Cybersecurity Dreigingsbeeld voor de zorg 2023

COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

Colofon

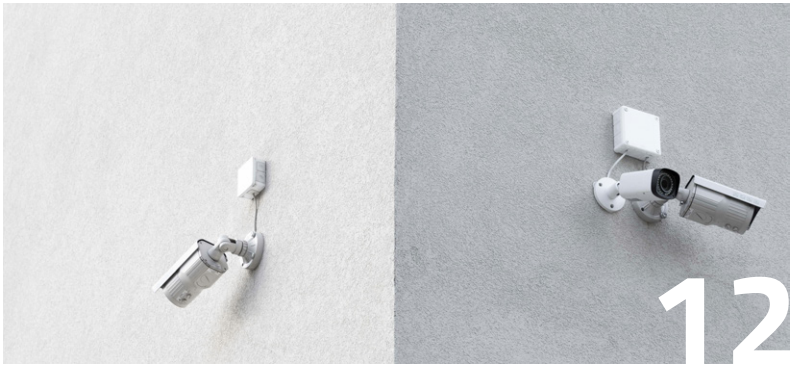
Stichting Z-CERT is hét expertisecentrum op het gebied van cybersecurity in de zorg. Het jaarlijkse Cybersecurity Dreigingsbeeld voor de zorg beschrijft de belangrijkste gevaren voor de Nederlandse zorgsector. We gebruiken hiervoor de informatie uit meldingen van deelnemers, informatie van (inter)nationale partners en kennisinstituten, eigen bevindingen, interviews met deskundigen, literatuuronderzoek, research van open bronnen en een enquête onder Nederlandse zorginstellingen.

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.

We vormen een professioneel netwerk 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 (CERT's). Met elkaar pakken we cyberuitdagingen aan, zoals ransomware, phishing, datalekken en hacken.

De inhoud van dit Cybersecurity Dreigingsbeeld voor de zorg 2023 is met grote zorgvuldigheid samengesteld. Toch kan er onverhoopt een fout of onvolledigheid in zijn geslopen. Z-CERT en eventuele andere betrokken partijen kunnen daarvoor niet aansprakelijk worden gesteld.

Inhoud



‘Het is belangrijk dat zorginstellingen goede afspraken maken met hun leveranciers over informatiebeveiliging’

Voorwoord

Het jaar 2023 wordt door veel mensen gezien als hét jaar van de generatieve AI, zoals het taalmodel ChatGPT en bijvoorbeeld de AI beeldengenerator Dall-E. Deze kunstmatig gestuurde chatbots bieden veel nieuwe mogelijkheden voor informatiebeveiligers, maar ook voor kwaadwillenden.

Het gebruik van AI door cybercriminelen lijkt op dit moment nog niet zo’n enorme impact te hebben. Anders is dat met ransomware en het afpersen van (zorg)organisaties met uitgelekte data. De dreiging van ransomware is in de zorg nog steeds heel groot, evenals de angst voor afpersing met datalekken. Ook lopen leveranciers van zorginstellingen een hoog risico om slachtoffer te worden van incidenten door ransomware en/of afpersen met datalekken.

Uit de gegevens die worden gepubliceerd op datalekwebsites blijkt dat IT-dienstverleners in Europa vaker worden getroffen door ransomware of afpersing met een datalek dan de zorgaanbieders zelf. Dergelijke incidenten bij leveranciers kunnen een flinke impact hebben op zorginstellingen. Het is daarom belangrijk dat zorginstellingen goede afspraken maken met hun leveranciers over informatiebeveiliging. Met de Europese NIS2-wetgeving worden de verplichtingen van leveranciers richting de zorgaanbieders strenger.

Scherp houden

Gelukkig gebruiken al steeds meer organisaties in de zorg (en daar buiten) multifactorauthenticatie (MFA) bij het inloggen op systemen. Dit is een belangrijk middel in strijd tegen cyberaanvallen. Helaas zijn cybercriminelen creatief en vinden ze telkens weer manieren om dergelijke MFA-hordes te omzeilen. Met dit jaarlijkse Dreigingsbeeld voor de zorg en onze andere activiteiten blijven wij als Z-CERT de sector scherp houden door te waarschuwen voor bestaande en nieuwe dreigingen.

Eén van die relatief nieuwe dreigingen, komt uit de hoek van domotica. In het jaarlijkse Cybersecurity Dreigingsbeeld voor de zorg van 2022 hebben we al geconstateerd dat het toegenomen gebruik van domotica in de zorg serieuze beveiligingsrisico's met zich meebrengt. De inzet van zorgdomotica kan direct invloed hebben op de zorgverlening omdat het gaat om apparaten zoals valmelders voor ouderen, rookmelders en camera's. Afgelopen jaar hebben we ook een aantal incidenten met domotica gezien met bijvoorbeeld alarmknoppen die niet meer functioneerden waardoor personeel extra rondes moest lopen.

Een ander punt van aandacht is het verschil in volwassenheid tussen verschillende zorginstellingen. De Inspectie Gezondheidszorg en Jeugd (IGJ) constateerde in november 2023 dat ziekenhuizen een stevige inhaalslag hebben gemaakt op het gebied van informatiebeveiliging. De zorgsector is echter veel breder dan ziekenhuizen. Steeds meer koepelorganisaties sluiten zich aan bij Z-CERT, zoals de Vereniging Gehandicaptenzorg Nederland (VGN) en ouderzorgorganisatie ActiZ. Wij verwachten dat er bij steeds meer Nederlandse zorginstellingen (meer) aandacht en budget wordt besteed aan informatiebeveiliging. Laten we hopen dat die voorspelling in 2024 wordt waargemaakt.

Ik wens u veel leesplezier en een digitaal veilig jaar toe.

Wim Hafkamp
Directeur stichting Z-CERT

Samenvatting

Ransomware en datalekken vormen een serieuze dreiging in de zorg. Dit komt vooral door nieuwe phishingtechnieken die criminelen gebruiken en doordat aanvallers steeds sneller zijn met het misbruiken van kwetsbaarheden.

Ransomware

Het aantal ransomware-incidenten is in de zorg in 2023 wereldwijd fors toegenomen. Deze trend hebben we in Nederland en Europa echter nog niet kunnen herkennen. Door nieuwe phishingtechnieken die criminelen gebruiken en doordat aanvallers steeds sneller zijn met het misbruiken van kwetsbaarheden, verwacht Z-CERT dat de dreiging voor de zorgsector in Nederland zal stijgen.

Niet alleen grote organisaties worden het slachtoffer van ransomware-aanvallen, ook kleine organisaties met 50-200 medewerkers zijn vaak het doelwit. Voor 2024 voorspelt Z-CERT vele ransomware-pogingen en enkele grote incidenten.

Z-CERT ziet dat leveranciers vaker worden getroffen dan zorginstellingen. Leveranciers en de transitie naar de cloud brengen dus nieuwe risico's met zich mee. De groeiende digitale afhankelijkheid rechtvaardigt een grotere focus op leveranciers. In 2023 meldde 9 procent van de respondenten ransomware-incidenten bij leveranciers.

Datalekken en DDoS-aanvallen

Datalekken kunnen ook een grote impact hebben op de zorg. Die datalekken kunnen het gevolg zijn van hackpogingen, pogingen van credential phishing, het ontbreken van multifactorauthenticatie, malware en misconfiguraties en onzorgvuldige omgang met apparatuur.

Bovendien signaleert Z-CERT een grotere dreiging voor DDoS-aanvallen door politiek geïnspireerde hacktivisten. In 2023 werden vijftien Nederlandse ziekenhuizen getroffen door DDoS-aanvallen, voornamelijk vanwege geopolitieke kwesties zoals de oorlog in Oekraïne. Hacktivisten richten zich actief op Nederlandse hostingpartijen, wat gevolgen heeft voor de zorgsector.

Cyberspionage en CEO-fraude

In 2024 blijft cyberspionage door statelijke actoren ook een dreiging voor zorginstellingen die relevant wetenschappelijk onderzoek doen of beschikken over voor statelijke actoren interessante persoonsgegevens. Het afgelopen jaar zijn statelijke actoren erin geslaagd om via de leveranciersketen toegang te krijgen tot organisaties.

Een veel meer voorkomend verschijnsel is digitale financiële fraude, zoals CEO-fraude, malafide facturen en frauduleuze webshopbestellingen. We verwachten dat criminelen in 2024 veel pogingen zullen ondernemen om financiële fraude te plegen.

Ontwikkelingen rond AI

Pogingen om financiële fraude te plegen, kunnen verbeterd worden door de inzet van generatieve AI, vooral bekend door de zogenaamde ‘large language models’ (zoals chatGPT). Het gebruik van AI bij het uitvoeren van cyberaanvallen neemt naar verwachting toe. De inzet van AI kan in de nabije toekomst ook zorgen voor moeilijker te herkennen phishingaanvallen of de inzet van geavanceerde nep-audio en -video.

Op diverse fronten neemt het aantal aanvallen toe, terwijl er ook nieuwe technieken opduiken die uitdagingen met zich meebrengen. Het is essentieel om een goede cyberhygiëne te handhaven en de maatregelen te verbeteren om dreigingen voor te blijven.

07

uitleg

Dreigingsradar

De dreigingsradar geeft de tijd, de impact en de ernst weer van cyberdreigingen in de zorg. De plaats van de diverse bolletjes in de binnenring, middenring of buitenste ring zegt iets over wanneer iets een dreiging zal zijn.

De grafiek is ingedeeld in drie taartpunten die iets zeggen over de weging van de dreiging. In de rechter taartpunt staan de ernstigste dreigingen. Hoe meer de bolletjes naar links staan, hoe lager de dreiging is die ervan uitgaat.

Tot slot geeft de kleur van de bolletjes de verwachte impact van een dreiging aan. Hoe donkerder, hoe groter de verwachte impact.

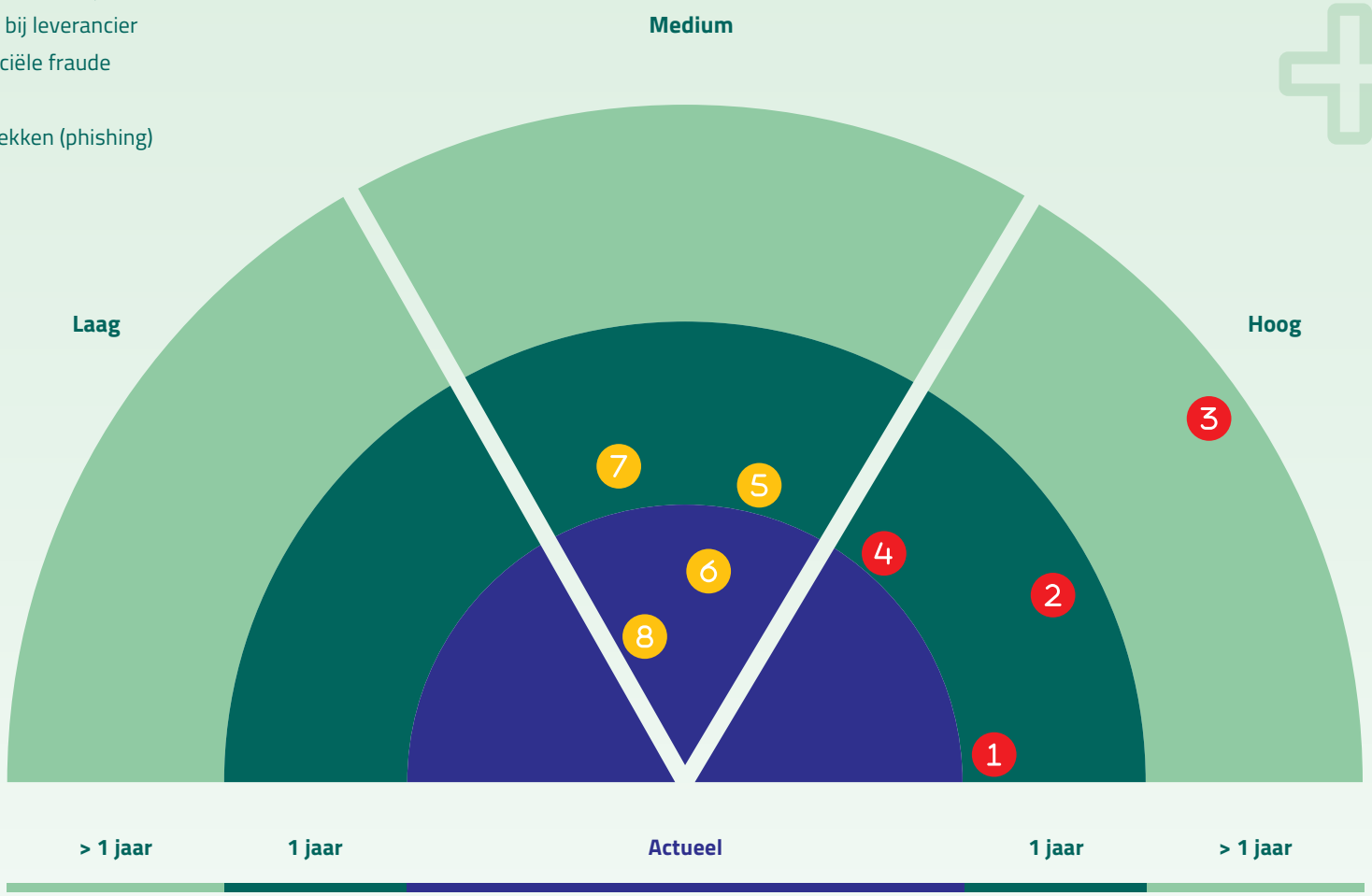
Een uitgebreide uitleg van de dreigingsradar staat in bijlage 1 op bladzijde 36.

