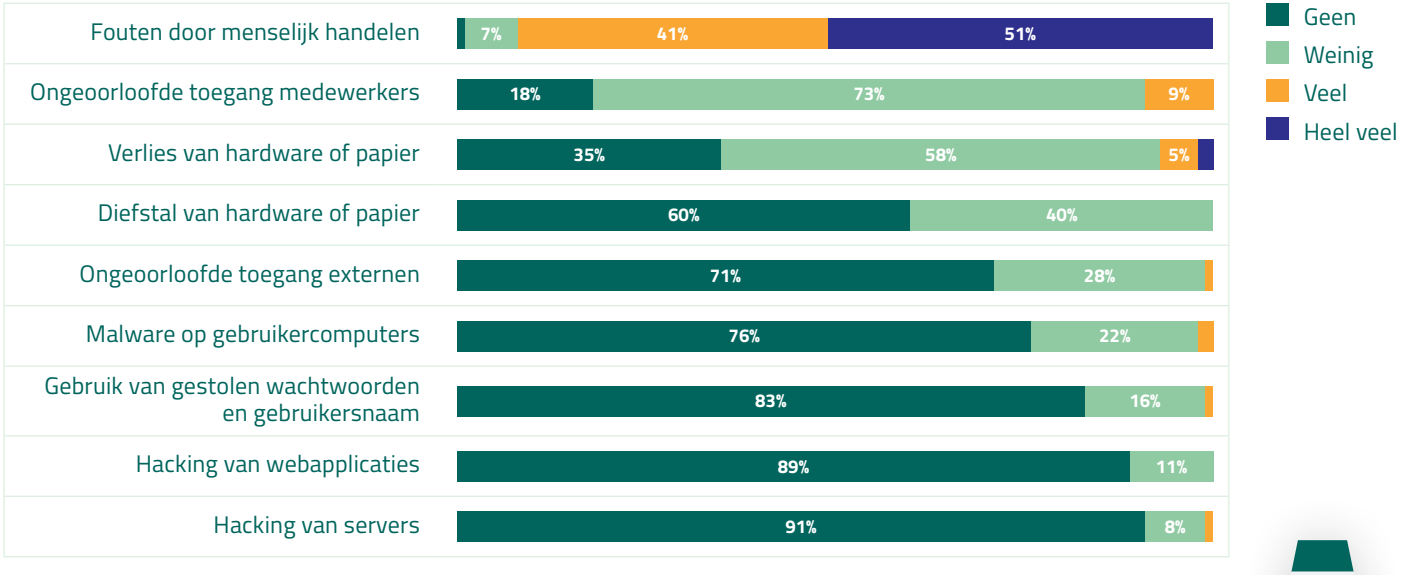
dreiging

Datalekken

Securityverantwoordelijken van zorginstellingen zien na ransomware, datalekken als de grootste zorg. Datalekken kunnen verschillende oorzaken hebben. Om de dreiging in kaart te brengen vroeg Z-CERT zorginstellingen in welke categorieën zij datalekken hadden in 2021. Op basis daarvan is onderstaande top 9 van datalekken gemaakt.

Figuur 1, top 9 datalekken in de zorg

In totaal gaven 92 zorginstellingen aan in welke categorieën ze datalekken hadden.
De organisaties maakten een ruwe schatting van de hoeveelheid datalekken.



18

Wat opvalt is dat de top 3 volledig bestaat uit het type datalekken dat wordt veroorzaakt door medewerkers. De laatste zes worden vaak veroorzaakt door externe spelers.

De meeste datalekken worden dus veroorzaakt door medewerkers (1,2,3). Van de ondervraagde zorginstellingen heeft 98,9 procent in 2021 te maken gehad met datalekken door fouten in menselijk handelen. Daarbij geeft 92 procent aan dat dit veel tot zeer veel voorkomt. Het gaat hier met name om fouten in adressering. Er worden per ongeluk twee brieven in een envelop gestopt of een mail wordt naar het verkeerde e-mailadres verstuurd. De impact is daarmee vaak beperkt.

Datalekken door diefstal of verlies

Verlies en diefstal van data blijken zeer reële risico's. Van de zorginstellingen geeft 40 procent aan te maken te hebben gehad met diefstal van apparaten of papier, 65 procent had te maken met verlies van papier of hardware.

Encryptie op apparaten en externe media (zoals usb-sticks) en het op afstand kunnen lokaliseren en verwijderen van data van de apparaten, blijken geen overbodige luxe. Het risico op lekken van gevoelige gegevens wordt groter als medewerkers hun eigen apparaat gebruiken en daarmee mogen inloggen op diensten zonder dat de apparaten in beheer zijn.

Hardware datalek

Bij Z-CERT zijn enkele datalekken gemeld waarbij hardware een rol speelde. Denk bij hardware aan harde schijven, maar ook aan printers, netwerkapparatuur of medische apparatuur. Ook apparaten waar je geen gevoelige informatie op verwacht, kunnen dat toch bevatten. Bijvoorbeeld accountinformatie. In een printer kan nog papier zitten en op een toner kan nog een fysieke afdruk van een document staan.

Volg het juiste vernietigingsproces

Z-CERT adviseert om voor elk afgeschreven elektronisch apparaat dat weer de markt op gaat, de data te verwijderen en de juiste vernietigingsprocessen en -procedures te volgen. Daarbij is het belangrijk dat dit centraal wordt geregeld en de uitstroom van datadragers aantoonbaar via deze processen verloopt. Een actuele CMDB is hiervoor onontbeerlijk. Een goed naslagwerk om zo'n proces vorm te geven is bijvoorbeeld de NIST-800-88 [34]. Sommige zorgorganisaties besteden de vernietiging van elektronische apparatuur uit aan gespecialiseerde bedrijven. Daarbij hoeven zij enkel nog de rapportages van deze bedrijven te controleren en steekproefsgewijs de kwaliteit van de vernietiging te toetsen.

Awareness net zo belangrijk

Veel zorginstellingen hebben protocollen voor het vernietigen van papier. Toch blijkt papier een risico. Een datalek kan namelijk makkelijk tot stand komen als personeel geprinte of geschreven lijstjes gebruikt die vervolgens blijven liggen of worden vergeten. Andere voorbeelden zijn archiefkasten met gevoelige data [35] die per abuis niet worden vernietigd of prullenbakken met papier dat niet is versnipperd. Datalekken voorkomen zit daarom niet altijd in geavanceerde technische oplossingen, maar ook in awareness, fysieke beveiliging en de praktische uitvoering van vernietigingsprocedures. Sommige zorginstellingen houden onderling verrassingsbezoeken om elkaar hierop te toetsen. Goedkoop, doeltreffend en het houdt elkaar scherp.

Ongeoorloofde toegang

Ongeoorloofde toegang tot data door medewerkers blijkt een uitdaging, want 82 procent van de ondervraagde zorginstellingen maakte een melding van een datalek in deze categorie. Dit lijkt veel, maar de hoeveelheid datalekken van deze vorm was beduidend lager dan die van fouten door menselijk handelen.

Zorginstellingen zijn steeds beter in staat om deze vorm van datalekken te detecteren. Zo monitoren zij bijvoorbeeld EPD's en ECD's op ongebruikelijke activiteiten. Als in een korte tijd zeer veel data van verschillende patiënten/cliënten wordt geraadpleegd, gaan de alarmbellen af. Als een zorgverlener informatie opvraagt van een patiënt/cliënt op een hele andere afdeling dan waar hij werkt vanwege een spoedgeval, kan dit alleen via een noodprocedure. De leidinggevende controleert achteraf of de aanvraag legitiem was. Door dit soort monitoringstechnologieën wordt de controle op ongeoorloofde toegang steeds strakker en gebruikersvriendelijker. Vanuit de sector zelf wordt hier ook op gestuurd. De zorgkoepels Nederlandse Federatie van Universitair Medische Centra (NFU) en Nederlandse Vereniging van Ziekenhuizen (NVZ) hebben bijvoorbeeld een gedragslijn opgesteld met best practices rond de toegangsbeveiliging van digitale patiëntdossiers [36].

Uitlekken van inloggegevens

Bij sommige datalekken speelden 'vergeten' inloggegevens in publieke clouddiensten als GitHub een rol. GitHub is een samenwerkingsplatform waar ontwikkelaars code van software plaatsen. Deze code bevat soms nog inloggegevens. Hackers konden op deze manier toegang krijgen tot patiëntdata [37] .

Het Radboudumc heeft in dit dreigingsbeeld een column geschreven over een incident met uitgelekte inloggegevens. In dit geval was het een ex-medewerker die inloggegevens op internet plaatste. Dit leidde tot een incident waarbij hackers cryptomunten konden minen.

Daarnaast is er bij Z-CERT ook een casus binnengekomen waarbij patiëntdata rechtstreeks op een publieke cloudservice te vinden waren. Het Luxemburgse nationale CERT heeft gratis software beschikbaar die helpt dit soort datalekken in publieke bronnen, in een vroeg stadium op te sporen [38].

