Cybersecurity Dreigingsbeeld Zorg 2022

COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

CERT

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.

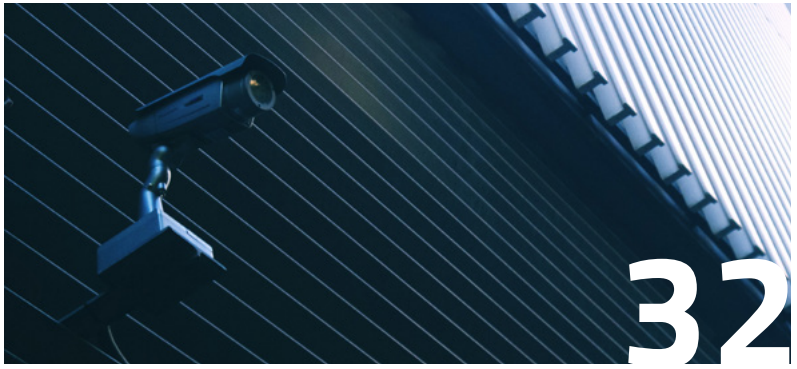
We vormen een professioneel netwerk met de bij ons aangesloten zorg-instellingen, het Nationaal Cyber Security Centrum (NCSC), Health-ISAC (Information Sharing and Analysis Center), brancheorganisaties, leveranciers en andere Computer Emergency Respons Teams (CERT's). Met elkaar pakken we cyberuitdagingen aan, zoals ransomware, phishing, datalekken en hacken.

De inhoud van dit Cybersecurity Dreigingsbeeld voor de zorg 2022 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.

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


ZA
CERT
COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

Inhoud



‘Ransomware vormt nog steeds de grootste dreiging voor zorginstellingen’

Voorwoord

Het jaar 2022 was in veel opzichten een bewogen jaar. In de zorg verlopen steeds meer processen digitaal en draaien meer systemen in de cloud. Door die groeiende digitalisering is de zorgsector vatbaarder voor verstoringen en datalekken. Uiteraard zijn er meer ontwikkelingen van invloed geweest op het dreigingsbeeld.

In deze derde editie van het Cybersecurity Dreigingsbeeld voor de zorg beschrijven we de trends en dreigingen die het afgelopen jaar de grootste impact hebben gehad op de Nederlandse zorgsector. Nieuw is dit jaar dat we de dreigingen hebben weergegeven in een dreigingsradar. Dat is een model dat is ontwikkeld door TNO en onder meer wordt gebruikt om cyber-dreigingen in de financiële sector weer te geven.

Nog steeds ransomware

Uit de feedback van onze respondenten, nieuwsberichten en uit ervaringen wereldwijd blijkt dat ransomware nog steeds de grootste dreiging vormt voor zorginstellingen. Dat is ook terug te zien op de teller die sinds oktober 2021 op de website van Z-CERT staat. Deze teller geeft aan hoeveel ransomware-incidenten binnen de zorg in Nederland en Europa bij Z-CERT bekend zijn. Met name in de landen om ons heen registreerde Z-CERT dit jaar fors meer zorggerelateerde ransomware-incidenten.

Dit wijst er op dat de hoeveelheid ransomware-incidenten dit jaar in de Europese zorg is toegenomen. Het bevestigt in ieder geval dat de zorgsector kwetsbaar is voor ransomware-incidenten. Positief is dat cybercriminelen vaak voorspelbaar zijn en geregeld bekende technieken gebruiken. Die handelswijze maakt ze gemakkelijker te detecteren. Dat is goed want vooral op het gebied van detectie kunnen zorginstellingen nog stappen maken, zo blijkt uit ons dreigingsbeeld.

Minder incidenten, meer impact

Hoewel Z-CERT in 2022 niet meer ransomware-incidenten bij Nederlandse zorginstellingen heeft geregistreerd dan het jaar daarvoor, was de impact op de totale hoeveelheid zorginstellingen wel groter dan een jaar eerder.