‘De dreigingsradar geeft de tijd, de impact en de ernst weer van cyberdreigingen in de zorg.’

Dreigingsradar

Legenda

① Ransomware
② Datalekken (hacking)
③ Spionage
④ Ransomware bij leverancier
⑤ DDoS bij leverancier
⑥ Financiële fraude
⑦ DDoS
⑧ Datalekken (phishing)



uitleg

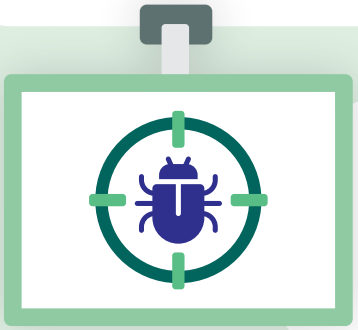
‘Deze informatie kan worden gebruikt om maatregelen te prioriteren’

Incidenten onder respondenten

Voor het dreigingsbeeld heeft Z-CERT bij deelnemers geïnformeerd naar het type security-incidenten dat zij hebben meegemaakt. Bijna een vierde van de deelnemers heeft de survey ingevuld. De resultaten worden naast deze tekst weergegeven in een grafiek. Deze informatie kan worden gebruikt om bewustwording te creëren binnen uw eigen organisatie en om maatregelen te prioriteren. De incidenten zullen verder besproken worden in de hoofdstukken over ‘dreigingen’ en zijn onder andere gebruikt om de dreigingsniveaus vast te stellen.

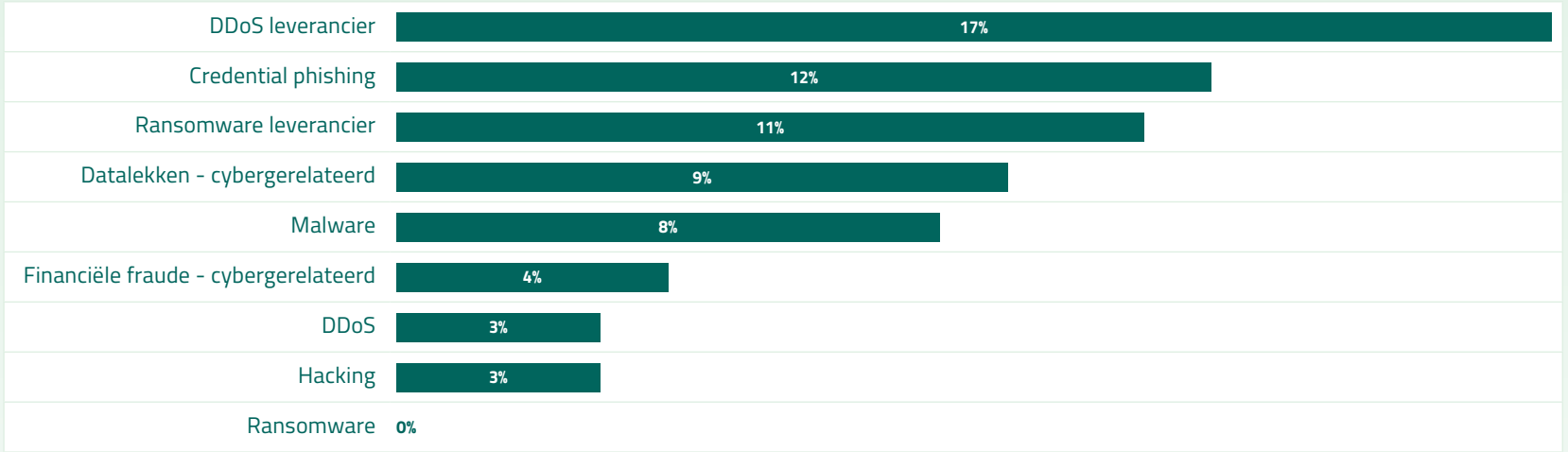
Toelichting

Het percentage geeft weer hoeveel procent van het totaal respondenten 1 of meerdere incidenten hadden in deze categorie. Onder ‘datalekken - cybergerelateerd’ verstaan we datalekken die plaatsvonden door malware, credential phishing of hacking. Bij de financiële fraude categorie in de grafiek gaat het om financiële fraude die gepleegd is door gebruik te maken van digitale media als mail en WhatsApp.



Figuur 1

Security-incidenten die plaatsvonden bij deelnemers van Z-CERT die de vragenlijst hebben ingevuld



dreiging

Ransomware

Inschatting dreiging: hoog

Z-CERT schat het dreigingsniveau door ransomware en/of afpersen met datalekken in als 'hoog'. We schatten de dreiging iets hoger in dan vorig jaar omdat de ransomware-sector effectiever en groter is geworden. Bovendien is de zorgsector kwetsbaarder doordat actoren nieuwe phishingtechnieken toepassen en sneller misbruik maken van kwetsbaarheden.

Voorspelling 2024

In 2024 verwacht Z-CERT veel pogingen door ransomware-actoren om binnen te dringen bij Nederlandse zorginstellingen. Z-CERT verwacht binnen een jaar enkele ransomware-incidenten in de Nederlandse zorgsector met grote impact.

Wereldwijde toename ransomware-incidenten in de zorg

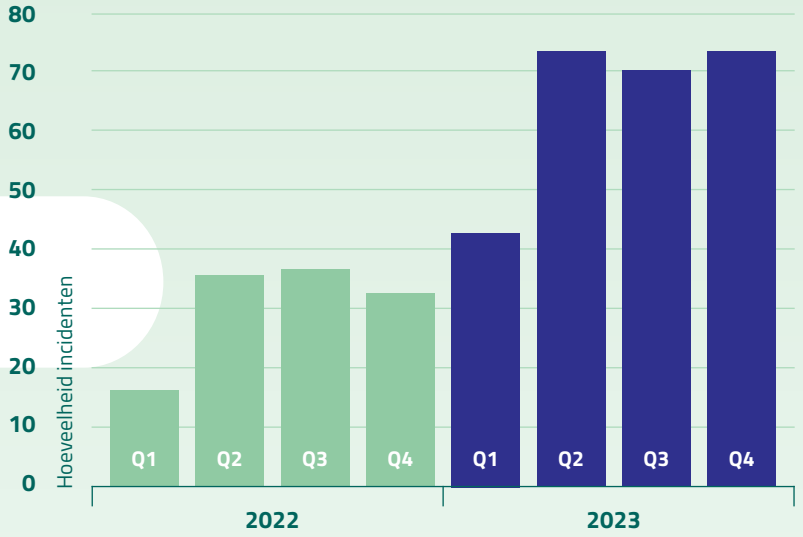
In 2023 registreerde Z-CERT een wereldwijde toename van 73 procent van incidenten die gepubliceerd werden op datalekwebsites ten opzichte van 2022. Figuur 2 laat dezelfde groei van incidenten zien bij zorgaanbieders wereldwijd. Ten opzichte van 2022 was de groei in totaal 115 procent. Deze toename is onder meer te wijten aan het feit dat organisaties veel minder vaak bereid zijn de afperssom te betalen waardoor er meer dan voorheen gegevens op een datalekwebsite terecht komen [1]. Daarnaast spelen ontwikkelingen binnen het ransomware-ecosysteem een rol. Microsoft registreerde bijvoorbeeld 12 procent meer criminele hackers bij ransomware-as-a-service groepen en verwacht daarom een toename van incidenten in 2024 [2]. Daarnaast was er een opkomst van nieuwe, vaak productieve groepen. Een andere factor die bijdroeg was de gevestigde ransomware groep Cl0p die talrijke incidenten veroorzaakte door het exploiteren van zeroday[1] kwetsbaarheden [3]. Ook zijn er groepen die steeds vaker alleen afpersen met het lekken van data zonder dat ransomware wordt ingezet. Dit bespaart tijd, wat hen in staat stelt meer incidenten af te handelen. Dit type hackers heeft er belang bij organisaties uit te kiezen waarvan de data extra gevoelig is, zoals zorginstellingen. Een voorbeeld van zo'n groep is Karakurt [4].

Nederland en Europa

Gemeten over alle sectoren heeft Z-CERT in Europa en Nederland in 2023 meer incidenten op datalekwebsites opgemerkt dan in 2022. Bij zorgaanbieders in Europa registreerde Z-CERT 29 incidenten, iets minder dan vorig jaar, met impact op 101 locaties. Bij Nederlandse zorgaanbieders registreerde Z-CERT in 2023 drie ransomware-incidenten, twee minder dan in 2022.

[1] Een zeroday kwetsbaarheid is een kwetsbaarheid waar nog geen patch voor beschikbaar is.

12



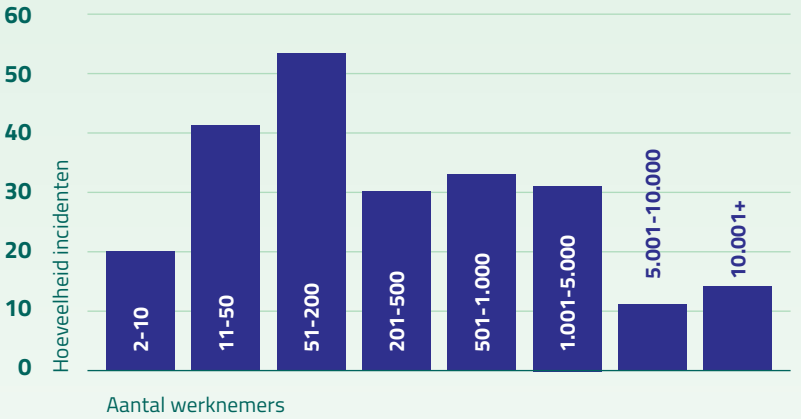
Figuur 2

Incidenten bij zorgaanbieders wereldwijd die op datalekwebsites van cybercriminelen gepubliceerd worden

De daling in Europa en Nederland is niet alleen maar goed nieuws. Zoals eerder genoemd registreerde Z-CERT wereldwijd een toename van het aantal ransomware-incidenten. Die cijfers zijn gebaseerd op grotere datasets dan de dataset met incidenten in Europa en Nederland.

Feit versus fabel: organisatiegrootte relevant?

Binnen Nederlandse zorgorganisaties heerst soms het misverstand dat ransomware-actoren zich voornamelijk richten op grote, vermogende organisaties. In figuur 3 is te zien dat ook organisaties met minder dan 200 medewerkers het afgelopen jaar vaak slachtoffer van een ransomware-aanval zijn geweest. Ook kleine zorgorganisaties, zoals huisartspraktijken werden getroffen.



Figuur 3

Incidenten in 2023 publiek gemaakt op datalekwebsites per zorgaanbieder grootteklasse

Impact

Enkele voorbeelden van de impact van incidenten bij Europese zorg-aanbieders waren:

- Domotica-oplossingen (b.v. alarmknoppen) functioneerden niet naar behoren waardoor personeel extra rondes moet lopen.
- Zorgorganisaties overschakelen op pen en papier voor patiëntregistratie [5].
- Urgente en/of niet urgente afspraken moesten afgezegd worden [6].
- Ambulances moesten uitwijken naar andere ziekenhuizen in de buurt [5].
- Spoedeisende hulp moest worden stopgezet [7].
- Onderzoek laat steeds vaker een verband zien tussen ransomware-aanvallen en een stijging van het sterftecijfer in ziekenhuizen [8].
- Bij 45 procent van de geraakte zorgaanbieders die op datalekwebsites verschenen, zijn de gestolen data uiteindelijk ook gelekt.

Trends in technieken en methoden

Cybercriminelen gebruiken nog steeds dezelfde manieren om binnen te komen als een jaar eerder. Kort gezegd: een cybercrimineel verschaft zichzelf toegang tot een extern systeem middels een account van een medewerker, bijvoorbeeld doordat een makkelijk te raden wachtwoord wordt gebruikt of doordat gestolen wachtwoorden gekocht worden van een andere cybercrimineel. Een gebruiker start malware op die via de mail of via een link is verkregen. Of criminelen misbruiken een kwetsbaarheid in een aan het internet ontsloten systeem.