Datalekken door externe actoren

De laatste vier categorieën datalekken worden vooral veroorzaakt door externe spelers die in het digitale domein opereren. Alhoewel deze datalekken minder vaak voorkomen, kan de impact veel groter zijn. Een bekend voorbeeld is de hack bij een Finse GGZ-instelling. De aanvaller maakte grote hoeveelheden cliëntendata buit. Hij gebruikte die niet alleen om de instelling af te persen, maar benaderde ook rechtstreeks de cliënten met een geldeis.

Malware en gestolen wachtwoorden

Malware-infecties vormen een klein deel van het aantal datalekken. Malware stelt de aanvaller in staat om van alles te downloaden van een met malware besmette computer. Daarnaast zijn deze kwaadaardige programma's gespecialiseerd in het stelen van wachtwoorden. Deze wachtwoorden kunnen worden gebruikt om elders in te loggen; nummer 7 op de lijst. Ook kan de aanvaller meeliften op de inloggegevens van de gebruiker, waardoor multifactorauthenticatie in sommige gevallen kan worden omzeild [39].

Hacking van webapplicaties

Hacking van webapplicaties wordt door 11 procent van de ondervraagde zorginstellingen gemeld. Alhoewel dit weinig is vergeleken met andere datalekken, staat deze categorie bij Z-CERT wel hoog op de agenda. Webapplicaties zijn namelijk in opmars in de zorg.

Webapplicaties zijn soms ook verborgen aanwezig. Mobiele apps maken bijvoorbeeld op de achtergrond gebruik van een webapplicatie. Deze heeft niet de vorm van een website, maar een zogenaamde API, Application Program Interface. Dat is een mechanisme om met andere applicaties op het internet te communiceren. Dus ook als u een mobiele app afneemt, is het belangrijk om de webapplicatie daarachter te beoordelen op security.

> **"Het is belangrijk dat een leverancier richtlijnen gebruikt voor de veilige ontwikkeling van software."**

Advies

Wij raden aan om softwareleveranciers van webapplicaties te selecteren die een gedegen Security Development Lifecycle (SDL) hebben. Een bekend model waarnaar kan worden verwezen, is het model dat Microsoft hiervoor heeft ontwikkeld [40]. Daarnaast is het belangrijk dat een leverancier richtlijnen gebruikt voor de veilige ontwikkeling van software, zoals de richtlijn die het Nationaal Cyber Security Centrum (NCSC) heeft ontwikkeld voor het veilig ontwikkelen van webapplicaties [41].

dreiging

DDoS

Zorgorganisaties maakten in 2021 bij Z-CERT zes keer melding van een gerichte DDoS-aanval. Daarbij was één zorgorganisatie zelfs twee keer slachtoffer. De aanval werd opgevangen door een Wasstraat te activeren. Dit is een manier om DDoS-aanvallen af te slaan.

Indirect hadden zorginstellingen meer last van DDoS-aanvallen. Zorginstellingen zijn in grote mate afhankelijk van Internet Service Providers (ISP's). Dit zijn leveranciers die internetconnectiviteit mogelijk maken en ook vaak andere internetdiensten leveren. Daarnaast gebruiken zorginstellingen leveranciers voor digitale diensten die ook afhankelijk zijn van ISP's. Juist deze ISP's hadden het in 2021 lastig wat betreft DDoS-aanvallen. In de eerste drie kwartalen van 2021 kregen zij 2.130 aanvallen te verduren. In 2020 waren dat er 'slechts' 1.610 over het hele jaar [42]. Daarnaast zijn de aanvallen complexer, krachtiger en nam de duur van een aanval toe [42]. De actoren achter deze aanvallen zijn er vaak op uit om serviceproviders af te persen. Ze stoppen met een aanval, alleen na betaling van een afperssom.

Zesentwintig van de ondervraagde zorginstellingen had in 2021 overlast van DDoS-aanvallen op de ISP's. Zeven daarvan meldden overlast door DDoS-aanvallen op meerdere leveranciers. De gevolgen van deze aanvallen waren heel divers.

Kader 1:

Slachtoffer	Impact
IT-leverancier	▪ Lag een week lang onder vuur. Daardoor waren de servers van de zorginstelling op verschillende momenten verminderd beschikbaar. ▪ Applicaties gehost in de cloud waren niet beschikbaar.
DNS-leverancier (Domain Name System)	▪ De afstandswerkplek op basis van Citrix was slecht bereikbaar. ▪ Websites niet goed bereikbaar.
SaaS-leverancier	Het human resource-systeem was een ochtend niet bereikbaar.
Hostingleverancier website	Website twee tot vier uur verminderd bereikbaar, waarvan vijftien minuten echt niet bereikbaar.
Patiëntenportaal	Patiëntenportaal niet bereikbaar.
Elektronisch Cliënten Portaal	Twee keer een aantal uur niet bereikbaar.
Internetprovider	Internet niet beschikbaar.

Uitval van een patiëntenportaal of een afstandswerkoplossing als Citrix is voor een ziekenhuis erg vervelend. Zeker wanneer artsen bijvoorbeeld op afstand een diagnose moeten stellen.

In het licht van de toenemende aanvallen in de cloud, wordt de groeiende DDoS-dreiging op ISP's wel steeds relevanter voor de zorgsector. Deze dreiging wordt een steeds belangrijker aspect van leveranciersmanagement. Daarnaast identificeert Z-CERT nog een dreiging: gemakkelijk te verkrijgen DDoS-aanvallen. Op het internet en het dark web zijn duizenden websites waar DDoS-aanvallen te koop zijn [43]. De drempel is laag en de impact kan groot zijn. Bovendien is er geen technische kennis voor nodig.

Z-CERT ziet een risico in makkelijk te verkrijgen cyberaanvallen in combinatie met hacktivisme (inzetten van de computerkennis en het internet als daad van protest) tegen de coronamaatregelen. Zo was het in juli door een DDoS-aanval op GGD-websites tijdelijk niet mogelijk om online een prikafspraak te maken of testuitslagen in te zien [44]. Het is op het moment van schrijven niet duidelijk wie er achter de aanval zat, maar het vermoeden is dat de DDoS uit de hacktivistische hoek kwam. Financieel motief leek uitgesloten omdat de criminelen geen losgeld eisten.

Advies

Z-CERT adviseert om uw eigen organisatie te beoordelen op de weerbaarheid tegen deze vorm van cyberdreiging. Daarbij is het belangrijk om zowel organisatorische als technische maatregelen in kaart te brengen en een responseplan op te stellen. Ook het bepalen van afhankelijkheden van leveranciers en het maken van afspraken met hen in een SLA zijn van belang. De afspraken moeten doorwerken naar de subleveranciers, omdat juist deze vaak worden getroffen. Zeker als er kleine, nieuwe leveranciers met gespecialiseerde digitale dienstverlening op de markt komen, is het belangrijk dat deze partijen zich bewust zijn van de dreigingen die spelen.

Voor meer informatie verwijzen we u naar de volgende documenten:

- **Continuïteit van onlinediensten [45]**
- **Technische maatregelen voor de continuïteit van onlinediensten [46]**
- **DDoS Overview and Response Guide [47]**

Tien gouden tips tegen ransomware

De 10 belangrijkste maatregelen om ransomware incidenten te voorkomen of de impact te beperken.

1

Implementeer Applicatiewhitelisting

Definieer software en code die u veilig acht voor uw organisatie. Blokkeer de rest. Denk aan uitvoerbare bestanden, scripts, dll's, installers, packages en ook powershell.exe.

2

Stop of reguleer Office macro's

Z-CERT raadt aan om macro's afkomstig van het internet niet toe te staan. Faseer het gebruik van macro's uit. Als dit (nog) niet kan reguleer het gebruik van macro's dan.

3

Patch applicaties en gebruik de laatste versies

Geef in het patchmanagementproces prioriteit aan de kwetsbaarheden die voor zowel de kans en impact ingeschaald zijn als high.

4

Beveilig afstandswerkoplossingen

Zorg ervoor dat afstandswerkoplossingen zoals Remote Desktop Protocol, Teamviewer en VNC niet ontsloten zijn aan het internet. Deze mogen alleen benaderbaar zijn via een beveiligde VPN of gateway-oplossing.

24

5 Scan de buitenkant van uw IT-infrastructuur

Scan regelmatig uw aan het internet ontsloten systemen op afwijkingen en kwetsbaarheden. Zoals RDP die onbedoeld openstaat, of systemen die onbedoeld toegankelijk zijn via het internet.

6 Beveilig uw applicaties

Bijvoorbeeld: check of u de beveiligingsopties in webbrowers optimaal benut. Er komen regelmatig functionaliteiten bij. Schakel niet gebruikte functionaliteiten met security risico's uit, zoals OLE in Microsoft Office.

7 Pas least privilege principes toe

Maak gebruik van een "tiered administration model". Gebruik JIT en JEA principes, geef geen localadmin rechten aan gebruikers en taken met hoge rechten alleen uitvoeren vanaf "Privileged Access Workstations".