Sinds het voorjaar van 2022 is het opvallend dat pro-Russische hacktivisten DDoS-aanvallen uitvoeren gericht op voornamelijk de NAVO-landen en Oekraïne. Deze aanvallen zijn gericht op diverse sectoren zoals banken, luchtvaart, spoorwegen, de energiesector, logistieke bedrijven, technologie-bedrijven en overheid. Ook de zorgsector is doelwit geweest. In januari van dit jaar werden een aantal ziekenhuizen getroffen door DDoS-aanvallen. Ook Z-CERT werd doelwit van aanvallen van hacktivistische groepen.

Deze en andere trends beschrijven we uitgebreid in dit dreigingsbeeld, maar we gaan verder dan het constateren van belangrijke trends. Om u te helpen met de kennis van nu, is dit rapport voorzien van vele tips en ‘best practices’ waarmee u de beveiliging van uw zorgorganisatie naar een hoger niveau kunt tillen. Juist door kennis te delen, zijn we in staat om bij te dragen aan een veiligere digitale samenleving.

Ik wens u veel leesplezier en een digitaal veilige toekomst toe.

Wim Hafkamp
Directeur stichting Z-CERT

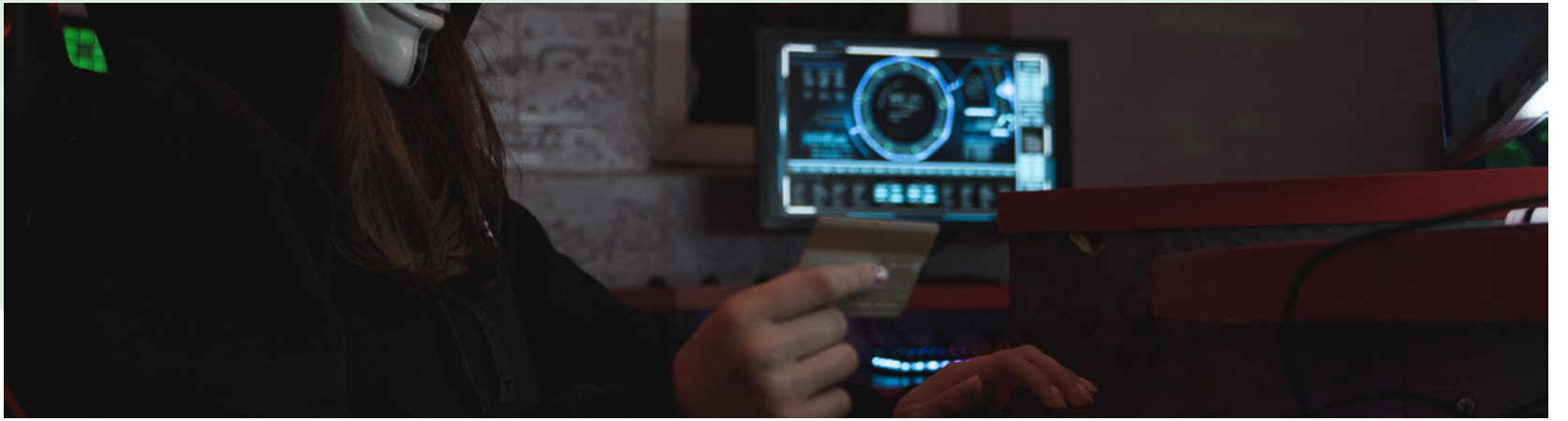
‘Belangrijk is het creëren van awareness binnen uw eigen organisatie en het prioriteren van maatregelen’

Incidenten onder respondenten

Voor het dreigingsbeeld heeft Z-CERT bij deelnemers uitgevraagd wat voor type security-incidenten zij gehad hebben. De resultaten zijn hiernaast in de grafiek weergegeven. Deze kan gebruikt worden bij het creëren van awareness binnen uw eigen organisatie en het prioriteren van maatregelen. De incidenten zullen in de hoofdstukken ‘dreigingen’ verder besproken worden en zijn onder andere gebruikt om de hoogte van de dreiging vast te stellen.