In vorige dreigingsbeelden hebben we hier uitgebreid bij stilgestaan en de genoemde mitigerende maatregelen zijn nog steeds actueel. Dit jaar willen we inzoomen op een aantal zaken die specifiek dit jaar zijn opgevallen en waar zorginstellingen op kunnen anticiperen:

- De opkomst van phishingaanvallen die MFA omzeilen (zie hoofdstuk datalekken). Dit stelt aanvallers in staat toegang te krijgen tot e-mail-boxen voor het verspreiden van malware of het stelen van data.
- Aanvallers zijn steeds sneller met het misbruiken van een gevonden kwetsbaarheid [9]. Uit een recent onderzoek blijkt dat 1 op de 5 kwetsbaarheden binnen 48 uur na het uitbrengen van een patch misbruikt wordt [10]. Z-CERT stuurde dit jaar 16 spoedeisende beveiligingsadviezen over kwetsbaarheden die vaak actief misbruikt werden. In 2023 nam het totaal aantal bekendgemaakte kwetsbaarheden die vervolgens als kritiek werden ingeschaald, toe met iets meer dan 3 procent [11].
- Grootschalige datadiefstal uit online systemen voor bestandsoverdracht zoals MOVEit Transfer vond dit jaar frequent plaats, doordat criminelen zero-day kwetsbaarheden exploiteerden. Dit resulteerde in tientallen incidenten bij zorginstellingen en hun leveranciers wereldwijd [12].
- We zagen veel aanvallen op VPN-oplossingen. Kwaadwillenden probeerden wachtwoorden te raden of ze proberen oude wachtwoorden die gelekt zijn bij datalekken. Deze aanvallen zijn vaak succesvol omdat voor bijna 50 procent van VPN-accounts geen multifactorauthenticatie gebruikt wordt [2].
- Er wordt op grote schaal malware verspreid (zie hoofdstuk datalekken).

Leerpunten uit 2023
Er is veel informatie beschikbaar over het voorkomen van en omgaan met een ransomware-aanval, zie hiervoor het kopje “handelingsperspectief ransomware”.

Tijdens ransomware-aanvallen of pogingen daartoe werden er door zorg-instellingen in Europa een aantal lessen geleerd die we in dit dreigingsbeeld graag willen meegeven:

- **Domotica en cloud** Zorg voor een alternatieve internetverbinding voor domotica-oplossingen die met de cloud moeten communiceren, zodat deze niet enkel afhankelijk zijn van het lokale netwerk.
- **On-premise domotica** Isoleer lokaal gehoste domotica-oplossingen op een apart netwerksegment en vermijd afhankelijkheid van netwerkdiensten in andere segmenten. Zorg dat verkeer van en naar dit netwerksegment ‘least-privilege’ is ingericht en controleer de firewallregels periodiek.
- **VPN-beveiliging** Versterk het wachtwoordbeleid en accountmanagement voor VPN-oplossingen. Zie bijvoorbeeld CIS Critical Controls 4 en 5 (versie 8). Dit in verband met de vele aanvallen op VPN-oplossingen.
- **Spoedpatch** Zorg ervoor dat internet-gekoppelde systemen met spoed gepatcht kunnen worden. Zoals in het volgende hoofdstuk besproken, maak hier ook afspraken over met je leverancier. Controleer na het patchen of er niet al ingebroken was op het systeem.
- **Beperk opslag gevoelige data** Beperk opslag van gevoelige data op systemen die ontsloten zijn aan het internet en stel een retentietijd in waarna de bestanden automatisch verwijderd worden. Dit naar aanleiding van misbruik van enkele zero-day kwetsbaarheden in online omgevingen voor bestandsoverdracht door ransomware-actoren.
- **Maatregelen tegen phishingaanvallen waar MFA wordt omzeild** Zie hoofdstuk ‘datalekken’ voor mitigaties.

Handelingsperspectief ransomware

- **CIS Critical Controls** Overweeg het gebruik van het CIS Critical Controls framework voor het selecteren en prioriteren van beveiligingsmaatregelen [13]. Raadpleeg het artikel ‘Praktijkverhaal: CIS Controls framework kan helpen om hackers buiten de deur te houden’ voor meer informatie, inclusief de relatie tot de NEN7510 [14].
- **Security baselines** Gebruik configuratiestandaarden zoals ‘CIS benchmarks’ of Microsoft security baselines, zowel voor software als clouddiensten. Hierdoor voorkomt u dat u belangrijke configuratieopties over het hoofd ziet. Z-CERT schat in dat hiermee met weinig moeite en kennis, toch veel winst kan worden behaald.
- **NCSC incident response-plan ransomware** Raadpleeg het NCSC-incidentresponse-plan voor gedetailleerde voorbereiding op ransomware-aanvallen [15].
- **CISA ransomware analyses** Lees CISA-papers over analyses van ransomware-actoren en tegenmaatregelen. Enkele relevante papers voor de zorgsector zijn het paper over de actor Lockbit [16] en Rhysida [17].

dreiging

Ransomware bij leveranciers

Inschatting dreiging: hoog

Z-CERT schat het dreigingsniveau voor incidenten door ransomware en/of afpersen met datalekken bij leveranciers van zorginstellingen in als 'hoog'. Dit dreigingsniveau is gebaseerd op dezelfde redenen die eerder zijn besproken in de dreigingsbeoordeling voor zorgaanbieders, zoals vermeld in het vorige hoofdstuk.

Verder heeft Z-CERT geobserveerd dat IT-dienstverleners in Europa vaker getroffen worden door dergelijke incidenten dan de zorgaanbieders zelf. Dit kan impact hebben op zorginstellingen indien zij diensten afnemen van deze leverancier.

Voorspelling 2024

In het komende jaar verwacht Z-CERT dat er meerdere ransomware-incidenten zullen plaatsvinden bij leveranciers, met impact op Nederlandse zorginstellingen.

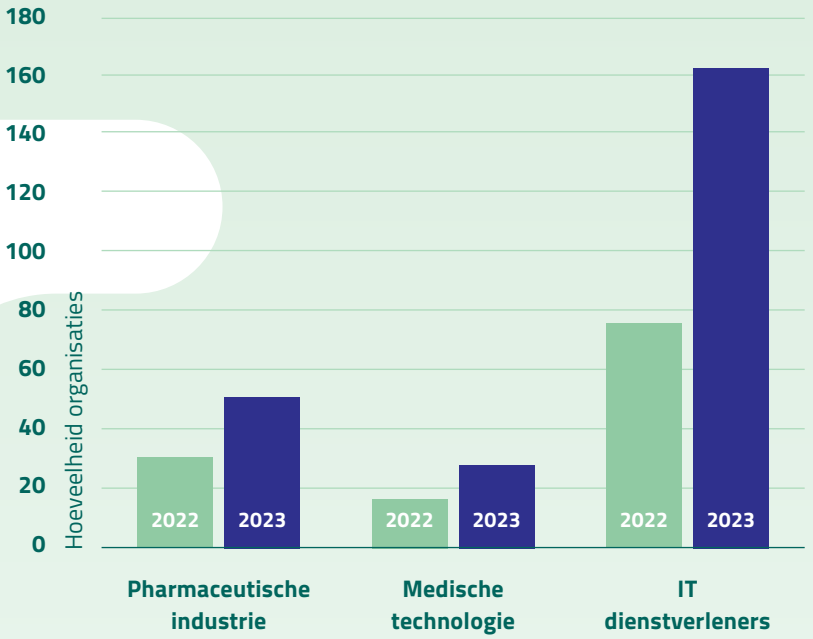
Waarom de focus op leveranciers?

De zorg ondergaat een digitale transformatie met een groeiende afhankelijkheid van digitale dienstverleners. Zorginstellingen zijn verantwoordelijk voor de bescherming van persoonsgegevens en voor het monitoren, beoordelen en auditen van externe leveranciers. Het is daarom belangrijk om met leveranciers het gesprek aan te gaan over hun weerbaarheid tegen ransomware-aanvallen.

Voor risicoanalyses is het van belang om rekening te houden met leveranciers van digitale diensten, maar ook met leveranciers van belangrijke fysieke producten. Incidenten bij leveranciers kunnen problemen veroorzaken als leveringen van bijvoorbeeld medicijnen of apparaten worden belemmerd.

Incidenttrends

Ook bij leveranciers van zorginstellingen werden er meer incidenten geregistreerd op datalekwebsites. Bij producenten van medische technologie was er wereldwijd een stijging van 63 procent en in de farmaceutische industrie 75 procent (zie figuur 4). Een andere sector die belangrijk is voor de zorgsector is de IT-sector. In deze sector steeg de hoeveelheid incidenten wereldwijd met 117 procent.



Figuur 4

Hoeveelheid incidenten in 2022 en 2023

Uit de vragenlijst die door de Z-CERT deelnemers is ingevuld, blijkt dat bij 9 procent van de respondenten in 2023 een leverancier was geraakt door ransomware. In twee gevallen ging het om meerdere ransomware-incidenten. Daarbij waren data gelekt en in één geval kon een zorginstelling tijdelijk geen gebruik maken van een financieel systeem waardoor een deel van de financiële afdeling stil lag.

Tevens moest gecontroleerd worden of data nog betrouwbaar waren. Ook moest in sommige gevallen de VPN-verbinding met leverancier preventief dicht worden gezet voor leveranciers van medische systemen en een leverancier van gebouwbeheersystemen. De impact lijkt dan klein, maar het kostte wel tijd om de handeling uit te voeren en te controleren of er geen malafide activiteiten zijn geweest.

Er waren in 2023 een aantal noemenswaardige incidenten in Nederland en Europa die de risico's van afhankelijkheid van leveranciers goed blootleggen. Zo heeft er een ransomware-incident plaats gevonden bij een leverancier van alarmknoppen [18]. De communicatie tussen de knoppen en de meldkamer was niet meer operationeel. In Nederland gebruiken veel zorgorganisaties een dergelijke oplossing. Doordat deze knoppen niet meer werkten, moest personeel van een organisatie extra maatregelen nemen om zeker te zijn, dat een cliënt niks zou overkomen.

"Een aantal noemenswaardige incidenten in 2023 leggen de risico's van afhankelijkheid van leveranciers goed bloot"

Bij een leverancier in Zweden heeft een cyberincident plaatsgevonden waardoor twee ambulancediensten in het Verenigd Koninkrijk geen toegang meer hadden tot hun elektronische patiëntendossier. Hoewel ransomware niet formeel als oorzaak is benoemd, werd ambulancepersoneel hierdoor afhankelijk van pen en papier voor het overdragen van een patiënt aan het ziekenhuis [19].

Trends methoden en technieken
Het risico op incidenten door het ontbreken van MFA op een leveranciers-account of het niet optimaal inrichten van privileged access management en netwerksegmentatie is nog steeds actueel. Wat in 2023 opviel bij zorginstellingen in Europa, is dat er incidenten waren doordat leveranciers te laat waren met het updaten van on-premise systemen van zorgaan-bieders. Deze vertraging gaf kwaadwillenden de kans om achterdeuren in systemen te creëren. Soms bleven deze achterdeuren in eerste instantie een tijd ongebruikt. Dit komt bijvoorbeeld omdat de kwaadwillende die de achterdeur heeft geplaatst deze niet zelf gebruikt, maar doorverkoopt aan anderen. Vervolgens kan degene die de achterdeur inkoopt de verkregen toegang gebruiken voor bijvoorbeeld het stelen van data of het verspreiden van ransomware. Dit verkoopproces kan even duren.

Handelingsperspectief
Zie ook het handelingsperspectief in het hoofdstuk 'Ransomware bij zorginstellingen'. De genoemde aanbevelingen zijn ook toepasbaar op leveranciers.

Tijdens ransomware-aanvallen of pogingen daartoe bij leveranciers of op systemen die door leveranciers worden beheerd in zorginstellingen, hebben zorginstellingen een aantal lessen geleerd die we graag willen delen in dit dreigingsbeeld:

- **Regievoering op leverancier** Controleer of leveranciers up-to-date zijn met patchen van uw systemen, bijvoorbeeld op basis van dreigings-informatie die u via Z-CERT krijgt. Houd hen aan patchafspraken die vastgelegd zijn in een Service Level Agreement (SLA). Z-CERT constateert dat dit regelmatig misgaat.
- **Afspraken met leveranciers en incident response** Leg duidelijk vast voor systemen, welke leverancier verantwoordelijk is voor incident response-taken. Dit voorkomt discussies tijdens een incident.
- **Stel vragen aan een leverancier**. Bijvoorbeeld: wat doet uw leverancier om phishingmethoden te mitigeren waar MFA wordt omzeild? Is uw leverancier er bewust van dat de snelheid waarmee kwetsbaarheden misbruikt worden, is toegenomen?
- **Vereis multifactorauthenticatie** voor leverancier accounts die toegang geven tot uw systemen en geef alleen toegang tot uw netwerk middels een 'privileged access management'-oplossing.
- **Pentest en red teaming** Voert uw leverancier regelmatig pentests en red teaming tests uit? Juist bij deze oefeningen wordt de 'papieren werkelijkheid' op de proef gesteld. Als input kan uw leverancier voor deze testen de documenten van CISA gebruiken [16] [17]. Zie ook de NEN7510 beheermaatregel A.15.2.1.

dreiging

Datalekken (niet door ransomware)

Inschatting dreiging: medium tot hoog

Z-CERT schat het dreigingsniveau voor datalekken (niet door ransomware) binnen de zorg in als 'medium' tot 'hoog'. Dit betekent dat er op korte termijn incidenten worden verwacht waarbij sprake is van een datalek.