8 Maak regelmatig back-ups van belangrijke data

Test het herstelproces regelmatig. Pas de 3-2-1 regel toe en zorg ook voor offline back-ups. Systemen waarop de back-ups worden bewaard moeten niet toegankelijk zijn met accounts die gebruikt worden voor andere systemen.

9 Patch de Operating Systems van uw apparaten

Draai alleen versies van het operating system die ondersteund worden. Denk daarbij ook aan medische- en netwerkapparaten. Hiervoor geldt hetzelfde advies als bij punt 3. Zet systemen die niet geüpdatet kunnen worden in een netwerk-segment achter een interne firewall.

10 Implementeer multifactor authenticatie

Voor toegang tot online diensten en voor alle externe toegangsoplossingen tot uw IT-infra-structuur. Ook voor accounts en computers die toegang geven tot gevoelige data.

25

Tip: *Goed om deze tips uit te printen en op te hangen op kantoor!*

column

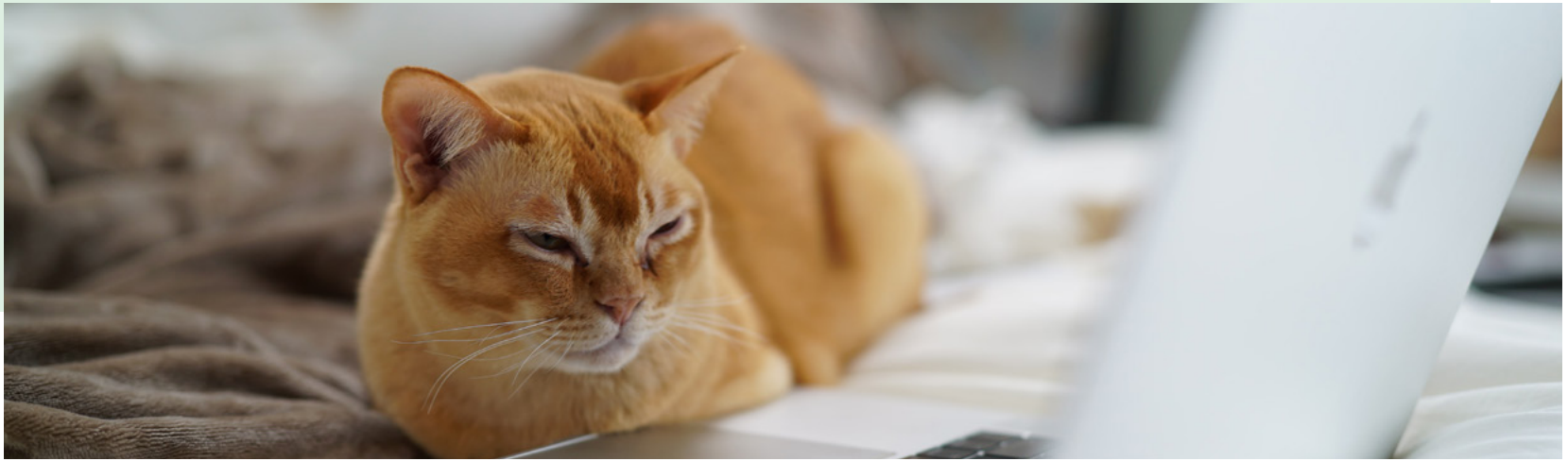
Mark Janssen, CFO Radboudumc

De heldere zomerse dag in juli kon niet donkerder eindigen: “Mark, we zijn erachter gekomen dat we zijn gehackt en we zijn kwetsbaar. We zijn al met een speciaal team van Microsoft gestart om te onderzoeken wat er speelt.” Dit was het bericht van onze security officer. Er schiet van alles door mij heen. Hoe kan dat? Wat voor hack? Hoe kwetsbaar? Kunnen we nog zorg verlenen? Ligt er wat op straat? Kunnen we bij onze onderzoeksdata?

Dat we wel kunnen blijven werken, maar nog niet weten hoe kwetsbaar we zijn, is een onzekerheid die ik de eerste uren moeilijk een plek kan geven. Alle acties zijn erop gericht om de eventuele veiligheidslekken te dichten en gegevens en systemen veilig te stellen. Tegelijkertijd start de analyse van wat er is gebeurd en wat er nog aan activiteit vanuit de hacker gaande is. Het crisisbeleidsteam is gestart en een eerste melding voor een datalek is gedaan.

Gaten dichten en dijkverzwaring aanleggen, zo noemen we het. Later, nadat we meer inzicht krijgen, noemen we het gaten dichten en dijken verhogen. Naast Microsoft hebben we de support van andere partijen ingeroepen. Alles wordt 24/7 in de gaten gehouden. Er wordt volop aan de dijken gewerkt. Onze mensen werken de klok rond. Wat een verantwoordelijkheid nemen zij!

‘Je loopt al snel een stap achter op cyber-criminelen.’



Naast de IT- en cybertechnische deskundigen hebben we snel contact gezocht met Z-CERT. Ons team ervaart direct professionele steun. Met name in het in contact brengen en onderhouden van communicatie met andere partijen, waaronder nationale veiligheid en justitie, en ondersteuning in de communicatie.

> **“We hebben onze veiligheidsplannen naar voren gehaald en geïntensiveerd.”**

Na een door een moedwillig geplaatste dataset op een platform, door een van onze (inmiddels ex) medewerkers, heeft een buitenlandse hacker kunnen gebruikmaken van onze accounts bij een datacenter en zo crypto-munten kunnen minen op onze kosten.

Geluk bij een ongeluk, daar is het bij gebleven en de systemen van het Radboudumc zijn niet gecompromitteerd in de periode dat de gaten nog niet waren gedicht. In een paar dagen tijd zijn wij met de neus op de feiten gedrukt. We hebben onze veiligheidsplannen naar voren gehaald en geïnten-siveerd. Nu kijk ik naar de situatie in de zomer als een groot leermoment. Je loopt al snel een stap achter op cybercriminelen. We hebben snel en met vereende krachten geacteerd. Een awareness-niveau dat we nu volhouden.

dreiging

Fraude

Phishing was ook in 2021 een groot probleem voor zorginstellingen. Zij krijgen regelmatig phishingmails binnen die niet altijd door spamfilters werden tegengehouden. Een derde van de ondervraagde zorginstellingen had te maken met succesvolle pogingen waarbij gebruikersnamen en wachtwoorden werden gestolen. Alles bij elkaar opgeteld zijn hierbij zeventig sets inloggegevens buitgemaakt. Dit leidde niet altijd tot datalekken. Eén zorginstelling meldde bijvoorbeeld tien phishingincidenten over 2021, maar niet 1 daarvan leidde tot datalekken, dankzij de vereiste multifactorauthenticatie.

Credential Phishing

Het niet hebben van multifactorauthenticatie is een risico. Niet alleen voor een zorginstelling zelf, maar vooral ook voor de contactpersonen die in het adresboek staan en vervolgens worden aangevallen. Het ontbreken van een multifactorauthenticatie heeft in 2021 geleid tot verschillende vormen van misbruik. Enkele voorbeelden uit de praktijk:

- Vertrouwde mail en bestanden komen in handen van kwaadwillenden. Zij scannen de mail op wachtwoorden wat kan leiden tot nieuwe incidenten.
- Gestolen mails worden gerecycled door cybercriminelen. Een cybercrimineel beantwoordt de gestolen mail en stuurt kwaadaardige software mee. Omdat de inhoud bekend en vertrouwd is bij de ontvanger, is de contactpersoon van het slachtoffer makkelijker te besmetten.
- Kwaadwillenden misbruiken mailboxen om spam te versturen.
- Ongeoorloofde toegang tot een mailbox kan zelfs financiële risico's met zich meebrengen. Cybercriminelen gaan ver in hun pogingen tot financiële fraude. In 1 geval had een crimineel zich via phishing toegang verschaft tot een medewerkersaccount van de partner van een zorgorganisatie. De crimineel monitorde de mailbox en onderschepte mailtjes van contactpersonen waar een financiële relatie mee was. Door mails te versturen vanuit de mailbox poogde de crimineel het rekeningnummer van een zorginstelling aan te passen.

Malafide informatieverzoeken

Naast financiële fraude en credential phishing heeft de zorg ook te maken met frauduleuze informatieverzoeken. Deze kunnen leiden tot datalekken. Enkele voorbeelden uit de praktijk:

- Het opvragen van loonstrookjes van medewerkers door een fraudeur.
- Een fraudeur registreert een domeinnaam dat erg lijkt op een bij veel zorginstellingen vertrouwde partner. De fraudeur mailt met dit domein een zorginstelling en vraagt onder het mom van 'een controle' patiëntdata op. Deze fraudepoging mislukte.