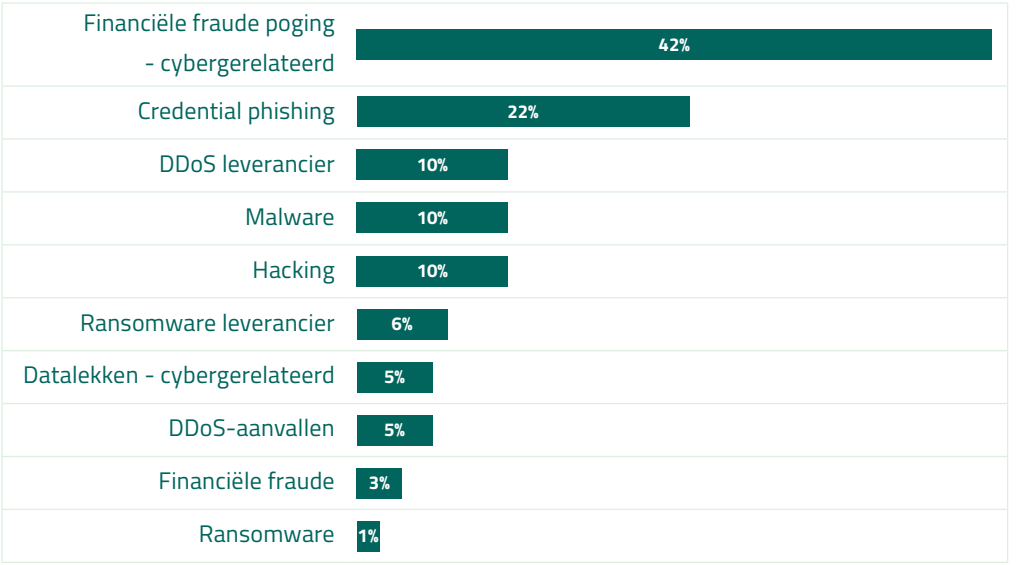
Veelvoorkomende incidenten

De respondenten van de vragenlijst van Z-CERT noemen een vrij breed spectrum van verschillende incidenten die ze tegenkomen. In de grafiek gaat het om incidenten die daadwerkelijk hebben plaatsgevonden. Echter voor financiële fraude hebben we ook de pogingen uitgevraagd, om zo de schaal van het probleem onder de aandacht te brengen. Het bleek dat 42 procent van de zorginstellingen 1 of meerdere pogingen tot financiële fraude registreerde. Dit zijn pogingen die verliepen via digitale media zoals e-mail en WhatsApp. Op de tweede plaats lijkt er onder de respondenten sprake te zijn van credential phishing (22%), gevolgd door DDoS-aanvallen bij de leverancier (10%), hacking en malware (beide 10%) en ransomware bij de leverancier (6%). Op de laatste plaats staan de cybergerelateerde datalekken (5%), DDoS-aanvallen gericht op de zorgorganisatie (5%) en de geslaagde financiële fraude (3%). Ransomware kwam bij 1 procent voor, echter de totale hoeveelheid ransomware-incidenten in de zorgsector ligt hoger.



Figuur 1

Meest voorkomende soorten security-incidenten bij ondervraagde Nederlandse zorginstellingen



Toelichting

Onder 'datalekken- cybergerelateerd' verstaan we datalekken die plaats vonden door malware, credential phishing of hacking. Bij 1 procent van de respondenten vond een ransomware-incident plaats. De werkelijke hoeveelheid ransomware-incidenten in de Nederlandse zorgsector lag echter hoger. Dit wordt verder toegelicht in het hoofdstuk over ransomware. Bij de financiële fraude categorieën in de grafiek gaat het om financiële fraude die gepleegd is door gebruik te maken van digitale media als mail en WhatsApp.

‘Z-CERT heeft gebruik gemaakt van open en gesloten bronnen, gemelde incidenten en een survey onder aangesloten zorgorganisaties’

Uitleg bij het dreigingsbeeld

Om dit dreigingsbeeld samen te stellen, heeft Z-CERT gebruik-gemaakt van open en gesloten bronnen evenals incidenten die bij Z-CERT gemeld zijn en een vragenlijst die is verstuurd naar zorgorganisaties die bij Z-CERT zijn aangesloten. Ook heeft Z-CERT interviews gehad met voornamelijk CISO’s van zorginstellingen uit verschillende subsectoren. De vragenlijst is ingevuld door deelnemers uit alle subsectoren die bij Z-CERT zijn aangesloten.