Er zijn verschillende manieren waarop datalekken plaatsvinden. Dit deel van het dreigingsbeeld zoomt in op de datalekken die plaatsvonden door de cyberincidenten, zoals credential phishing, malware, hacking. Datalekken door foutieve e-mails en verlies van gegevensdragers zijn niet meegenomen in dit dreigingsbeeld. Datalekken als gevolg van afpersing zijn in het vorige hoofdstuk besproken.

Z-CERT schat het dreigingsniveau voor datalekken veroorzaakt door hacking in als 'hoog'. Z-CERT verwacht binnen een jaar enkele datalekken die veroorzaakt worden door hacking. In deze gevallen zal de impact hoger zijn dan bijvoorbeeld bij een phishingincident omdat er meer gevoelige data worden buitgemaakt. Z-CERT schat het dreigingsniveau voor datalekken veroorzaakt door credential phishing, malware in als 'medium'. Daarnaast willen wij aandacht vragen voor het risico van het lekken van data door misconfiguraties en niet correct buiten gebruik stellen van (medische) apparatuur.

> **"Z-CERT verwacht binnen een jaar enkele datalekken die veroorzaakt worden door hacking"**

Incidenten

Bij Z-CERT worden wekelijks meerdere credential phishing-pogingen en malware-phishingmails gemeld die door de spamfilters zijn gekomen. In het onderzoek onder onze deelnemers geeft 12 procent aan dat er bij credential phishing-incidenten wachtwoorden zijn gestolen. Bij deze incidenten was geen sprake van compromittatie dankzij het gebruik van multifactor-authenticatie (MFA). Ook werden dit jaar vijf aanvallen gemeld waarbij MFA wel werd omzeild. Bij een van deze gevallen leidde dit tot de compromittatie van vier mailboxen. Gecompromitteerde mailboxen worden door kwaadwillenden vaak gebruikt voor verdere malware- en phishingaanvallen. De gecompromitteerde mailbox van een medicijnleverancier heeft voor aanzienlijke impact gezorgd bij meerdere zorginstellingen. De phishingmail die vanuit die mailbox werd verstuurd, leidde uiteindelijk tot het lekken van wachtwoorden van meer dan 50 zorgorganisaties en enkele datalekken bij de organisaties die MFA niet op orde hadden. Het is goed om te realiseren dat kwaadwillenden de verkregen toegang vaak kunnen gebruiken om verder een cloudomgeving binnen te dringen en naast mail b.v. ook andere data buit te maken.

Webapplicaties

Datalekken kunnen ook naar voren komen bij het scannen van webapplicaties op kwetsbaarheden. Dat kan dan gaan om cliënt-/patiëntportalen, uitwisselingssystemen voor zorgverleners en dergelijken. Kwaadwillenden kunnen deze kwetsbaarheden misbruiken en data stelen. Afgelopen jaar heeft Z-CERT bijvoorbeeld een melding ontvangen waarbij e-mailadressen en gehashte wachtwoorden waren gesloten uit een kwetsbare online leeromgeving. Z-CERT kent daarnaast ook voorbeelden waarbij ethische hackers aantonen dat gevoelige persoonsgegevens zichtbaar zijn via het internet.

Datalekken bij leveranciers

Bij Z-CERT zijn acht Nederlandse gevallen bekend waarbij er data van zorginstellingen werden gelekt via een leverancier. In twee gevallen was dit gebeurd via een onderleverancier. De impact viel gelukkig vaak mee. Maar dat het flink mis kan gaan, kwam sterk naar voren door incidenten bij Nebu [20] en bij MoveIT [21], waarover veel in de media is verschenen. Z-CERT ziet de afgelopen jaren een toename van de afhankelijkheid in de keten tussen zorgorganisaties en leveranciers van IT. Dit brengt het risico met zich mee dat een zorginstelling de eigen cyberhygiëne wel op orde heeft, terwijl een externe partij niet voldoende is toegerust op de digitale dreigingen van nu.

Samenvattend kan worden gesteld dat de dreiging dat data uitlekken via een (onder)leverancier reëel is.

Datalekken cloud

De zorg maakt steeds meer de transitie naar de cloud waarbij veel gebruik gemaakt wordt van webapplicaties en mobiele apps. In 2023 werd deze dreiging zichtbaar toen een ethische hacker toegang kreeg tot gevoelige data verzameld via een app voor het melden van grensoverschrijdend gedrag in ziekenhuizen. Dankzij een misconfiguratie kon hij gevoelige informatie inzien en het beheerderwachtwoord onderscheppen. In Zwitserland speelde eenzelfde situatie waarbij informatie over de geestelijke gezondheid van patiënten kon worden ingezien. Dit werd door een van de gedupeerden als een ernstige inbreuk ervaren.

Ook speelde in 2023 het probleem dat gevoelige data, in de vorm van configuratiebestanden, door een fout van een medewerker publiek werden gezet. In configuratiebestanden staan vaak credentials, waaronder API-keys die zonder MFA-toegang geven tot andere cloudservices. Deze bestanden worden over het algemeen twee minuten na publiek zetten al door kwaadwillenden gevonden [22]. Een ander voorbeeld is dat per ongeluk meer toegang gegeven wordt dan nodig. Bij een Indiaas medisch diagnostisch laboratorium is in 2023 op die manier een database met informatie over 12 miljoen patiënten toegankelijk gemaakt [23].

> **“Configuratiebestanden worden over het algemeen twee minuten na publiek zetten al door kwaadwillende gevonden”**

Naast de besproken misconfiguraties is het gebruik van third-party apps binnen cloudoplossingen een risico voor de gehele cloudomgeving. Z-CERT ziet dit risico bij b.v. Microsoft Appsource en Google Suite Marketplace waar apps vaak hoge rechten verkrijgen na installatie [24].

Cybercriminelen kunnen de verkregen toegang tot de Office 365-omgeving van een legitieme organisatie misbruiken door kwaadaardige apps onder hun naam te creëren en te publiceren [25]. Ze versturen vervolgens phishingmails naar gebruikers, waarin ze vragen om deze malafide apps toegang te verlenen tot gevoelige gegevens, zoals cliënten- of patiënten-data. Omdat de app lijkt te zijn gepubliceerd door een legitieme partij, vertrouwt de gebruiker deze en geeft de app toegang. Eenmaal verkregen, kan MFA het lekken van data niet meer voorkomen.

Datalekken en afgedankte medische apparatuur

Een apparaat voldoet niet meer aan de eisen die een organisatie eraan stelt, maar is nog niet aan het einde van de levensduur. Of het leasecontract van een medisch apparaat loopt af. Als het apparaat wordt verkocht, gedoneerd of hergebruikt, kan het volledig verwijderen van de daarop opgeslagen data een uitdaging zijn. Incidenteel kunnen fouten optreden, wat resulteert in datalekken. Er is bij Z-CERT één casus bekend waarbij datadragers onvoldoende opgeschoond waren. Als het een medisch apparaat is, dan kan dat behoorlijk ernstig zijn.
Van dat laatste zijn er bij Z-CERT in 2023 geen voorbeelden bekend, maar het risico is reëel. Rapid7 heeft in de Verenigde Staten onderzoek gedaan naar tweedehands infuuspompen en kwam tot de bevinding dat daar vaak de wifi-inloggegevens nog in waren achtergebleven [26].

Technieken en trends

Om te beginnen blijft het aantal business email compromise (BEC) gevallen aanhouden. Ook het lekken van data via API's blijft actueel. Daarnaast constateerde Z-CERT in 2023 de volgende trends:

- Z-CERT zag in 2023 voor het eerst Attacker in the Middle (AitM) phishing-aanvallen in de zorg. Een kwaadwillende omzeilt bij dit type phishing de MFA-barrière. Het MFA-verzoek wordt doorgespeeld aan het slachtoffer en als die deze beantwoordt, heeft de kwaadwillende toegang.
  Door maatregelen van Microsoft gebruiken kwaadwillenden steeds minder vaak Office macro's. Met het wegvallen van deze aanvalsmogelijkheid hebben kwaadwillenden afwisselend veel verschillende andere methoden gebruikt om malware en phishinglinks te verspreiden. Hierbij worden grote, bekende cloudproviders vaak gebruikt (zoals Adobe, Google, Dropbox, Microsoft) om phishinglinks legitiem te laten lijken. Op onze website staat een artikel waar hier dieper op ingegaan wordt [27].
- Een ander fenomeen dat sinds afgelopen zomer werd waargenomen, was Microsoft Teams-phishing. Hierbij worden phishingberichten gestuurd naar Microsoft Teams-gebruikers [28] [29]. In Office365 kan de functionaliteit "Safe links" geactiveerd worden om gebruikers te beschermen tegen phishing url's in zowel e-mail als in Teams.

Handelingsperspectief

Er is veel informatie beschikbaar over het voorkomen van datalekken door de cyberincidenten. We verwijzen hier zoveel mogelijk naar bestaande kennisproducten zoals de Critical Controls (versie 8) van het Centre for Internet Security (CIS) [30].

1. Gebruik phishing resistente MFA om te voorkomen dat MFA wordt omzeild. Zie de factsheet van het NCSC 'Volwassen authenticeren – gebruik veilige middelen voor authenticatie' [31].

2. Zorg voor een awareness-programma voor het herkennen van phishing en malware. Een eenmalige training is onvoldoende. Besteed hierbij ook aandacht aan QR-code phishing en beveiligingsrisico's bij het gebruik van de cloud. Zie CIS Critical Control 14 [30].
3. Voorkom Teams-phishing door te managen vanaf welke domeinen contact gelegd mag worden met uw gebruikers [32].
4. Gebruik de 'Identity and access'-functionaliteiten in de cloud en richt deze in volgens security best practices, zoals bijvoorbeeld gedefinieerd in CIS Critical Controls 5 en 6. Zie ook 'cloud companion' van CIS Critical Controls [33].
5. Informatiebeveiligingseisen moeten worden vastgelegd in de overeenkomst die u met een leverancier van digitale diensten sluit. Gebruik voor het inschatten van de risico's de door Z-CERT en haar deelnemers opgestelde vragenlijst, voortkomend uit het leveranciersrisicomanagementproject [34]. Ook het NCSC kwam dit jaar met handvatten over hoe om te gaan met de cybersecurity risico's in de toeleveringsketen [35].
6. Aanvullend op het bovenstaande is het raadzaam om gemaakte afspraken over databeveiliging ook te laten gelden voor onderleveranciers die data verwerken. Dergelijke afspraken kunnen bijvoorbeeld worden vastgelegd in een verwerkersovereenkomst, zoals vanuit de AVG vereist kan zijn. Omdat bij dataverwerking vaak diverse partijen onderling samenwerken, is het belangrijk om te verifiëren of over de gehele keten voldoende beveiligingsmaatregelen getroffen zijn, om het risico op datalekken te beperken.
7. Gebruik standaarden voor het veilig configureren van applicaties, netwerkapparaten en cloud omgevingen. Bijvoorbeeld de CIS-benchmarks [36], die zijn leverancier/product specifiek en ook beschikbaar voor alle grote cloud providers.
8. Neem maatregelen om het uitvoeren of downloaden van malware te voorkomen. Zie CIS Controls 2, 4, 9 en 10. Overweeg in Windows omgevingen 'Attack surface reduction rules' te activeren.
9. Voor het voorkomen van misbruik van kwetsbaarheden zijn pentests, vulnerability management en patchmanagement zeer belangrijk. Zie hiervoor CIS Critical Controls 7 en 18. Als u zelf software ontwikkelt is CIS control 16 relevant. Belangrijk om mee te nemen in pentests zijn webapplicaties, mobiele apps en API-endpoints.
10. Het is raadzaam om een CVD-proces in te richten zodat ethische hackers weten hoe ze hun bevindingen kunnen rapporteren. Z-CERT kan deelnemers hierbij ondersteunen [37].
11. Manage third-party apps in uw cloudomgevingen en geef enkel permissies die nodig zijn. Blokkeer de mogelijkheid voor gebruikers om rechtstreeks third-party apps toegang te geven tot uw data. Op die manier voorkomt u dat 'consent phishing' succes heeft.
12. Sla wachtwoorden nooit op in configuratiebestanden (zoals .env-bestanden of git-configuratiebestanden) maar alleen in daarvoor speciaal beveiligde wachtwoordkluizen. Stel op uw webservers regels in zodat deze bestanden nooit inzichtelijk kunnen zijn vanaf het internet.
13. Z-CERT adviseert bij buiten gebruik stellen van elektronische apparaten data te verwijderen en vernietigingsprocessen te volgen. Centrale regie en een actuele database van assets (Configuration Management Database, CMDB) zijn hiervoor belangrijk. Sommige zorgorganisaties besteden vernietiging uit aan gespecialiseerde bedrijven, waarbij ze rapportages controleren en steekproefsgewijs de kwaliteit toetsen. Raadpleeg "NIST SP 800-88 Guidelines for Media Sanitization" voor meer informatie [38].

dreiging

DDoS

Inschatting dreiging: medium

Z-CERT schat het dreigingsniveau voor DDoS-aanvallen op zorginstellingen in op 'medium'. De dreiging is echter groter dan vorig jaar, aangezien het afgelopen jaar duidelijk is geworden dat ook de Nederlandse zorgsector actief wordt aangevallen door politiek activistisch geïnspireerde actoren (hacktivisten).