Financiële fraude

De pogingen tot financiële fraude die bij Z-CERT worden gemeld zijn vaak fraudepogingen die worden ondernomen via de mail. De aanvallen zijn doelgerichter dan bij credential phishing en het per mail verspreiden van malware. Cybercriminelen zoeken gericht naar slachtoffers op LinkedIn, bijvoorbeeld medewerkers van de financiële afdeling.
De aanvallers spreken vaak goed Nederlands en nemen de tijd voor een aanval. Deze e-mails bevatten vaak geen kwaadaardige links of malware. Ook worden ze veelal verstuurd vanuit gerespecteerde mailproviders. Daardoor is de kans redelijk groot dat de fraudepoging door de spamfilters heen komt. Een organisatie is dan aangewezen op de security-awareness van medewerkers en de beveiligingsmaatregelen rondom betalingen.

CEO-fraude

Een voorbeeld van financiële fraude die bij Z-CERT vaak binnenkomt, is CEO-fraude. Bij CEO-fraude stuurt een cybercrimineel een werknemer van een zorginstelling een mail waarbij hij zich voordoet als de directeur van die zorginstelling. De crimineel oefent druk uit op de medewerker om even wat geld voor te schieten om bijvoorbeeld cadeaubonnen te betalen. Vaak probeert de crimineel een mailwisseling of WhatsApp-gesprek op te zetten. Ook zet hij het slachtoffer aan tot actie door middel van psychologische trucjes en geestelijke druk. Zowel uit de geestelijke gezondheidszorg als ziekenhuizen ontving Z-CERT hiervan voorbeelden.

De meeste pogingen tot CEO-fraude zijn in 2021 onderschept, maar in één geval was het toch raak. Een medewerker met betalingsbevoegdheid bij een zorginstelling werd verleid om meer dan 1.500 euro over te maken aan een cybercrimineel. Dit kon gebeuren doordat financiële controles bij deze afdeling nog niet op hetzelfde niveau waren als bij de financiële afdeling. Inmiddels is de controleprocedure bij de instelling aangepast.

> **“Overal waar binnen de organisatie wordt betaald, moet extra worden opgelet.”**

Advies
De geleerde lessen uit deze casus zijn dat overal waar binnen de organisatie wordt betaald, extra moet worden opgelet. De frauderesistente procedures moeten worden gevolgd, zoals deze ook bij de financiële afdeling bestaan.

Voorbeeld uit de praktijk:
Eén telefoontje voorkomt grote fraude
Bij een zorgaanbieder, aangesloten bij Z-CERT, komen vanaf een bepaald moment facturen van een grote leverancier binnen. Dit gebeurt vanaf een ander e-mailadres, met op de factuur een ander bankrekeningnummer dan gebruikelijk. De facturen zijn volledig juist: ze gaan over daadwerkelijk geleverde diensten, bevatten de afgesproken prijzen, in de bijlagen zitten exact kloppende prestatieverklaringen. De lay-out van de facturen is precies hetzelfde als anders. Wat zou u doen? De facturen betalen? Niet betalen? De administratief medewerker handelde gelukkig volgens de afgesproken procedure van de zorgaanbieder: bij nieuwe contactgegevens of bankgegevens bellen met het oude telefoonnummer of e-mailen met het oude e-mailadres. Op deze manier is door één telefoontje de betaling van meerdere facturen met grote bedragen naar een kwaadwillende voorkomen.

Wat is er precies gebeurd?
Een kwaadwillende registreert twee domeinnamen. De ene lijkt op het kloppende maildomein van de zorgaanbieder, de andere op die van de leverancier. In dit voorbeeld kon de kwaadwillende daardoor mailen vanuit administratie@finance-zorgaanbieder.nl, waar in het normale mailadres het stuk 'finance-' niet bestaat. Vanuit dit adres is vervolgens naar de leverancier een nepmail gestuurd met de vraag het e-mailadres voor verzending van facturen voor de zorgaanbieder aan te passen. De leverancier heeft dit gedaan, waarna de kwaadwillende de facturen gemaild kreeg in plaats van de zorgaanbieder. Na aanpassing stuurde de kwaadwillende vanuit het nepadres dat op dat van de leverancier lijkt, de facturen door naar het normale e-mailadres van de zorgaanbieder.

Handelingsperspectief
Hanteer een werkwijze om veranderende contactgegevens of betalingsgegevens van leveranciers na te bellen. Gebruik daarbij de al eerder bekende contactgegevens. Als u te maken krijgt met een poging tot e-mailfraude: informeer dan Z-CERT, meld het bij de Fraudehelpdesk, probeer het domein uit de lucht te halen en overweeg aangifte te doen bij de politie.

dreiging

Cyberspionage door statelijke actoren

De Nederlandse zorgsector is interessant voor statelijke actoren. Er vindt in Nederland veel innovatief onderzoek plaats, bijvoorbeeld op het gebied van COVID-19[48], waar statelijke actoren interesse in hebben. Waardevol onderzoek wordt niet alleen gedaan door ziekenhuizen en laboratoria, maar ook in de GGZ en andere takken van de zorgsector [49]. Z-CERT is zich bewust van tenminste dertien cybergroepen die worden betaald door staten die de afgelopen jaren interesse hebben getoond in Nederland en in de zorg. Hier gaat een potentiële dreiging van uit.

Incidenten door statelijke actoren

In reactie op de enquête van Z-CERT laten 94 ondervraagde instellingen weten geen cyberspionage door statelijke actoren te hebben waargenomen. Er zijn in 2021 wel enkele incidenten geweest die te relateren zijn aan statelijke actoren.

Nobelium

In december 2020 werd door FireEye bekendgemaakt dat Orion (een veelgebruikte monitoringssoftwaretool) software had aangepast door een dreigingsactor [50]. Hierdoor ontvingen 18.000 organisaties een malafide update waardoor de actoren toegang kregen tot de interne infrastructuur van de organisaties. Veel van deze organisaties waren bijvangst voor de hackers, die uit al de geïnfecteerde slachtoffers honderd relevante organisaties selecteerden [15]. De dreigingsactor, ook wel Nobelium genoemd, heeft het vooral gemunt op overheden, NGO's (niet-gouvernementele organisaties), IT-services en professional services.

Een beperkt aantal Nederlandse zorginstellingen raakte geïnfecteerd als gevolg van de inmiddels beroemde 'state sponsored' hack. Grootschalige spionage of datadiefstal kon niet worden aangetoond, meestal bleef het slechts bij een besmetting. Op zich niet heel verwonderlijk, omdat de hackers uit de 18.000 slachtoffers, honderd organisaties selecteerden waarmee ze actief aan de slag gingen [15]. Hun prioriteit lag (gelukkig) minder bij de zorg.

Microsoft Exchange

In maart 2021 maakte Microsoft bekend dat de statelijke actor Hafnium een aantal kwetsbaarheden in hun on-premise mailoplossing (Exchange) actief misbruikte [51]. Hafnium was in januari al actief [52], maar de updates kwamen in maart pas beschikbaar. Deze actor heeft ook onderzoekers van infectieziekten als doelwit [15]. Z-CERT heeft in het ZorgDetectieNetwerk interactie gezien van deze actor met de infrastructuur van zorginstellingen. Maar ook in deze casus werd net als bij de Solarwinds-casus geen spionage vastgesteld.

32

Analyse

Cyberspionage en datadiefstal zijn lastig vast te stellen. Bij Z-CERT zijn er geen meldingen over gedaan in 2021. Dat betekent niet dat cyberspionage niet voorkomt in de zorgsector. Ook is het mogelijk dat spionage of datadiefstal pas later plaatsvindt. Een bekende tactiek van statelijke actoren is namelijk dat ze wetenschappelijke instellingen binnendringen zonder daar direct iets mee te doen. Op het moment dat er interessante ontwikkelingen zijn worden ze wakker en gaan ze over op het inwinnen van inlichtingen [53].

Kwetsbaar

De besproken casussen leggen een kwetsbaarheid bloot. De grote hoeveelheden organisaties die in korte tijd worden geïnfecteerd door statelijke actoren via de supply chain of door misbruik van zero-day kwetsbaarheden, is verontrustend. Het zegt iets over de offensieve programma's die overheden hebben waarbij er veel geld wordt geïnvesteerd en veel mankracht wordt ingezet. Microsoft geeft aan dat de Solarwinds-hack de grootste en meest geavanceerde operatie is die ze hebben gezien. Ze schatten dat er minstens 1.000 mensen aan hebben meegewerkt. Het is alleen niet altijd vuurwerk, ook worden op grote schaal standaardmethoden gebruikt zoals die ook bij het hoofdstuk ransomware aan bod komen [15].

Verwachting

Onze verwachting is, gezien de budgetten en geboekte successen dat dit soort supply chain en zero day-aanvallen door zullen zetten in het komend jaar. Het is een trend die al een tijdje gaande is, maar de operaties zijn niet altijd zo opvallend als de hack bij Solarwinds. Z-CERT raadt de Nederlandse zorgsector aan de kroonjuwelen wat betreft onderzoek en innovatie te identificeren en passende verdedigingsmechanismen en monitoring in te richten.