Dit dreigingsbeeld is generiek voor de zorg. Z-CERT adviseert elke zorg-instelling het dreigingsbeeld te interpreteren en door te vertalen naar de eigen situatie. Als een zorgorganisatie bijvoorbeeld vooral SaaS-applicaties afneemt, zullen de dreigingen op het gebied van leveranciers waarschijnlijk zwaarder moeten worden ingeschat. Als een zorginstelling wetenschappelijk onderzoek doet en bezig is met productontwikkeling in samenwerking met leveranciers van medische apparaten en unversiteiten, zullen statelijke dreigingen zwaarder moeten worden ingeschat. Als u cyberweerbaarheid op een hoog volwassenheidsniveau heeft gebracht, zullen veel dreigingen voor uw organisatie minder zwaar ingeschat worden als bij organisaties die hier nog veel stappen in moeten maken.

De dreigingsradar

Om zorginstellingen te helpen om dreigingen binnen hun organisatie effectief te kunnen communiceren heeft Z-CERT ervoor gekozen de dreigingen in een visualisatie weer te geven die we de "dreigingsradar" noemen. De radar wordt ook in andere sectoren gebruikt.

De dreigingsradar is tot stand gekomen door de informatie die onze deelnemers in de survey hebben ingevuld in te voeren in een model. Het model is gebaseerd op het FAIR (Factor Analysis of Information Risk) framework (https://www.fairinstitute.org) en gekoppeld aan een systeem dat een dreigingsscore uitrekent. Deze dreigingsscore wordt gebruikt om de dreigingen visueel weer te geven in de radar.

De methodiek is ontwikkeld in het Shared Research Programma (SRP) Cyber Security dat is gecoördineerd door TNO. Hieraan hebben ook ING, ABN AMRO, Rabobank, Volksbank en Achmea deelgenomen.

De radar is verdeeld in een 3x3 matrix en geeft de tijd en impact weer van cyberdreigingen 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 blikt Z-CERT ook vooruit door de dreigingen die over meer dan 1 jaar worden verwacht, in de buitenste ring te plaatsen.

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.

op dit moment

korte termijn <1 jr

lange termijn >1 jr

De impact-codering verbonden aan de dreiging is:

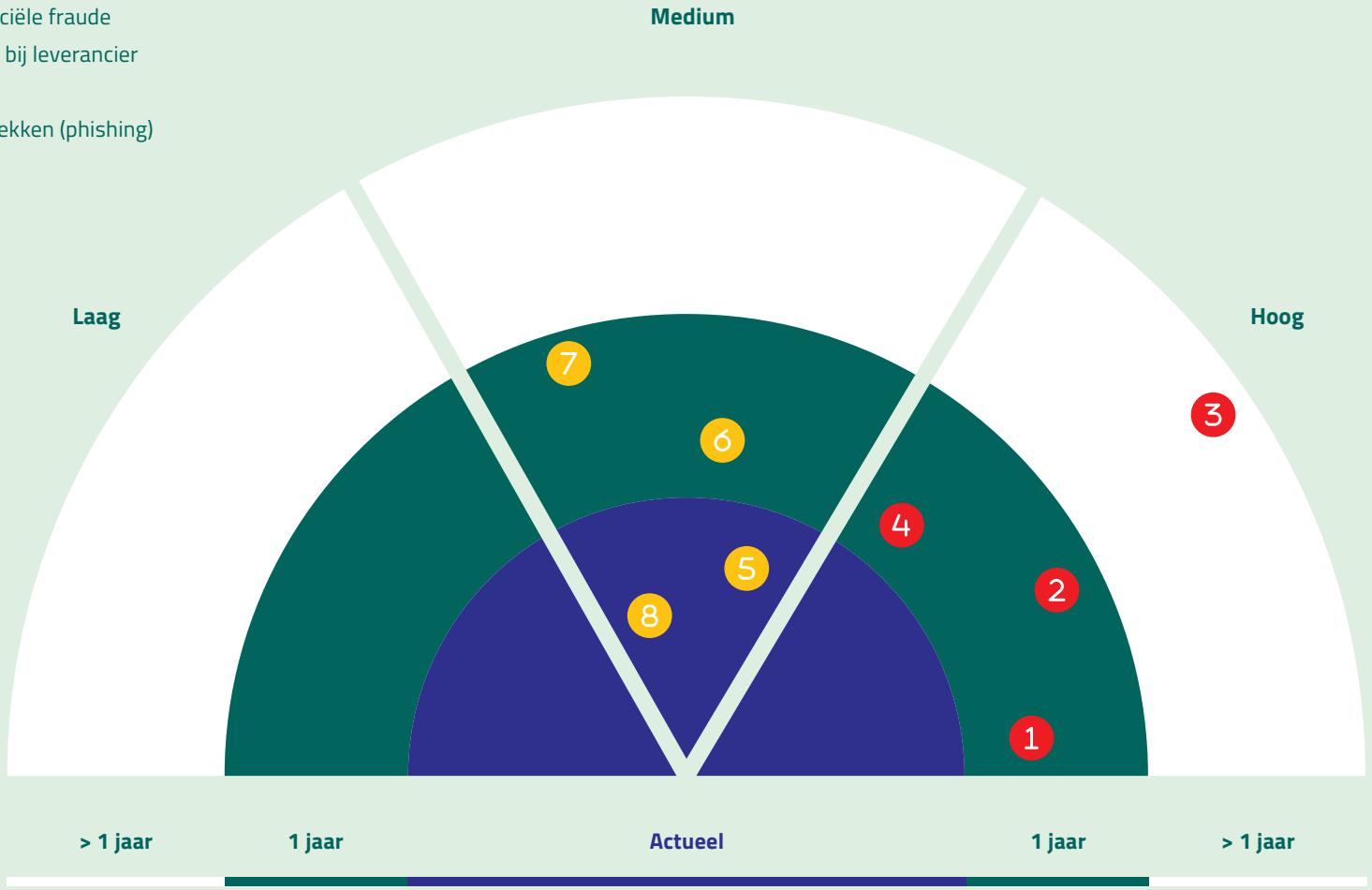
Kleur	Impact
	Hoog
	Medium
	Laag

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.

Dreigingsradar

Legenda

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



13

> **Gedeelde IT-infrastructuur kan de impact van één enkel incident flink opvoeren**

dreiging

Ransomware bij zorginstellingen

Inschatting dreiging: hoog

Z-CERT schat het dreigingsniveau voor disrupties door ransomware in als 'hoog'. In 2023 verwacht Z-CERT veel pogingen door ransomware-actoren om binnen te dringen. Z-CERT verwacht binnen een jaar enkele ransomware-incidenten in de Nederlandse zorgsector.

Incidenten

De hoge dreiging wordt onder andere zichtbaar in de hoeveelheid incidenten. Het is niet mogelijk om de werkelijke hoeveelheid incidenten in de zorgsector in Europa vast te stellen aangezien er in veel landen geen meldingsplicht is. Echter door het monitoren van datalekwebsites op het darkweb en incidenten die in de publiciteit zijn geweest, registreerde Z-CERT 65 procent meer ransomware-incidenten bij Europese zorginstellingen dan in 2021. Wereldwijd registreerde Z-CERT 28 procent meer ransomware-incidenten bij zorgorganisaties dan een jaar eerder.

In 2022 registreerde Z-CERT vijf ransomware-incidenten bij Nederlandse zorginstellingen. Dat zijn er evenveel als in het jaar daarvoor. Een verschil met 2021 is wel dat de impact op de totale hoeveelheid zorginstellingen die in Nederland overlast ondervonden, veel groter was. Dit kwam door één ransomware-incident waarbij 120 tandartspraktijken tijdelijk geen toegang hadden tot het patiëntendossier omdat hun moederbedrijf getroffen was door ransomware [1]. Gedeelde IT-infrastructuur kan de impact van één enkel incident flink opvoeren.

Keteneffecten

Een incident op een zorginstelling beperkt zich zelden tot de instelling zelf. Als ziekenhuizen bijvoorbeeld hun patiënten niet kunnen ontslaan naar een ouderenzorg instelling, of als een ambulancedienst uitvalt, heeft dat effect op de keten. Als zorg niet geleverd kan worden en er is spoed, zal dat door een andere zorginstelling vaak moeten worden opgevangen.