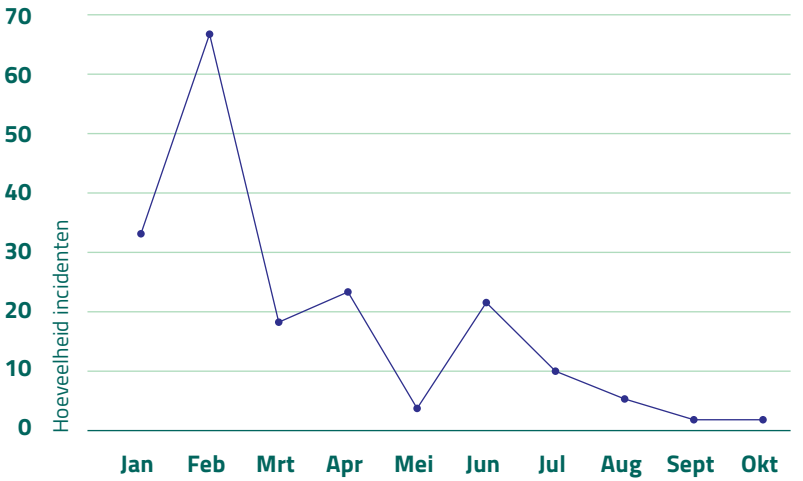
Voorspelling 2024

Z-CERT verwacht dit jaar enkele DDoS-incidenten met geringe tot medium impact op Nederlandse zorginstellingen, op basis van geopolitieke ontwikkelingen kan dit oplopen tot tientallen incidenten.

Incidenten

Het dreigingsbeeld voor DDoS-aanvallen veranderde dit jaar toen de zorg het doelwit werd van hacktivisten. Vijftien ziekenhuizen meldden aanvallen tussen 28 en 31 januari 2023. In februari volgden nog enkele DDoS-aanvallen op Nederlandse ziekenhuizen en zagen we een grote stijging in Europa (zie figuur 5). Hacktivisten richtten zich niet alleen op ziekenhuizen. Ook diverse zorggerelateerde partijen werden in hacktivistische Telegram-kanalen genoemd als doelwit. Ook Microsoft observeerde begin 2023 aanvallen op ziekenhuizen (26%) , andere zorggerelateerde organisaties (16%) en zorgverzekeraars (16%) [39].

Hoewel de focus in de eerste twee maanden van 2023 gericht was op de zorg, verschoof deze in de loop van 2023 steeds meer naar andere sectoren [40].



Figuur 5

DDoS-aanvallen uitgevoerd door hacktivistische groepen op zorgsector in Europa

Motief hacktivisme

Bij DDoS-aanvallen op zorgaanbieders heeft Z-CERT verschillende actoren met uiteenlopende motieven geïdentificeerd. Afgelopen jaar registreerde Z-CERT vooral DDoS-aanvallen die werden uitgevoerd vanuit een hacktivistisch perspectief. Een groot deel was bijvoorbeeld gemotiveerd door de Nederlandse steun aan Oekraïne. Hacktivistische actoren reageren vaak op politieke ontwikkelingen of gebeurtenissen die in het nieuws komen. Daarbij zijn er ook groepen die op andere zaken reageren dan de oorlog in Oekraïne. Voorbeelden waren bijvoorbeeld de DDoS-aanvallen als reactie op verbranding van een koran in Denemarken [41] en de rol van de Verenigde Staten in relatie tot een conflict in Sudan [42].
Samenwerking tussen pro-Russische groepen en groepen met andere motieven is vaak nauw. De mate van verbondenheid tussen deze groepen is moeilijk vast te stellen.

DDoS-aanvallen met een ander motief dan hacktivisme

Naast DDoS-aanvallen met een hacktivistisch motief registreerde Z-CERT meerdere DDoS-aanvallen waar het motief niet te achterhalen was. In één geval hebben we het vermoeden dat het ging om iemand die niet tevreden was over de dienstverlening van een zorgorganisatie (en de soms gevoelige casussen die ze behandelen).

Impact DDoS-aanvallen

Hacktivistische aanvallen veroorzaakten meestal enkele uren en in één geval drie dagen overlast op websites, resulterend in vertraging of uitval. Patiënten konden tijdens de aanval de link naar het patiëntenportaal niet bereiken. Bij één zorginstelling was de impact breder doordat de website was gekoppeld aan de achterliggende IT-infrastructuur, wat leidde tot kortdurende overlast bij andere digitale diensten, de impact was minimaal. Bij deze incidenten is het ook het geval dat veel belanghebbenden geïnformeerd moeten worden en dat het incident negatieve publiciteit kan opleveren.
Bij één incident veroorzaakte de DDoS-aanval vertraging in de ontvangst van alarmmeldingen van cliënten, doordat het betreffende domotica systeem in de cloud niet meer bereikbaar was. De impact werd gemitigeerd door DDoS-bescherming van de cloudoplossing te activeren. Hier waren kosten aan verbonden.

> **“Hacktivistische aanvallen veroorzaakten vaak enkele uren en in één geval drie dagen overlast op websites, resulterend in vertraging of uitval”**

Trends methoden en technieken

DDoS-groepen maken gebruik van een veelheid aan technieken. Deze zullen in het hoofdstuk over DDoS en leveranciers worden toegelicht.

24

Leerpunten uit 2023

Tijdens de aanvallen werden er door zorginstellingen een aantal lessen geleerd die we in dit dreigingsbeeld graag willen delen. Onder deze lijst zullen we het algemene handelingsperspectief meegeven.

1. **Geo-blocking** Tijdens een DDoS-aanval kan het zinvol zijn om netwerkverkeer uit andere landen te blokkeren. Afgelopen jaar kwamen bij incidenten in Nederland de meeste DDoS-aanvallen uit China [43]. Dat wil niet zeggen dat de actoren hierachter Chinees zijn, maar dat de gebruikte infrastructuur in China staat. Op deze website [43] is een actueel overzicht te vinden van waar de DDoS-aanvallen vandaan komen.
2. **Proactieve DDoS-beveiliging in de cloud** Identificeer belangrijke systemen en IP-adressen in de cloud en monitor deze actief op DDoS-aanvallen. Verifieer of uw cloudleverancier hiervoor functionaliteit aanbiedt en zorg dat u in staat bent DDoS-beveiliging voor de betreffende IP-adressen te activeren.
3. **Beperk verstoringen op andere diensten** Zorg dat een DDoS-aanval op de website geen verstoringen elders in het netwerk oplevert. Dit doet u door de website gescheiden van de rest van het netwerk te hosten, bijvoorbeeld bij een andere webhostingpartij.
4. **Beperk de impact van een aanval**
   - Schakel tijdens een aanval over naar een vereenvoudigde, statische website voor betere prestaties en minder downtime.
   - Implementeer maatregelen zoals Content Distribution Networks en webcaching.
5. **Stel een incident response plan op**
   Wanneer kritische systemen worden aangevallen (on-premise of in de cloud), wil je voorbereid zijn. Zie [44] voor een voorbeeld incident response plan.

Handelingsperspectief

- Factsheet Continuïteit van online diensten [45]
- Factsheet Technische maatregelen voor continuïteit voor online diensten [46]

dreiging

DDoS bij leveranciers

Inschatting dreiging: medium

Z-CERT schat het dreigingsniveau voor DDoS-aanvallen op leveranciers van zorginstellingen in op 'medium'. De dreiging is echter wel iets groter dan vorig jaar omdat in 2023 bleek dat ook Nederlandse hostingpartijen actief aangevallen zijn door hacktivisten. Dit heeft impact op zorginstellingen en leveranciers van zorginstellingen.

Voorspelling 2024

Z-CERT verwacht in 2024 meerdere DDoS-incidenten met impact op de zorg te zullen registeren. Op basis van geopolitieke ontwikkelingen kan dit oplopen tot tientallen. Afhankelijk van het type leverancier kan de impact klein zijn, maar als bijvoorbeeld een SaaS-leverancier geraakt wordt die belangrijk is voor het zorgproces kan de impact groter zijn.

Incidentfrequentie leveranciers

17 Procent van de respondenten meldde een DDoS-aanval op een leverancier met impact op zorgorganisaties (zie grafiek 1). Opvallend is dat het vooral bedrijven van digitale diensten betreft. In enkele gevallen was dit doordat hacktivisten de hostingpartij aanvielen, zonder dat de aanval specifiek gericht was op de zorginstelling. Dit had impact op een jeugd-zorginstelling, een ouderenzorginstelling en een ziekenhuis.
Bij andere aanvallen was het motief van de aanval niet duidelijk. Wel is duidelijk dat aanvallen met een hacktivistisch motief sterk in opkomst zijn. Uit onderzoek blijkt dat 66 procent van de aanvallen geopolitiek gemotiveerd is. Slechts 5 procent had een andere motivatie (zoals financieel) en van 28 procent was het motief niet bekend [40] . De ISP-sector had in 2023 rond de 500 DDoS-aanvallen per kwartaal.

Dit laat zien dat de dreiging voor dit soort leveranciers veel groter is dan die van zorginstellingen zelf. Ook voordat de oorlog in Oekraïne begon had deze sector al last van grote hoeveelheid DDoS-aanvallen. In 2021 werden er gemiddeld ongeveer 700 incidenten per kwartaal geregistreerd [47].

Type dienstverlener	Impact op zorginstelling
DNS-provider	Website via de domeinnaam niet bereik-baar of vertraagd bereikbaar
SaaS-provider	
Website hoster	Websites niet bereikbaar of vertraagd
Cloudleverancier	
Netwerkleverancier	DDoS-aanval werd gemitigeerd
Patiëntenportaal	Niet bereikbaar

Figuur 6

Leveranciers van zorginstellingen die geraakt werden door een DDoS-aanval

De impact was meestal niet groot. Maar met de 'verSaaSing' van het applicatielandschap, wordt het steeds belangrijker voor de zorgsector om het met leveranciers te hebben over bescherming tegen DDoS-aanvallen. Illustratief was de aanval die we in het vorig hoofdstuk beschreven waar de cloudinfrastructuur van een zorginstelling werd aangevallen. Dit kan ook gebeuren bij bijvoorbeeld een leverancier die een domotica-dienst of een aanbieder van een patiëntmonitoringdienst in de cloud. Zij moeten in staat zijn op een DDoS-aanval te reageren en het liefst op een geautomatiseerde manier. Het is reëel dat een clouddienst wordt aangevallen. Begin juni 2023 werd Microsoft Azure aangevallen met een DDoS-aanval, wat leidde tot verstoringen. Motief van de groep die dit uitvoerde was deels afpersing en deels hacktivisme [40]. Ook gaf een zorginstelling aan overlast te hebben ervaren door deze DDoS-aanvallen. Naast Microsoft geeft ook Google aan dat er aanvallen zijn geweest op Google services en de Google Cloud infrastructuur, waaronder dit jaar de grootste aanval die ze ooit hebben gehad [48].

Trends methoden en technieken

Er zijn verschillende typen DDoS-aanvallen. Zowel op de netwerklaag als op de applicatielaag. Nederland werd op de netwerklaag in 2023 met name aangevallen met SYN floods (70%), Memcached Floods (10%) en Ack floods (6%) [43]. De laatste stand van zaken, specifiek voor Nederland, is online te vinden [43] en kan input vormen voor gesprekken met leveranciers. Alhoewel deze technieken veel gebruikt worden, is het beeld genuanceerder. Organisaties die DDoS-aanvallen monitoren geven aan dat de moderne DDoS-aanvaller veel meer aanvalsvectoren tot zijn beschikking heeft dan tien jaar geleden. Een serviceprovider meldde dat in het eerste helft van 2023 bij 53 procent één aanvalsvector werd gebruikt. Bij 38 procent waren dat twee tot vijf aanvalsvectoren en bij 9 procent zes tot tien aanvals-vectoren. Verdediging tegen meerdere aanvalsvectoren is complexer. Ook binnen een bepaalde aanvalsvector kan een aanvaller soms variëren [49]. Daarnaast geven bronnen aan dat bij aanvallen een groter volume wordt gebruikt en dat de hoeveelheid aanvallen is toegenomen, met name voor Europa [50].

Een andere trend dit jaar was een 20 procent toename van 'DDoS for hire'-platformen. Op deze platformen kan een DDoS-aanval gekocht worden voor soms weinig geld (vijf dollar). Deze laagdrempeligheid geeft personen die wraak willen nemen, zonder veel kennis, een krachtig wapen in handen [40].

Leerpunten uit 2023

Tijdens de aanvallen werden er door zorginstellingen een aantal lessen geleerd die we in dit dreigingsbeeld graag willen delen. Voor het algemene handelingsperspectief verwijzen we naar het vorige hoofdstuk (DDoS).