Advies

De AIVD en MIVD hebben recent een rapport uitgebracht dat u op weg kan helpen om adequate (technische) maatregelen te treffen. In het rapport wordt de lezer meegenomen in een offensieve mindset van de hacker en wordt in elke fase aangegeven wat u kunt doen [53]. Als uw organisatie interessant onderzoek doet voor staten is het goed om een 'threat hunting'-proces te hebben waarbij wordt gezocht op latente aanwezigheid van deze actoren. Een bekend model hiervoor is de TaHiTI Threat Hunting Methodology van de Nederlandse betaalvereniging [54].

thema

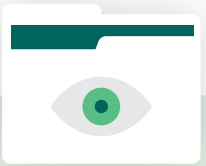
Log4j

Op het moment van schrijven van het dreigingsbeeld was de kwetsbaarheid in Log4j net bekend. De kwetsbaarheid heeft de dreiging op ransomware, datalekken, cyberspionage en andere type incidenten in de zorg verhoogd. Log4j is een software-component die in de meeste applicaties wordt gebruikt, die zijn geprogrammeerd in Java. Dit component is zeer wijdverspreid aanwezig in allerlei (gerenommeerde) softwareproducten [55], zo ook in applicaties die toegankelijk zijn via het internet en die toegang geven tot patiëntendata. Er zijn voor aanvallers dus veel nieuwe mogelijkheden ontstaan om binnen te dringen.

Vanaf 1 december werd beperkt misbruik van de kwetsbaarheid geconstateerd. Het bestaan van de kwetsbaarheid is vrijdag 10 december bekendgemaakt en toen zijn ook updates beschikbaar gesteld. In de tussentijd zijn dus veel organisaties die kwetsbaar waren, vatbaar geweest voor misbruik zonder dat het bekend was.
Na 10 december steeg het misbruik van deze zero-day aanzienlijk. Voor organisaties duurde het soms even voordat ze konden overzien wat kwetsbaar was en wat ze moesten doen om zich te beschermen. Dit betekent dat er veel gelegenheid was voor hackers om in te breken. Er zijn internationaal beperkt praktijkvoorbeelden bekend van ernstig misbruik, maar de verwachting is dat er nog naweeën zullen komen [56] [57].

Advies
Organisaties doen er goed aan om te controleren op sporen van compromittatie vanaf 1 december. Daarnaast is er een heel concreet stappenplan beschikbaar hoe je als organisatie op deze kwetsbaarheid zou kunnen reageren [58]. Voor de laatste informatie verwijzen we naar een website die het NCSC heeft gelanceerd met nuttige informatie over alles rond Log4j. Veel organisaties (waaronder Z-CERT) dragen bij aan deze website [55].

> **“Er zijn voor aanvallers veel nieuwe mogelijkheden ontstaan om binnen te dringen.”**



“ De kwetsbaarheid in Log4j heeft de dreiging op ransomware, datalekken, cyberspionage en andere type incidenten in de zorg verhoogd. ”

Samenvatting

Ransomware

De grootste digitale dreiging in de zorgsector is ransomware. Het afgelopen jaar steeg de hoeveelheid ransomware-incidenten in de zorgsector in Nederland en Europa aanzienlijk.

17 procent van de onze ondervraagde deelnemers melden ransomware-incidenten bij leveranciers. Ransomware-incidenten bij leveranciers hebben vaak impact op meerdere zorginstellingen. De incidenten leidden tot datalekken, vertragingen in leveringen, stagnatie van onderhoud, maar ook ernstige verstoringen van operationele processen.

De methodes die ransomware-groepen gebruiken om binnen te komen, zijn in veel gevallen voorspelbaar. Z-CERT stelt voor te beoordelen of uw organisatie voldoende weerbaar is tegen 3 veelgebruikte methoden om binnen te komen en veelgebruikte methoden om een netwerk te infiltreren. Z-CERT adviseert bij leveranciersmanagment aandacht te besteden aan deze dreiging en de weerbaarheid van de leverancier tegen ransomware-aanvallen in te schatten.

Datalekken

Z-CERT schat het optreden van “datalekken” in als de tweede grootste digitale dreiging in de zorgsector. De dreiging is anders van aard dan bij ransomware, omdat bij datalekken operationele processen in mindere mate verstoord worden. Wel is de dreiging hoog omdat dit type incident veelvoorkomend is. Z-CERT heeft middels een enquête een top 9 van oorzaken van datalekken vastgesteld.

- De meeste datalekken binnen de 93 ondervraagde zorginstellingen vallen in de categorie “fouten door menselijk handelen”. Wel viel de impact bij veel incidenten mee.
- Nummer 2 op de lijst is “ongeoorloofde toegang medewerkers”, de hoeveelheid datalekken in deze categorie per instelling is veel minder dan in de categorie “fouten door menselijk handelen”. Er zijn op dit vlak positieve ontwikkelingen. Bijvoorbeeld de publicatie van de gedragslijn “toegangsbeveiliging van digitale patiëntdossiers” opgesteld door zorgkoepels NVZ en NFU [36]. Ook zijn er steeds meer gebruiksvriendelijke oplossingen om dit soort datalekken vast te stellen.
- De laatste 5 oorzaken van datalekken worden veelal veroorzaakt door externe actoren. Het gaat bijvoorbeeld om datalekken veroorzaakt door het stelen of raden van wachtwoorden of het verleiden van gebruikers om kwaadaardige software (malware) op te starten. Bij dit type datalekken kan de impact groot zijn, omdat vaak toegang verkregen wordt tot grote hoeveelheid data.

DDoS

Zorginstellingen worden niet vaak zelf direct aangevallen met een DDoS-aanval, instellingen meldden 6 incidenten. Echter de Internet Service Providers die zorginstellingen en de leveranciers van zorginstellingen gebruiken worden veel vaker aangevallen. Zij kampten in Q1 t/m Q3 2021 met 2130 aanvallen, veel meer dan vorig jaar.
Dit leidde bij 29 procent van de ondervraagde deelnemers tot verstoringen. Zo konden voor een aantal uur zorgverleners niet inloggen op hun Citrix thuiswerkoplossing, waren cloudapplicaties niet bereikbaar en kon een zorginstelling een bepaalde tijd niet inloggen op servers. In veel gevallen duurde de verstoringen een paar uur lang, maar in 1 geval ook een week. DDoS-aanvallen zijn een belangrijk agendapunt voor het management van leveranciers van digitale diensten.