1. **Beoordeel leveranciers** Beoordeel leveranciers op hun weerbaarheid tegen DDoS-aanvallen. (zie NEN 7510 beheersmaatregel A.15.2.1).
2. **Kiezen nieuwe leverancier** Kies leveranciers die hun DDoS-mitigatie op orde hebben omdat zij bijvoorbeeld aangesloten zijn bij een wasstraat. Controleer wel of IP-adressen die u afneemt zijn meegenomen in de mitigatie. Z-CERT constateert dat dit niet altijd het geval is.
3. **Vooraf overleg met leveranciers** Voorkom discussies over kosten tijdens een DDoS-aanval. Bespreek vooraf met leveranciers welke DDoS-maat-regelen zijn genomen en maak duidelijke afspraken om conflicten over kosten te vermijden.

dreiging

Cyberspionage door statelijke actoren

Inschatting dreiging: hoog of laag (afhankelijk van type organisatie)

Z-CERT schat het dreigingsniveau voor cyberspionage door statelijke actoren voor verschillende typen organisaties anders in. Voor zorgorganisaties waar veel wetenschappelijk onderzoek wordt gedaan dat relevant is voor statelijke actoren of die relevante persoonsgegevens hebben, schat Z-CERT deze dreiging in als 'hoog'. De hoge dreiging wordt veroorzaakt doordat de aanvallers een hoog niveau, veel geduld en veel geld hebben om hun missies te volbrengen.

Daarnaast kunnen zorginstellingen een doelwit zijn als informatie hebben over mensen die gebruikt kan worden ten behoeve van onder meer rekruterings- en/of beïnvloedingsdoeleinden. Voor zorginstellingen die geen relevante informatie of data hebben schatten we de dreiging in als 'laag'.

Voorspelling 2024

Z-CERT verwacht dat cyberspionage in 2024 actueel zal blijven.

Incidenten

Statelijke actoren staan erom bekend via de leverancierskеten toegang te verkrijgen tot organisaties. Dit jaar was dat ook het geval. De legitieme desktopapplicatie van de VoIP-softwareoplossing 3CX bleek malware te bevatten. De kwaadaardige update werd actief verspreid onder klanten. Ook enkele deelnemers van Z-CERT en tientallen eerstelijns praktijken, zoals huisartspraktijken en fysiotherapiepraktijken bleken de software te gebruiken. De actor achter deze aanval was een subgroep van Lazarus, een groep geassocieerd met Noord-Korea. Het motief van deze groep is hoogstwaarschijnlijk financieel gewin want ze was voornamelijk gericht op bedrijven die actief zijn in cryptovaluta [51]. De zorginstellingen waren hoogstwaarschijnlijk bijvangst. Bij Z-CERT zijn er geen meldingen binnengekomen van concreet misbruik.

Nederland staat op de achtste plaats op de ranglijst van Europese landen die het meest doelwit zijn van digitale aanvallen door statelijke actoren [9]. Toch lijkt het niet waarschijnlijk dat de zorgsector op dit moment het voornaamste doelwit is van statelijke spionagecampagnes. Zo zijn er bij Z-CERT geen incidenten gemeld waarbij spionageactiviteiten worden uitgevoerd. Ook staat de zorgsector in het jaarlijkse dreigingsrapport van Microsoft niet in de top 10 van de door cyberspionage geraakte actoren [2]. We weten echter vanuit internationale bronnen dat de zorg wel degelijk doelwit is doordat er zo nu en dan incidenten bekend worden gemaakt [52]. Bovendien signaleert de AIVD dat kennisinstellingen en wetenschappers frequent het doelwit zijn van diverse digitale aanvalscampagnes, met als voornaamste doel het bemachtigen van hoogwaardige technologische kennis [53]. Daarnaast hebben sommige overheden belang bij het vergaren van grote hoeveelheden persoonsgegevens, die voor allerlei doeleinden

kunnen worden gebruikt. Deze gegevens worden in grote hoeveelheden bewaard door zorginstellingen. Z-CERT acht het denkbaar dat er op beperkte schaal doelgerichte professionele aanvallen plaatsvinden op instellingen met als doel informatie te vergaren over voor hen belangrijke personen.

Impact

De gevolgen van gestolen kennis kunnen variëren van oneerlijke concurrentie tot ongewenst gebruik, bijvoorbeeld voor militaire doeleinden. Daarnaast bestaat het risico dat informatie over personen wordt aangewend voor rekruterings- of beïnvloedingsdoeleinden [53]. Gegevens bijvoorbeeld over de psychische en fysieke gezondheid kunnen gebruikt worden om personen onder druk te zetten.

Trends en ontwikkelingen

- Een trend die we in 2023 en 2022 zagen, heeft geen betrekking op spionage maar op ransomware. Er zijn diverse voorbeelden van aan Noord-Korea geassocieerde actoren die Amerikaanse zorginstellingen aanvallen met ransomware [54]. Wij hebben deze aanvallen nog niet gezien in Europa. Het is niet uit te sluiten dat deze actoren in dienst van bekende ransomware groepen aanvallen uitvoeren. Aangezien dit soort actoren uit zijn op financieel gewin en de intentie hebben om zorginstellingen aan te vallen, zijn dergelijke aanvallen ook voorstelbaar in Europa.
- Statelijke actoren gebruikten dit jaar veel 'Living of the land'-technieken. Bij deze technieken probeert de aanvaller vooral functionaliteiten van het systeem zelf te gebruiken om tot zijn doel te komen [9] [55]. Dit duidt erop dat de aanvallers zoveel mogelijk onder de radar willen blijven.

Handelingsperspectief

- **Cyberhygiëne** Handelingsperspectief bij hoofdstuk ransomware en datalekken is wat betreft cyberhygiëne maatregelen ook van toepassing op de dreiging van spionage door statelijke actoren. Een framework als 'CIS Critical Controls' is daarbij erg praktisch.
- **Risicoanalyse en risicomanagement** Kijk naar uw organisatie vanuit het perspectief van een aanvaller en identificeer technologieën, kroonjuwelen wat betreft kennis en onderzoek, die mogelijk interessant zijn voor statelijke actoren. De AIVD heeft hier b.v. de 'handleiding kwetsbaarheidsonderzoek spionage' [56] dat u hierbij kan helpen. Het loket kennisveiligheid heeft een document 'Nationale leidraad kennisveiligheid Veilig internationaal samenwerken' dat hier ook verder op in gaat [57].
- **Detectie en mitigatie 'living of the land'-technieken** Technischer van aard zijn de aanbevelingen van CISA rondom Chinese statelijke actoren die detectie proberen te omzeilen [55].
- **Quickscan** Bij de overheid wordt de 'Quickscan/risicomitigatie nationale veiligheid bij inkoop en aanbesteden' gebruikt [58]. Op basis van de quickscan wordt vastgesteld of er een risicoanalyse nodig is.

dreiging

Digitale financiële fraude

Inschatting dreiging: medium

We bakenen in dit dreigingsbeeld digitale financiële fraude af tot fraude door gebruik te maken van digitale media als mail en WhatsApp. Z-CERT schat het dreigingsniveau hiervan in op 'medium'. Deelnemers melden zeer regelmatig pogingen tot financiële fraude bij Z-CERT. Daarom staat deze dreiging in de radar op dreigingsniveau 'actueel'.

De meeste deelnemers schatten de impact van financiële fraude in als 'beperkt'. In een enkel geval gaat het om incidenten waarbij grote bedragen van meer dan een ton zijn buitgemaakt. Dit overkwam in 2023 twee gemeenten [59] [60] .

Voorspelling voor 2024

Z-CERT verwacht in 2024 vele pogingen tot financiële fraude en verwacht enkele daadwerkelijke incidenten.

Incidenten

Ook in 2023 waren er weer veel pogingen tot financiële fraude waarbij digitale middelen werden ingezet. Die pogingen bestonden in veel gevallen uit het sturen van frauduleuze e-mails, maar ook WhatsApp, sms en telefonie werden gebruikt als medium. In de voor het dreigingsbeeld uitgestuurde vragenlijst gaf 33 procent van de respondenten aan dat zij bij elkaar opgeteld 415 pogingen tot digitale financiële fraude hebben gezien. Ruim 4 procent van de respondenten gaf aan dat de poging succesvol was.
De incidenten zijn in een paar soorten uit te splitsen.

CxO-fraude

Een specifieke vorm van financiële fraude die ook dit jaar weer naar voren kwam, is CEO-fraude. Dat is een vorm van fraude waarbij een leidinggevende nagebootst wordt en waarbij de aanvaller een medewerker van de organisatie probeert over te halen een bedrag over maken. Van de ondervraagde deelnemers heeft 40 procent pogingen tot CEO-fraude gedetecteerd (de totale hoeveelheid kan dus hoger liggen). Bij 2 procent van de ondervraagde deelnemers slaagde een poging tot CEO-fraude. Waar in het bovenstaande CEO staat, kan ook gelezen worden CFO, CIO, CISO en andere vergelijkbare rollen. Daarom hebben we de kop van deze alinea CxO-fraude genoemd.

Malafide facturen

Frauduleuze facturen of spookfacturen komen nog steeds voor. Deels worden deze geautomatiseerd tegengehouden, maar de e-mails komen ook in de mailboxen van medewerkers terecht.

Wijzigen van bankrekeningen

Wat voor malafide facturen geldt, geldt ook voor pogingen om bankrekeningnummers van medewerkers of leveranciers te laten wijzigen. In de survey van Z-CERT zijn de nepfacturen en het wijzigen van bankrekeningnummers in één vraag uitgevraagd. 21 Procent van de respondenten detecteerde frauduleuze facturen of een frauduleuze poging om een rekeningnummer te laten wijzigen. 3 Procent van de ondervraagde deelnemers meldde een geslaagde poging.

Impact en actoren

Financiële fraude richt zich op financiële impact: Kwaadwillenden proberen geld over te laten maken of (digitale) cadeaubonnen te bemachtigen. De actoren kunnen eenlingen zijn die steeds dezelfde techniek herhalen. In geval van cadeaubonnen fraude of frauduleuze facturen is de impact meestal beperkt tot enkele honderden euro's. In andere gevallen, als oneigenlijk medische- of IT-apparatuur aangeschaft wordt uit naam van de organisatie kan de schade tienduizenden euro's bedragen. In een enkel geval lukte een kwaadwillende het om een rekening te wijzigen, waardoor deze eenmalig in staat was een bedrag te confisqueren.

Andere actoren verdiepen zich beter in hun doelwit en zijn daardoor in staat om meer gerichte aanvallen op te zetten. De actoren spreken goed Nederlands en zijn goed in social engineering om hun doelen te bereiken. Ze kunnen leren van informatie op LinkedIn, uit sjablonen voor e-mail handtekeningen die de organisatie verplicht stelt en andere bronnen. Ter indicatie van mogelijke schade: de eerder genoemde incidenten bij gemeenten leidde afgelopen jaar tot schadeposten van 176.040 euro [59] en 236.000 euro [59].

Methoden en technieken

De verschijningsvormen van financiële fraude zijn vergelijkbaar met vorige jaren en zijn reeds eerder benoemd in dit hoofdstuk. Z-CERT registreerde ook een aantal nieuwe technieken waarvan het belangrijk is dat ze op uw radar staan:

- Uit naam van een zorginstelling werden bestellingen gedaan bij webshops. Hiervoor werd een 'lookalike' domein van de zorginstelling geregistreerd. De goederen worden geleverd aan de kwaadwillende en de rekening gaat naar de zorgaanbieder.
- Een kwaadwillende verzamelde van andere websites vacatures (bijvoorbeeld zorggerelateerd of voor IT-specialisten) en verstuurt een factuur voor geleverde diensten naar de organisaties waarvan vacatures op hun site staan. Omdat jouw feitelijke vacatures zichtbaar zijn op de betreffende site ben je sneller geneigd de factuur te betalen. Gezien de krapte op de arbeidsmarkt is het mogelijk dat dit soort fraudepogingen gaat toenemen.
- Een aanvaller creëerde een malafide website waar tegen betaling een afspraak kan maken met een medisch specialist. De 'spookafspraak' waarmee de bezoeker vervolgens de zorginstelling bezoekt is door de instelling zelf nooit geregistreerd en veroorzaakt daarmee de nodige frustratie. Bovendien kan het mogelijk ook medisch nadelige gevolgen hebben voor de bezoeker omdat de diagnose of behandeling is vertraagd.

Leerpunten uit 2023

Tijdens de aanvallen werden er door zorginstellingen een aantal lessen geleerd die we in dit dreigingsbeeld graag willen delen. Onder deze lijst zullen we het algemene handelingsperspectief meegeven.

- Creëer een cultuur waar (bijna-)incidenten makkelijk gemeld worden en maak voorbeelden van dergelijke meldingen bekend zodat collega's ervan kunnen leren.
- Activeer policies in uw mailoplossing, waarbij het niet mogelijk is een leidinggevende na te bootsen (spoofen) omdat de mail dan geblokkeerd wordt.
- Processen gelden ook voor uw directie en bestuur. Als ook hoge functionarissen zich aan de reguliere processen houden, is er veel minder kans op CEO fraude. De nepberichten vallen in dat geval als uitzondering namelijk veel meer op.