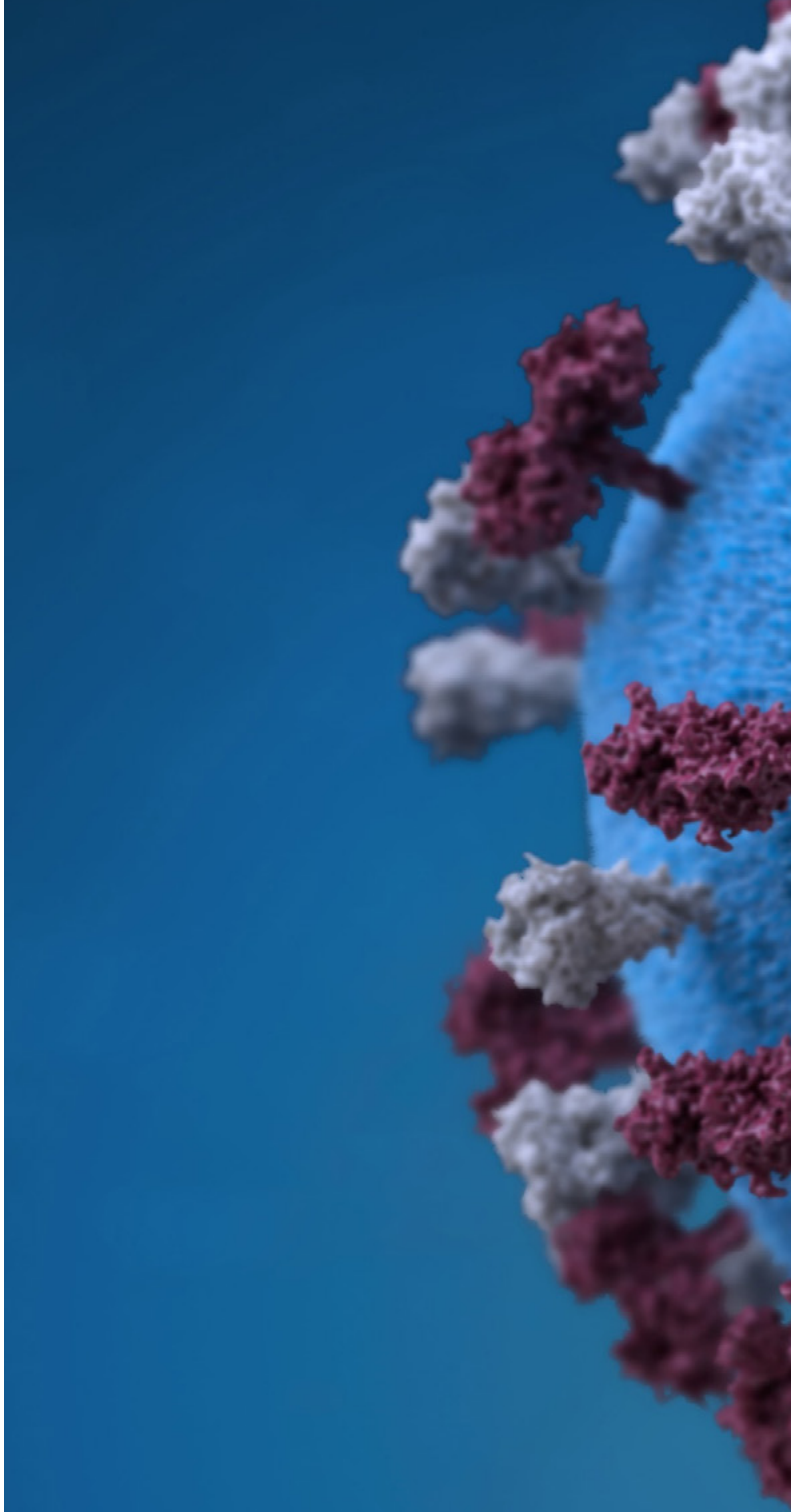
Fraude

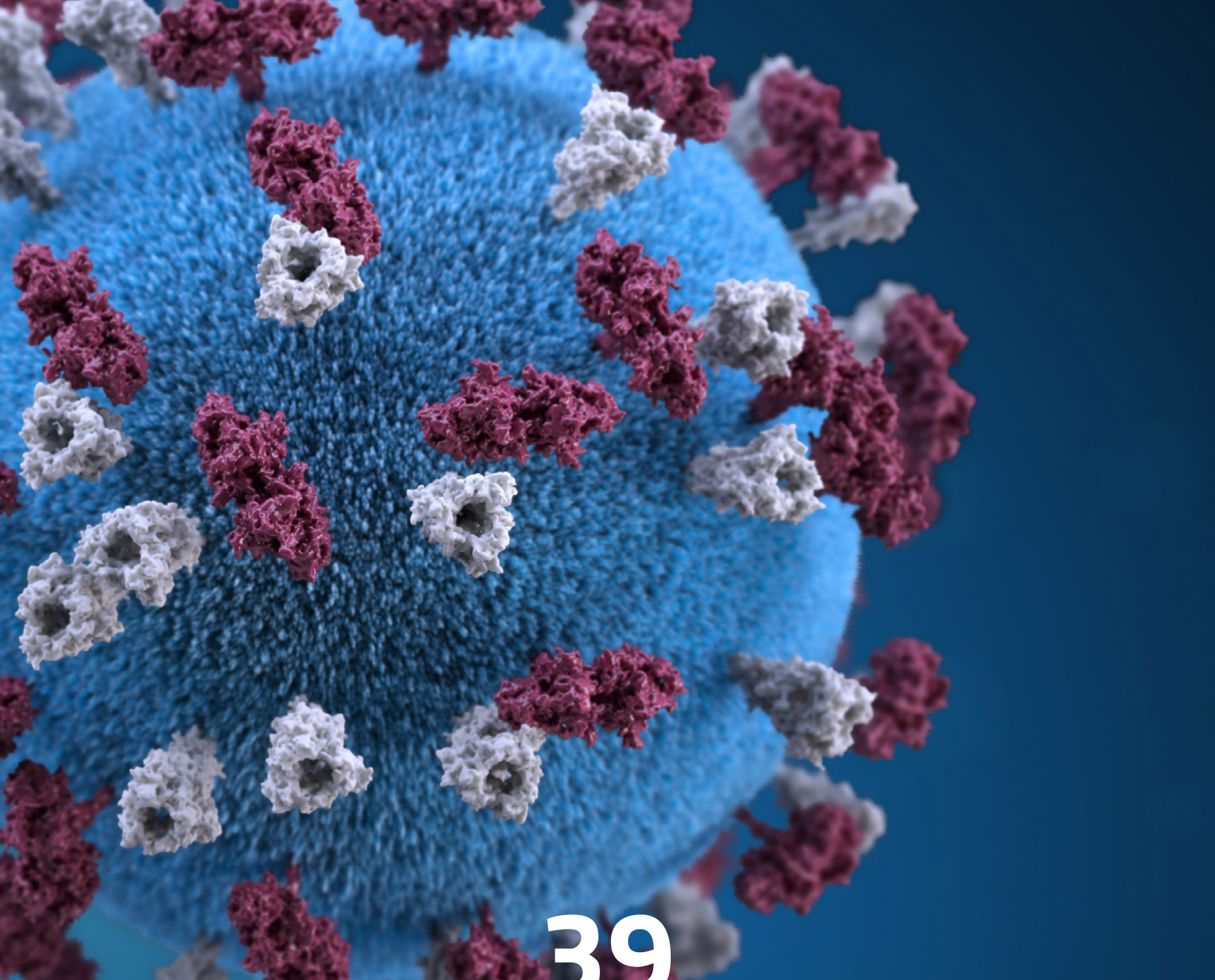
Het stelen van wachtwoorden door middel van credential phishing is een grote dreiging voor de zorgsector. Bij een derde van de bevraagde deelnemers werden er door de aanvallers succesvol wachtwoorden gestolen. Dit leidde tot verschillende type misbruik en in 1 geval werd gepoogd een gecompromitteerde mailbox te misbruiken voor financiële fraude. Opvallend was dat organisaties die multifactorauthenticatie gebruikten, veel datalekken konden voorkomen.

Er werden veel pogingen tot financiële fraude per mail bij Z-CERT gemeld. Vaak probeert een aanvaller uit naam van de directeur een werknemer onder druk te zetten om een betaling voor te schieten (CEO-fraude). Indien mensen bereid zijn uit eigen zak te betalen of niet de frauderesistente procedures gevolgd worden voor betalingen, hebben deze aanvallers af en toe succes. Omdat het hier om communicatie gaat zonder kwaadaardige software of malafide formulieren, worden deze pogingen minder vaak onderschept en is security awareness training op dit onderwerp zeer belangrijk.
Andere vormen van fraude waren pogingen tot het veranderen van rekeningen, valse facturen en malafide informatieaanvragen.

Cyberspionage door statelijke actoren

Ondervraagde organisaties maakten geen melding van cyberspionage van statelijke actoren. Echter er waren wel incidenten die terug te voeren zijn op statelijke actoren. Nederlandse zorginstellingen ondervonden overlast van hacks op SolarWinds en Exchange, wat voor zover we weten niet leidde tot cyberspionage of datadiefstal. Echter het is goed te beseffen dat het doel van een statelijke actor in veel gevallen alleen is om toegang te verkrijgen tot het netwerk van een organisatie. Op het moment dat er binnen de gecompromitteerde organisatie relevante ontwikkelingen zijn voor deze actoren, kan men over gaan tot spionage.





Bibliografie

[1] **Golem.de**, *„Mehrere Kliniken nach Hackerangriff vom Netz genommen,"* [Online]. Available: https://www.golem.de/news/malware-mehrere-kliniken-nach-hackerangriff-vom-netz-genommen-2109-159795.html. [Geopend September 2021].

[2] **Pallas Kliniken**, *„Pallas Kliniken wieder im Normalbetrieb nach Cyber-Attacke,"* 23 Augustus 2021. [Online]. Available: https://www.pallas-kliniken.ch/fileadmin/user_upload/12_medienmitteilungen/20210823_MM_Pallas_Kliniken_Cyberattacke.pdf.

[3] **Lemonde Informatique**, *„La fondation santé des étudiants de France victime d'un ransomware,"* 21 April 2021. [Online]. Available: https://www.lemondeinformatique.fr/actualites/lire-la-fondation-sante-des-etudiants-de-france-victime-d-un-ransomware-82694.html.

[4] **Z-CERT**, *„Cybersecurity Dreigingsbeeld Zorg 2020,"* Februari 2020. [Online]. Available: https://www.z-cert.nl/wp-content/uploads/2021/02/Z-CERT_RapportDreigingsbeeld2020.pdf.

[5] **Govinfosecurity**, *„Information Security Media Group (ISMG),"* 29 September 2021. [Online]. Available: https://www.govinfosecurity.com/mental-health-clinic-notifies-patients-6-months-after-hack-a-17642.

[6] **Coveware**, *„Ransomware attackers down shift to 'Mid-Game' hunting in Q3 2021,"* 21 Oktober 2021. [Online]. Available: https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts.

[7] **Sophos**, *„The State of Ransomware 2021,"* 2021. [Online]. Available: https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf.

[8] **Fireye**, *„M-trends 2021,"* 2021. [Online]. Available: https://content.fireeye.com/m-trends/rpt-m-trends-2021.

[9] **Sophos**, *„The State of Ransomware in Healthcare 2021,"* 2021. [Online]. Available: https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-healthcare-2021-wp.pdf.

[10] **Crowdstrike**, *„2021 Global Threat Rapport,"* 2021. [Online]. Available: https://www.crowdstrike.com/resources/reports/global-threat-report/.

[11] **S. Gatlan**, *„Researchers compile list of vulnerabilities abused by ransomware gangs,"* 18 September 2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/researchers-compile-list-of-vulnerabilities-abused-by-ransomware-gangs/.

[12] **The Record**, *„Ransomware gangs are abusing a zero-day in EntroLink VPN appliances,"* 25 Oktober 2021. [Online]. Available: https://therecord.media/ransomware-gangs-are-abusing-a-zero-day-in-entrolink-vpn-appliances/.

[13] **Madniant**, *„UNC2447 SOMBRAT and FIVEHANDS Ransomware: A Sophisticated Financial Threat,"* 29 April 2021. [Online]. Available: https://www.mandiant.com/resources/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.

[14] **Huntress**, *„Threat Advisory: Hackers Are Exploiting a Vulnerability in Popular Billing Software to Deploy Ransomware,"* 22 Oktober 2021. [Online]. Available: https://www.huntress.com/blog/threat-advisory-hackers-are-exploiting-a-vulnerability-in-popular-billing-software-to-deploy-ransomware.

[15] **Microsoft**, *„Microsoft Digital Defense Rapport,"* Oktober 2021. [Online]. Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi.

[16] **Europol**, *„Ransomware gang arrested in Ukraine with Europol's support,"* 4 Oktober 2021. [Online]. Available: https://www.europol.europa.eu/newsroom/news/ransomware-gang-arrested-in-ukraine-europol%E2%80%99s-support.

[17] **Department of Justice**, *„NetWalker Defendant Charged, Dark Web Resource Disabled, Nearly $500,000 Seized,"* 27 Januari 2021. [Online]. Available: https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware.

[18] **Europol**, *„12 targeted for involvement in ransomware attacks against critical infrastructure,"* 29 Oktober 2021. [Online]. Available: https://www.europol.europa.eu/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure.

[19] **L. Sterk**, *„Goed nieuws voor de zorgsector: Goodbye Emotet,"* 28 Januari 2021. [Online]. Available: https://www.z-cert.nl/nieuws/goed-nieuws-voor-de-zorgsector-goodbye-emotet/.

[20] **Reuters**, *„EXCLUSIVE Governments turn tables on ransomware gang REvil by pushing it offline,"* 21 Oktober 2021. [Online]. Available: https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/.

[21] **BleepingComputer**, *„DarkSide ransomware gang returns as new BlackMatter operation,"* 31 Juli 2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/darkside-ransomware-gang-returns-as-new-blackmatter-operation/.

[22] **TheHill**, *„World leaders recognize ransomware attacks as 'global security threat,'"* 14 Oktober 2021. [Online]. Available: https://thehill.com/policy/cybersecurity/576763-world-leaders-recognize-ransomware-attacks-as-global-security-threat.

[23] **Microsoft**, 20 july 2021. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2021/07/20/the-growing-threat-of-ransomware/.

[24] **Trend Micro**, *„LockBit Resurfaces With Version 2.0 Ransomware Detections in Chile, Italy, Taiwan, UK,"* 16 Augustus 2021. [Online]. Available: https://www.trendmicro.com/en_us/research/21/h/lockbit-resurfaces-with-version-2-0-ransomware-detections-in-chi.html.

[25] **ANSSI**, *„RYUK RANSOMWARE,"* 25 Februari 2021. [Online]. Available: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf.

[26] **Z-CERT**, *„Tien gouden tips tegen Ransomware,"* 2021. [Online]. Available: https://www.z-cert.nl/wp-content/uploads/2021/02/Z-CERT_FactsheetRansomware_2560x1920px_04-1.pdf.

[27] **NCSC**, *„Factsheet Ransomware,"* 2020. [Online]. Available: https://www.ncsc.nl/documenten/factsheets/2020/juni/30/factsheet-ransomware.

[28] **Z-CERT**, *„Bescherm uw zorgorganisatie tegen Ransomware,"* 2019. [Online]. Available: https://www.z-cert.nl/wp-content/uploads/2021/02/Bescherm-uw-organisatie-tegen-ransomware.pdf.

[29] **SANS**, *„The Pyramid of Pain,"* [Online]. Available: https://www.sans.org/tools/the-pyramid-of-pain/. [Geopend 2021].

[30] **Microsoft**, *„Windows Credential Theft Mitigation Guide Abstract,"* 2016. [Online]. Available: https://download.microsoft.com/download/C/1/4/C14579CA-E564-4743-8B51-61C0882662AC/Windows%2010%20credential%20theft%20mitigation%20guide.docx.

[31] **Madiant**, *„Ransomware Protection and Containment Strategies,"* [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/wp-ransomware-protection-and-containment-strategies.pdf.

[32] **Palantir**, *„Restricting SMB-based lateral movement in a Windows environment,"* [Online]. Available: https://blog.palantir.com/restricting-smb-based-lateral-movement-in-a-windows-environment-ed033b888721. [Geopend 2020].

[33] **Unit 42**, *„Observing Attacks Against Hundreds of Exposed Services in Public Clouds,"* 22 November 2021. [Online]. Available: https://unit42.paloaltonetworks.com/exposed-services-public-clouds/.

[34] **NIST**, *„Guidelines for Media Sanitization,"* 2014. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

[35] **De Noordoostpolder**, *„Datalek bij Zorggroep Oude en Nieuwe Land,"* 14 September 2021. [Online]. Available: https://denoordoostpolder.nl/artikel/1177826/datalek-bij-zorggroep-oude-en-nieuwe-land.html.

[36] **NVZ en NFU**, *„Toegangsbeveiliging digitale patiëntdossiers,"* 12 Oktober 2020. [Online]. Available: https://nvz-ziekenhuizen.nl/toegangsbeveiliging-digitale-patientdossiers.

[37] **ECCOUNCIL**, *„Repository Blunder! GitHub Data Leak Incidents Impact Over 200,000 U.S. Patient,"* 18 Augustus 2020. [Online]. Available: https://cisomag.eccouncil.org/9-leaky-github-repositories/.

[38] **CIRCL**, *„AIL framework - Framework for Analysis of Information Leaks,"* 2021. [Online]. Available: https://github.com/ail-project/ail-framework.

[39] **D.-J. Mollema**, *„Abusing Azure AD SSO with the Primary Refresh Token,"* 21 Juli 2021. [Online]. Available: https://dirkjanm.io/abusing-azure-ad-sso-with-the-primary-refresh-token/.

[40] **Microsoft**, *„What are the Microsoft SDL practices?,"* 2021. [Online]. Available: https://www.microsoft.com/en-us/securityengineering/sdl/practices.

[41] **NCSC**, *„ICT-beveiligingsrichtlijnen voor webapplicaties,"* 01 September 2015. [Online]. Available: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties.

[42] **NBIP**, *„Quarterly update about DDoS attacks,"* 2021. [Online]. Available: https://www.nbip.nl/en/news/quarterly-update-about-ddos-attacks-q3-2021/.

[43] **NBIP**, *„DDoS data report 2020,"* 2021. [Online]. Available: https://www.nbip.nl/wp-content/uploads/2021/05/NBIP-DDoS-data-report-2020.pdf.

[44] **GGD GHOR**, *„GGD GHOR Nederland ondervindt ernstige hinder door DDoS-aanvallen,"* 21 Juli 2021. [Online]. Available: https://ggdghor.nl/actueel-bericht/ddos/.

[45] **NCSC**, *„Factsheet Continuïteit van online diensten,"* [Online]. Available: https://www.ncsc.nl/onderwerpen/ddos/documenten/factsheets/2019/juni/01/factsheet-continuiteit-van-onlinediensten.

[46] **NCSC**, *„Factsheet Technische maatregelen voor continuïteit voor online diensten,"* Juni 2019. [Online]. Available: https://www.ncsc.nl/onderwerpen/ddos/documenten/factsheets/2019/juni/01/factsheet-technische-maatregelen-voor-continuiteit-van-online-diensten.

[47] **CERT-EU**, *„DDoS Overview and Response Guide,"* 2017. [Online]. Available: https://cert.europa.eu/static/WhitePapers/CERT-EU_Security_Whitepaper_DDoS_17-003.pdf.

[48] **COVID-19 Programma**, *„COVID-19 Programma,"* November 2021. [Online]. Available: https://www.zonmw.nl/nl/over-zonmw/coronavirus/programmas/programma-detail/covid-19-programma/projecten/.

[49] **GGZ Centraal**, *„Wetenschappelijk onderzoek,"* [Online]. Available: https://www.ggzcentraal.nl/werken-leren/wetenschappelijk-onderzoek/.

[50] **FireEye**, *„Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor,"* 13 december 2021. [Online]. Available: https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.