> **"Als ook hoge functionarissen zich aan de reguliere processen houden, is er veel minder kans op CEO fraude"**

Handelingsperspectief digitale financiële fraude

- Implementeer e-mailstandaarden (SPF, DKIM en DMARC).
- Monitor op 'look-a-like' domeinnamen die mogelijk misbruikt worden voor criminele doeleinden.
- Security awareness training over dit onderwerp is belangrijk omdat juist bij dit type fraude technische maatregelen niet veel uithalen.
- Pas interne autorisatieprocedures en -processen zo aan dat fraude voorkomen wordt.
- Creëer een procedure waarbij medewerkers pogingen tot financiële fraude kunnen melden. Medewerkers moeten ruimte ervaren om zaken te kunnen melden, zonder het gevoel te krijgen afgestraft te worden als zij een inschattingsfout maken.
- Financiële fraude is een belangrijk punt bij leveranciersmanagement. Het zijn niet altijd de zorginstellingen die 'erin trappen'. Ook de leveranciers worden verleid om artikelen te verzenden naar een adres waar het pakketje makkelijk onderschept kan worden door de crimineel. Maak daarom goede afspraken met de leverancier voor het wijzigen van e-mailadressen, rekeningnummers en leverlocaties. Daarnaast mogen alleen facturen in behandeling worden genomen die via de afgesproken procedures worden aangeboden.

- Aanvullend heeft Z-CERT een factsheet gemaakt met aanbevelingen en een checklist [61]. Het betreft bijvoorbeeld maatregelen rondom e-mailbeveiliging, het trainen van medewerkers en procescontroles.

32

thema

Gebruik van generatieve AI bij cyberaanvallen

Huidige stand van zaken en toekomstige ontwikkelingen

Generatieve AI, vooral bekend door de zogenaamde 'large language models' (zoals chatGPT), heeft revolutionaire veranderingen teweeggebracht. Generatieve AI zal onze manier van werken, leren en creëren fundamenteel veranderen. Het is in staat om tekst, afbeeldingen, audio en video te genereren, gebaseerd op opdrachten van gebruikers. Maar wat is de impact op cybercriminaliteit en hoe kunnen organisaties zich hierop voorbereiden?

Huidige stand van zaken

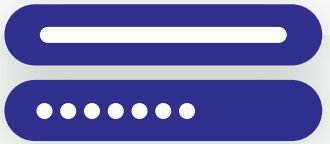
Momenteel is het gebruik van generatieve AI bij cyberaanvallen nog beperkt [62]. Bij Z-CERT zijn nog geen incidenten gemeld, maar het is ook niet altijd mogelijk dit te bepalen omdat bijvoorbeeld door AI genereerde phishingmails niet altijd van echt te onderscheiden zijn. Z-CERT acht het zeer waarschijnlijk dat generatieve AI inmiddels gebruikt wordt voor doelgerichte aanvallen, zoals bij digitale financiële fraude en spearphishing [63].

Verandering van het dreigingslandschap

De inzet van AI bij cybercriminaliteit zal toenemen, aanvankelijk geleidelijk, maar mogelijk met een plotselinge versnelling. Bijvoorbeeld doordat opensource-initiatieven steeds volwassener en meer bruikbaar voor cybercriminelen worden [63]. Er zijn reeds enkele initiatieven op het gebied van AI toegespitst op cybercriminaliteit die mogelijk ook steeds volwassener zullen worden [64].

Hoe zal het dreigingslandschap veranderen?

- **Verbeterde phishingaanvallen** Cybercriminelen die voorheen zorginstellingen aanvielen met generieke e-mails van slechte kwaliteit, kunnen nu op het doelwit afgestemde mails in goed Nederlands sturen.
- **Geavanceerde fraude met audio en video** Fraude zal ook steeds vaker gepleegd worden middels nepaudio en -video, ook wel bekend als deepfakes, die bijna niet te onderscheiden zijn van de werkelijkheid.
- **Efficiëntere cyberaanvallen door AI** Cybercriminelen worden effectiever met behulp van AI. Het kan worden ingezet bij het ontwikkelen van malware, exploits en het automatiseren van complexe aanvallen zoals ransomware. Wel blijft technische kennis van de aanvaller nodig.
- **Toename van succesvolle aanvallen, maar ook betere verdediging** De verwachting is dat door AI het aantal succesvolle cyberaanvallen toeneemt. De kans en impact kan verminderd worden doordat AI ook steeds meer gebruikt zal worden bij defensieve technologieën. Echter, bij de introductie van nieuwe technologieën kunnen er kloven ontstaan die aanvallers een tijdelijk voordeel bieden.



Typen AI-gedreven cyberaanvallen in de zorgsector

De volgende aanvallen worden in de nabije toekomst het meest relevant:

- **Frauduleuze e-mail**
  AI kan worden gebruikt om overtuigende, doelgerichte e-mails te genereren. Dit gebeurt door taalmodellen te trainen op specifieke informatie van het doelwit, zoals LinkedIn-profielen of eerder onderschepte e-mails. Het onderscheppen van e-mail gebeurt geregeld in de zorg.
  Deze gegenereerde mails kunnen ingezet worden voor het opvragen van gevoelige informatie, credential phishing en digitale financiële fraude.

- **Deepfake audio en video**
  Bij deepfake audio of video worden stemmen of beelden van individuen nagebootst, vaak met behulp van materiaal dat online beschikbaar is.
  Dit kan gebruikt worden voor allerlei typen fraude. Bij zorginstellingen kennen we hier nog geen voorbeelden van, echter dit jaar was er een incident in het nieuws waarbij criminelen hulpvraagfraude probeerden te plegen door de stem van een familielid van iemand na te bootsen [65].

Leerpunten uit 2023

De aanvaller van de toekomst is meer gefocust op zijn doelwit, is effectiever en heeft fraudemiddelen die haast niet van de werkelijkheid te onderscheiden zijn. Hoe moeten we hierop reageren?
Eigenlijk worden alle eerder beschreven aanbevelingen, zoals in de hoofdstukken over ransomware, financiële fraude en datalekken, belangrijker. Toch willen we een aantal prioriteiten aanstippen die u helpen om voorbereid te zijn op deze nieuwe werkelijkheid.

- **Identiteit en access management**
  Technologieën die identiteit van iemand verifieert en controleert worden steeds belangrijker:
  - E-mailbeveiligingsstandaarden SPF/DKIM/DMARC en BIMI.
  - Controleer uw mailoplossing op functionaliteit ter voorkoming van identiteitsimpersonatie [66] en activeer deze.
  - Activeer phishing resistente MFA.
  - Voeg extra voorwaarden toe voor toegang tot gegevens, bijvoorbeeld dat men enkel toegang krijgt vanaf een door de organisatie beheerd systeem.

> **“De aanvaller van de toekomst is meer gefocust op zijn doelwit, is effectiever en heeft fraudemiddelen die haast niet van de werkelijkheid te onderscheiden zijn”**

- **Financiële fraude**
  Het wordt steeds belangrijker om financiële processen zo in te richten dat ze niet te omzeilen zijn door een misleide medewerker. In ons kennisproduct over financiële fraude (https://z-cert.nl/factsheet-financiele-fraude) staan diverse maatregelen die hierop inspringen. Een goed voorbeeld is dat bijvoorbeeld alleen de medewerker zelf zijn eigen bankrekening kan wijzigen.

- **Blokkeer malware**
  Preventieve maatregelen tegen malware worden belangrijker. Wat we nu zien is dat e-mails gestolen worden door malware en weer hergebruikt worden voor fraude. Met AI kan een aanvaller zijn modellen trainen met dit gestolen materiaal om mails te genereren in de stijl van het slachtoffer.

- **Security awareness**
  Security awareness training wordt nog belangrijker dan het al is. Ook hier is het van belang om iemand te trainen om echt van nep te onderscheiden door de bron te verifiëren. Mensen moeten getraind worden om professionele cyberaanvallen te herkennen waarbij gebruikt wordt gemaakt van AI, zoals in gevallen waarbij een stem wordt nagebootst.

AI-toepassingen in de zorg

Hoewel dit hoofdstuk zich voornamelijk richt op het gebruik van AI bij cyberaanvallen, wordt AI ook steeds vaker toegepast in de zorgsector voor een breed scala aan toepassingen. Van diagnostiek tot spraakgestuurd rapporteren. Deze integratie van AI brengt risico's met zich mee op het gebied van cybersecurity en privacy. Voor meer informatie hierover, bevelen wij de volgende bronnen aan:

- Cybersecurity and privacy in AI - Medical imaging diagnosis [67] door ENISA.
- AI-systemen: ontwikkel ze veilig [68] door de AIVD.
- Guidelines for secure AI system development [69] door 22 voornamelijk nationale CERTs.

bijlage

‘De dreigingsradar geeft de tijd, de impact en de ernst weer van cyberdreigingen in de zorg.’

Toelichting dreigingsradar

De dreigingsradar is gebaseerd op het Factor Analysis of Information Risk framework (kortweg FAIR) (www.fairinstitute.org) **om dreigingen naar prioriteit te wegen. Het model is ontwikkeld in het Shared Research Programma (SRP) Cyber Security dat is gecoördineerd door TNO. Hieraan hebben ook partners als ING, ABN AMRO, Rabobank, Volksbank en Achmea deelgenomen.**

Het is verdeeld in een 3x3 matrix en geeft de tijd en impact weer van cyber-dreigingen in de zorg. De impact van een dreiging kan laag/middel/hoog zijn. De tijdlijn is verdeeld in de situatie op het moment van schrijven, de situatie die is te verwachten op korte termijn (binnen 1 jaar) of de dreigingen die in de toekomst (over meer dan 1 jaar) impact kunnen gaan hebben.

De positionering van de diverse bolletjes (met impact laag/middel/hoog) in de radarfiguur hangt samen met de weging van de dreiging in relatie tot de tijd. Is er op dit moment een bepaalde dreiging te signaleren, dan zal de dreiging met het daaraan verbonden nummer gepositioneerd worden in het radargedeelte van actuele dreigingen. Is een bepaald type dreiging op korte termijn te verwachten, binnen nu en één jaar, dan zal de betreffende dreiging worden gepositioneerd in de tweede ring. Tenslotte blikken wij ook vooruit en dreigingen die Z-CERT verwacht over meer dan 1 jaar zullen geplaatst worden in de buitenste ring.

De plaatsing van de bolletjes geeft bovendien de ernst van de dreiging aan. In de rechter taartpunt staan de ernstigste dreigingen. Hoe meer de bolletjes naar links staan, hoe lager de dreiging is die ervan uitgaat.

De impact-codering verbonden aan de dreiging is:

Kleur	Impact
	Hoog
	Medium
	Laag

De inschaling van de impact en de positie van de dreiging is gebaseerd op een rekenmodel van TNO. De geschatte tijd is gebaseerd op kennis van experts.

op dit moment

korte termijn <1 jr

lange termijn >1 jr

Bibliografie

[1] **Coveware**, Januari 2024. [Online]. Available: https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying.

[2] **Microsoft**, *"Microsoft Digital Defense Report 2023,"* 2023. [Online]. Available: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

[3] **CISA**, *"#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability,"* 7 Juni 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a. [Accessed 2023].

[4] **CISA**, *"Karakurt Data Extortion Group,"* 12 December 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-152a.

[5] **Le Soir**, *"Retour à la normale au CHU Saint-Pierre cible d'une cyberattaque,"* 11 Maart 2023. [Online]. Available: https://www.lesoir.be/500384/article/2023-03-11/retour-la-normale-au-chu-saint-pierre-cible-dune-cyberattaque.

[6] **Bleeping Computer**, *"Hospital Clínic de Barcelona severely impacted by ransomware attack,"* 7 Maart 2023. [Online]. Available: https://www.bleepingcomputer.com/news/security/hospital-cl-nic-de-barcelona-severely-impacted-by-ransomware-attack/.

[7] **KHO**, *"IT-Systemausfall nach Cyberattacke,"* 24 December 2023. [Online]. Available: https://www.kho.de/kho/index.php.

[8] **C. C. McGlave**, H. Neprash and S. Nikpay, *"Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients,"* 4 Oktober 2023.

[Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292.

[9] **Microsoft**, *"Microsoft Digital Defense Report 2023,"* 2023. [Online]. Available: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

[10] **ASD**, *"ASD Cyber Threat Report 2022-2023,"* 14 November 2023. [Online]. Available: https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023.

[11] **CVEdetails.com**, *"CVSS Scores Between 2022-01-01 and 2023-12-31,"* 2023. [Online]. Available: https://www.cvedetails.com/cvss-score-charts.php?fromform=1&vendor_id=&product_id=&startdate=2022-01-01&enddate=2023-12-31&groupbyyear=1.

[12] **CISA**, *"#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability,"* 7 Juni 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[13] **CIS**, *"CIS Critical Security Controls,"* [Online]. Available: https://www.cisecurity.org/controls.

[14] **SURF**, *"Praktijkverhaal: CIS Controls framework kan helpen om hackers buiten de deur te houden,"* [Online]. Available: https://www.surf.nl/praktijkverhaal-cis-controls-framework-kan-helpen-om-hackers-buiten-de-deur-te-houden.

[15] **NCSC**, *"Incidentresponsplan Ransomware,"* 3 juni 2022. [Online]. Available: https://www.ncsc.nl/documenten/publicaties/2022/juni/3/incidentresponsplan-ransomware.

[16] **CISA**, *"Understanding Ransomware Threat Actors: LockBit,"* 14 Juni 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a.

[17] **CISA**, *"#StopRansomware: Rhysida Ransomware,"* 15 November 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a.

[18] *"Q & A Cyberaanval (update 16 november 2023),"* Tunstall, 16 November 2023. [Online]. Available: https://www.tunstall.nl/q-a-cyberaanval-update-16-november-2023/.

[19] **Ortivus**, *"Ortivus' electronic patient record system are down for some United Kingdom based customers due to a cyber-attack,"* Juli 2023. [Online]. Available: https://www.ortivus.com/mfn_news/ortivus-electronic-patient-record-system-are-down-for-some-united-kingdom-based-customers-due-to-a-cyber-attack/.

[20] **NOS**, *"Nos.nl,"* 6 4 2023. [Online]. Available: https://nos.nl/artikel/2470392-softwarebedrijf-moet-marktonderzoeker-meer-over-datalek-vertellen. [Accessed 3 12 2023].

[21] *"Techtarget - Health IT Security,"* 17 10 2023. [Online]. Available: https://healthitsecurity.com/news/rcm-company-reports-data-breach-tied-to-moveit-software-1.9m-impacted. [Accessed 3 12 2023].

[22] *"2023 Honeypotting in the Cloud Report,"* 2023. [Online]. Available: https://orca.security/lp/2023-honeypotting-cloud-report/.

[23] **J. Fowler**, *"Millions of Highly Sensitive Patient Records Exposed in Medical Diagnostic Company Data Breach,"* 25 Oktober 2023. [Online]. Available: https://www.websiteplanet.com/news/redcliffe-breach-report/.

[24] **Adaptive Shield**, *"Kickstarting a Robust Security Program,"* 2023.

[25] **Proofpoint**, *"OiVaVoii – An Active Malicious Hybrid Cloud Campaign,"* 27 Januari 2022. [Online]. Available: https://www.proofpoint.com/us/blog/cloud-security/oivavoii-active-malicious-hybrid-cloud-threats-campaign.

[26] **Rapid7**, *"New Report: Medical Health Care Organizations Highly Vulnerable Due to Improper De-acquisition Processes,"* 2023. [Online]. Available: https://www.rapid7.com/info/medical-devices-report/.

[27] **Z-CERT**, Februari 2024. [Online]. Available: https://z-cert.nl/nieuwe-phishingtechnieken.

[28] **J. Nordenlund**, *"DarkGate Loader Malware Delivered via Microsoft Teams,"* 9 Juni 2023. [Online]. Available: https://www.truesec.com/hub/blog/darkgate-loader-delivered-via-teams.

[29] **Y. Tas**, *"Microsoft Teams Chat: the rising phishing threat and how to stop it,"* 2023. [Online]. Available: https://www.eye.security/blog/microsoft-teams-chat-the-rising-phishing-threat-and-how-to-stop-it#.

[30] **Center for Internet Security**, *"CIS Critical Security Controls (vesie 8),"* [Online]. Available: https://www.cisecurity.org/controls.

[31] **NCSC**, *"Factsheet 'Volwassen authenticeren – gebruik veilige middelen voor authenticatie,"* 25 April 2022. [Online]. Available: https://www.ncsc.nl/documenten/factsheets/2022/april/24/factsheet-volwassen-authentiseren-gebruik-veilige-middelen-voor-authenticatie.

[32] **Microsoft**, *"IT Admins - Manage external meetings and chat with people and organizations using Microsoft identities,"* 1 Juni 2023. [Online]. Available: https://learn.microsoft.com/en-us/microsoftteams/trusted-organizations-external-meetings-chat?tabs=organization-settings.

[33] **CIS**, *"CIS Controls Cloud Companion Guide (versie 8),"* 2022. [Online]. Available: https://learn.cisecurity.org/cis-controls-v8-cloud-companion-guide.

[34] **Z.-C. e. m. v. e. a. d. v. Z-CERT**, *"CSAP (Z-CERT's besloten platform voor het delen van informatie),"* 07 December 2023. [Online]. Available: https://z-cert.cyware.com/dashboard/doc-library/9e6e4eb6-e224-41b2-86f1-d7299f8850a9/.

[35] **NCSC**, *"https://www.ncsc.nl/documenten/publicaties/2023/augustus/15/risicos-in-de-toeleveringsketen,"* 2023.

[36] **C. f. I. Security**, *"CIS Benchmarks List,"* [Online]. Available: https://www.cisecurity.org/cis-benchmarks.

[37] **Z-CERT**, *"Coordinated Vulnerability Disclosure,"* [Online]. Available: https://z-cert.nl/cvd-meldingen/.

[38] **NIST**, *"Guidelines for Media Sanitization,"* 2014. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/88/r1/final.

[39] **Microsoft**, *"KillNet and affiliate hacktivist groups targeting healthcare with DDoS attacks,"* 17 Maart 2023. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2023/03/17/killnet-and-affiliate-hacktivist-groups-targeting-healthcare-with-ddos-attacks/.

[40] **ENISA**, *"ENISA THREAT LANDSCAPE FOR DoS ATTACKS,"* 10 December 2023. [Online]. Available: https://www.enisa.europa.eu/publications/

enisa-threat-landscape-for-dos-attacks/@@download/fullReport.

[41] *"SC Media,"* 26 Februari 2023. [Online]. Available: https://www.scmagazine.com/news/danish-hospitals-latest-target-of-ddos-attacks-on-nato-backed-countries.

[42] **Radware**, *"Anonymous Sudan,"* 2023. [Online]. Available: https://www.radware.com/cyberpedia/ddos-attacks/anonymous-sudan/.

[43] **Cloudflare**, *"Security & Attacks in,"* 1 Januari 2023. [Online]. Available: https://radar.cloudflare.com/security-and-attacks/nl?dateRange=52w.

[44] **The Scottish Government**, [Online]. Available: Google: *"scottish government ddos incident response"*.

[45] **NCSC**, *"Factsheet Continuïteit van online diensten,"* 2 Maart 2023. [Online]. Available: https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-continuiteit-van-onlinediensten.

[46] **NCSC**, *"Factsheet Technische maatregelen voor continuïteit voor online diensten,"* 2 Maart 2023. [Online]. Available: https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-technische-maatregelen-voor-continuiteit-van-online-diensten.

[47] **NBIP**, *"Cijfers DDoS-aanvallen in het vierde kwartaal 2021,"* 2021. [Online]. Available: https://www.nbip.nl/wp-content/uploads/2022/01/NBIP-Infographic-DDoS-data-Q4-2022-01.png.

[48] **Google**, *"Google mitigated the largest DDoS attack to date, peaking above 398 million rps,"* 10 Oktober 2023. [Online]. Available: https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps.

[49] **Akamai**, *"The Relentless Evolution of DDoS Attacks,"* 23 Juni 2022. [Online]. Available: https://www.akamai.com/blog/security/relentless-evolution-of-ddos-attacks.

[50] **Netscout**, *"NETSCOUT DDoS THREAT INTELLIGENCE REPORT / FINDINGS FROM 1ST HALF 2023,"* 2023. [Online]. Available: https://www.netscout.com/threatreport/emea/.

[51] **Kaspersky**, *"3CX attack targeted cryptocurrency companies with Gopuram malware,"* 3 April 2023. [Online]. Available: https://usa.kaspersky.com/about/press-releases/2023_3cx-attack-targeted-cryptocurrency-companies-with-gopuram-malware.

[52] **American Hospital Association**, *"HC3 TLP Clear Threat Profile: China-Based Threat Actors - August 16, 2023,"* 16 Agustus 2023. [Online]. Available: https://www.aha.org/cybersecurity-government-intelligence-reports/2023-08-16-hc3-tlp-clear-threat-profile-china-based-threat-actors-august-16-2023.

[53] **AIVD**, *"Dreigingsbeeld Statelijke Actoren (DBSA 2),"* 28 November 2022. [Online]. Available: https://www.aivd.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-dbsa-2.

[54] *"#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities,"* 9 Februari 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a.

[55] **CISA**, *"People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection,"* 24 Mei 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a.

[56] **AIVD**, *"Handleiding Kwetsbaarheidsonderzoek spionage,"* 2 Februari 2011. [Online]. Available: https://www.aivd.nl/documenten/publicaties/2011/02/17/handleiding-kwetsbaarheidsonderzoek-spionage.

[57] **Loket Kennisveiligheid**, *"Nationale leidraad kennisveiligheid - Veilig internationaal samenwerken,"* 14 Januari 2022. [Online]. Available: https://www.rijksoverheid.nl/documenten/rapporten/2022/01/14/nationale-leidraad-kennisveiligheid.

[58] **Rijksoverheid**, *"Quickscan/risicomitigatie nationale veiligheid bij inkoop en aanbesteden,"* 2019. [Online]. Available: https://www.pianoo.nl/nl/regelgeving/crisis-en-inkoop/nationale-veiligheid/quickscanrisicomitigatie-nationale-veiligheid-bij.

[59] **Gemeente Krimpen aan den IJssel**, *"Gemeente Krimpen aan den IJssel,"* 14 Maart 2023. [Online]. Available: https://krimpenaandenijssel.nl/gemeente-krimpen-aan-den-ijssel-doelwit-van-externe-fraude/.

[60] **Gemeente Alkmaar**, "*De gemeente Alkmaar getroffen door internetfraude,"* 14 September 2023. [Online]. Available: https://www.alkmaar.nl/actueel/de-gemeente-alkmaar-getroffen-door-internetfraude/.

[61] **Z-CERT**, *"Factsheet digitale financiële fraude,"* 2024. [Online]. Available: https://z-cert.nl/factsheet-financiele-fraude.

[62] **Mandiant**, *"Threat Actors are Interested in Generative AI, but Use Remains Limited,"* 19 Oktober 2023. [Online]. Available: https://www.mandiant.com/resources/blog/threat-actors-generative-ai-limited.

[63] **NCSC**, *"AI: Cruciaal moment in de geschiedenis of een hype?,"* 6 Juni 2023. [Online]. Available: https://www.ncsc.nl/actueel/weblog/weblog/2023/ai-cruciaal-moment-in-de-geschiedenis-of-een-hype. [Accessed 2023].

[64] **D. Kelley**, *"WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks,"* 13 Juli 2023. [Online]. Available: https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/.

[65] **RTL Nieuws**, *"Marion werd opgelicht met stem van zoon: 'Hij liep net op tijd de woonkamer binnen',"* 23 Mei 2023. [Online]. Available: https://www.rtlnieuws.nl/nieuws/nederland/artikel/5385957/oplichting-stem-klonen-familie-kunstmatige-intelligentie.

[66] **Microsoft**, *"Anti-spoofing protection in EOP,"* [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-protection-spoofing-about?view=o365-worldwide. [Accessed 2023].

[67] **Enisa**, *"Cybersecurity and privacy in AI - Medical imaging diagnosis,"* 7 Juni 2023. [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-and-privacy-in-ai-medical-imaging-diagnosis.

[68] **AIVD**, *"AI-systemen: ontwikkel ze veilig,"* 15 Februari 2023. [Online]. Available: https://www.aivd.nl/documenten/publicaties/2023/02/15/ai-systemen-ontwikkel-ze-veilig.

[69] **NCSC UK**, *"Guidelines for secure AI system development,"* 27 November 2023. [Online]. Available: https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development.

Dankwoord

We danken iedereen die heeft meegewerkt aan de productie van dit Cybersecurity Dreigingsbeeld voor de zorg, onder wie een aantal reviewers van zorginstellingen, CISO's van verschillende zorginstellingen en leveranciers.

We willen met name onze dank uitbrengen aan:

Nationaal Cyber Security Centrum (NCSC)
Ewald Beekman (Amsterdam UMC)
Lion van Galen (CuraMare Spijkenisse, onderdeel van de Stichting Samenwerkende Rijnmond Ziekenhuizen)
Renco van Leeuwen (WVO Zorg)
Dick van Mourik (Stichting Beweging 3.0)
Adrie Rolloos (Parnassia Groep)
Mitchell Sudmeijer (GGD-ZW)
Jos Toet (Franciscus Gasthuis & Vlietland, onderdeel van de Stichting Samenwerkende Rijnmond Ziekenhuizen)
Leon Urbanus (ASVZ)
Erick van Veghel (Catharina Ziekenhuis)
Dennis Verschuuren (Maasstad Ziekenhuis, onderdeel van de Stichting Samenwerkende Rijnmond Ziekenhuizen)

En tot slot danken we **Artiënne Buissant des Amorie** van Artgen voor de opmaak van het dreigingsbeeld.

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

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