[51] **Microsoft**, *„A moment of reckoning: the need for a strong and global cybersecurity response,"* 17 December 2020. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/.

[52] **Volexity**, 2 Maart 2021. [Online]. Available: https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/.

[53] **AIVD en MIVB**, *„Publicatie AIVD/MIVD: Cyberaanvallen door statelijke actoren - zeven momenten om een aanval te stoppen,"* 28 Juni 2021. [Online]. Available: https://www.aivd.nl/documenten/publicaties/2021/06/28/cyberaanvallen-door-statelijke-actoren---zeven-momenten-om-een-aanval-te-stoppen.

[54] **Nederlanse betaalvereniging**, *„TaHiTI Threat Hunting Methodology,"* 2022. [Online]. Available: https://www.betaalvereniging.nl/veiligheid/publiek-private-samenwerking/tahiti/.

[55] **NCSC**, *„Overview of software (un)affected by Log4j,"* 2022. [Online]. Available: https://github.com/NCSC-NL/log4shell/tree/main/software.

[56] **Microsoft**, *„Guidance for preventing, detecting, and hunting for exploitation of the Log4j 2 vulnerability,"* 2022. [Online]. Available: https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/.

[57] **NHS**, *„Log4Shell Vulnerabilities in VMware Horizon Targeted to Install Web Shells,"* 5 Januari 2022. [Online]. Available: https://digital.nhs.uk/cyber-alerts/2022/cc-4002.

[58] **NCSC**, *„Log4j,"* 2021. [Online]. Available: https://www.ncsc.nl/onderwerpen/log4j.

[59] **SonicWall**, *„SONICWALLCYBER THREATREPORT,"* Juni 2021. [Online]. Available: https://www.sonicwall.com/resources/white-papers/2021-sonicwall-cyber-threat-report/.

[60] **Hof van Twente**, *„Te go ed van vertrouwen?,"* 8 Maart 2021. [Online]. Available: https://www.hofvantwente.nl/fileadmin/files/hofvantwente/inwoners/actueel/Te-goed-van-vertrouwen.pdf.

[61] **Zeit Online**, 26 Oktober 2021. [Online]. Available: https://www.zeit.de/digital/internet/2021-10/ransomware-group-revil-member-hacker-russia-investigation.

[62] **abcNews**, *„In hour-long call, Biden discusses ransomware with Putin after another massive attack,"* 10 Juli 2021. [Online]. Available: https://abcnews.go.com/Politics/hour-long-call-biden-discusses-ransomware-putin-massive/story?id=78761441.

[63] **Security News Paper**, *„Ziggy ransomware hackers shut down their operations for fear of being imprisoned; retrieve your information without paying the ransom,"* 8 Februari 2021. [Online]. Available: https://www.securitynewspaper.com/2021/02/08/ziggy-ransomware-hackers-shut-down-their-operations-for-fear-of-being-imprisoned-retrieve-your-information-without-paying-the-ransom/.

[64] **C. Tilbury**, *„Windows Credentials - Attack - Mitigation - Defense,"* 2017. [Online]. Available: https://www.first.org/resources/papers/conf2017/Windows-Credentials-Attacks-and-Mitigation-Techniques.pdf.

[65] **RTBF**, *„Attaque informatique au CHwapi: les opérations non urgentes reportées, les consultations maintenues,"* 18 Januari 2021. [Online]. Available: https://www.rtbf.be/info/regions/hainaut/detail_le-chwapi-victime-d-une-attaque-informatique-en-pleine-pandemie?id=10676223.

[66] **Bleepingcomputer**, *„French MNH health insurance company hit by RansomExx ransomware,"* 10 februari 2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/french-mnh-health-insurance-company-hit-by-ransomexx-ransomware/.

[67] **Le progres**, *„Cyberattaque à l'hôpital Nord-Ouest : des opérations reportées,"* 15 Februari 2021. [Online]. Available: https://www.leprogres.fr/sante/2021/02/15/cyberattaque-a-l-hopital-nord-ouest-3-000-postes-informatiques-touches.

[68] **Franceinfo**, *„Cyberattaque : les hôpitaux de Dordogne ont failli connaître le même sort que celui de Dax,"* 11 februari 2021. [Online]. Available: https://france3-regions.francetvinfo.fr/nouvelle-aquitaine/dordogne/perigord/cyberattaque-les-hopitaux-de-dordogne-ont-failli-connaitre-le-meme-sort-que-celui-de-dax-1952401.html.

[69] **CERT-RO**, *„Infectare cu PHOBOS ransomware la Spitalul Clinic Nr.1 CF Witting din București,"* 7 Juli 2021. [Online]. Available: https://cert.ro/citeste/infectare-ransomware-phobos-witting-bucuresti.

[70] **Sudouest**, *„Béarn : l'hôpital d'Oloron Sainte-Marie victime d'une cyberattaque, le parquet de Paris saisi,"* 9 Maart 2021. [Online]. Available: https://www.sudouest.fr/pyrenees-atlantiques/oloron-sainte-marie/bearn-l-hopital-d-oloron-sainte-marie-victime-d-une-cyberattaque-1558161.php.

[71] **NCSC Ireland**, *„Ransomware Attack on Health Sector - UPDATE,"* 16 Mei 2021. [Online]. Available: https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf.

[72] **Cybercrime**: Ransomware legt IT des Klinikums Wolfenbüttel lahm , *„Das Klinikum Wolfenbuettel ist Ziel einer Hacker Attacke Erpressung Patienten Versorgung,"* [Online]. Available: https://www.heise.de/news/Cybercrime-Ransomware-legt-IT-des-Klinikums-Wolfenbuettel-lahm-6140048.html.

[73] **NCSC Ierland**, *„Ransomware Attack on Health Sector,"* 16 Mei 2021. [Online]. Available: https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf.

[74] **Z-CERT**, *„Wereldwijde ransomware aanvallen REvil via supply chain attack Kaseya,"* 2 juli 2021. [Online]. Available: https://www.z-cert.nl/nieuws/wereldwijde-ransomware-aanvallen-revil-via-supply-chain-attack-kaseya/.

[75] **Digital Shadows**, *„Initial Access Brokers Listings Increasing in 2021,"* 13 April 2021. [Online]. Available: https://www.digitalshadows.com/blog-and-research/initial-access-brokers-listings-increasing-in-2021/.

[76] **Enisa**, *„ENISA Threat Landscape 2021,"* 27 Oktober 2021. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

[77] **ThreatPost**, *„Groove Calls for Cyberattacks on US as REvil Payback,"* 21 Oktober 2021. [Online]. Available: https://threatpost.com/groove-ransomware-revil-revenge-us-cyberattacks/175726/.

[78] **NCTV**, *„Cybersecuritybeeld Nederland 2021,"* 28 Juni 2021. [Online]. Available: https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021.

[79] **Cloudflare**, *„What is Anycast? | How does Anycast work?,"* 2021. [Online]. Available: https://www.cloudflare.com/learning/cdn/glossary/anycast-network/.

[80] **QS Quacquarelli Symonds Limited**, *„QS World University Rankings,"* [Online]. Available: https://www.topuniversities.com/university-rankings/university-subject-rankings/2021/medicine.

[81] **RIVM**, *„Onderzoek naar COVID-19 in Nederland,"* [Online]. Available: https://www.rivm.nl/coronavirus-covid-19/onderzoek.

[82] **Deloitte**, *„Digital transformation - shaping the future of European healthcare,"* September 2020. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/life-sciences-health-care/deloitte-uk-shaping-the-future-of-european-healthcare.pdf.

[83] **NCSC**, *„Log4shell vulnerabilities (CVE-2021-44228, CVE-2021-45046, CVE-2021-4104, CVE-2021-45105),"* 2022. [Online]. Available: https://github.com/NCSC-NL/log4shell.

Dankwoord

Dit document is een initiatief van Stichting Z-CERT en is mede tot stand gekomen dankzij de steun van onze deelnemers en het Ministerie van Volksgezondheid Welzijn en Sport.

Onze speciale dank gaat uit naar columnisten **Daan Brinkhuis** en **Mark Janssen** voor hun bijdrage aan dit Cyberdreigingsbeeld.

Dank ook aan alle specialisten van Z-CERT voor hun inhoudelijke bijdrage, advies, geduld en tegenlezen van de tekst.

Veel dank aan de **CISO's** die mee wilden werken aan de interviews en zo de basis vormden voor dit Dreigingsbeeld. Evenals de **94 zorginstellingen** die hun input leverden via een online enquête. Maar ook **leveranciers** waren een onmisbare bron van informatie. Dank allen voor het compleet maken van dit Dreigingsbeeld.

Tot slot, dank aan **Artiënne Buissant des Amorie** van Artgen voor de opmaak van het Cyberdreigingsbeeld voor de Zorg.

Vragen of opmerkingen over dit rapport:
communicatie@z-cert.nl

Stichting Z-CERT
Stationsplein 121
3818 LE Amersfoort
033 737 06 09

info@z-cert.nl
www.z-cert.nl