Voorbereidende activiteiten

De malware- en phishing-incidenten uit de incidentengrafiek aan het begin van dit dreigingsbeeld geven een beeld van voorbereidende activiteiten die voor een deel toe te schrijven zijn aan ransomware-groepen of hun partners. Het laat zien dat de dreiging van ransomware actueel is voor Nederlandse zorginstellingen.

Actoren

Z-CERT stelt vast dat er in 2022 minstens vijftien groepen actief waren die zowel de intentie als de middelen hebben om ransomware-aanvallen succesvol uit te voeren bij Europese zorginstellingen. Van drie groepen was de bedrijfsvoering dermate volwassen dat ze in staat zijn gebleken om tientallen (soms meer dan honderd) incidenten per maand te creëren.

Voor de actoren die Z-CERT dit jaar heeft gemonitord, is het motief financieel gewin. In uitzonderlijke gevallen blijkt dat als een ransomware-slachtoffer uitlegt een zorginstelling te zijn, dat de gedupeerde organisatie gratis de decryptiesleutel kan krijgen [2].

> **“Voor de actoren die Z-CERT dit jaar heeft gemonitord, is het motief financieel gewin”**

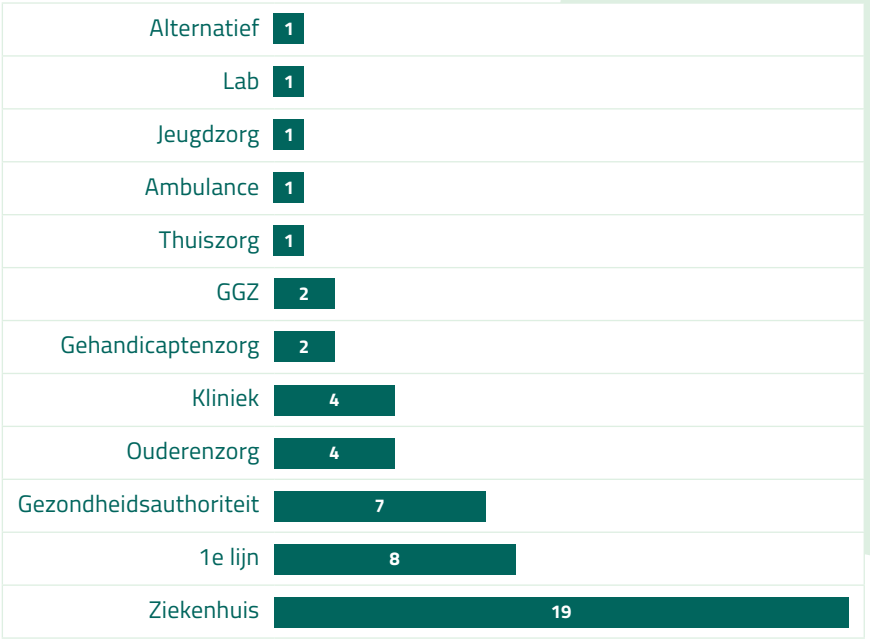
Vatbaarheid voor de dreiging

Uit onderzoek van Z-CERT blijkt dat de zorg vatbaar is voor ransomware-incidenten omdat op gebied van preventie en met name detectie de volwassenheid onvoldoende is.

Het erkennen dat de preventie verbeterd kan worden, is belangrijk zodat risico’s niet onnodig hoog oplopen. Een voorbeeld hiervan is het ontsluiten van systemen aan het internet zonder dat men in staat is snel te reageren met het patchen van kritieke kwetsbaarheden. Dit pakte in 2022 verkeerd uit toen een Nederlandse zorginstelling een mailserver niet tijdig patchte waardoor een aanvaller kon binnendringen en ransomware activeerde. Deze zorginstelling heeft zijn patchmanagement voor de mailoplossing intussen uitbesteed aan een partij die dit middels hun cloudoplossing wel kan garanderen. Het vereist een zekere nuchterheid om te onderkennen dat een organisatie de race tegen de klok met cybercriminelen niet aan kan en dat er een andere weg ingeslagen moet worden.

Maakt het type organisatie en organisatiegrootte uit?

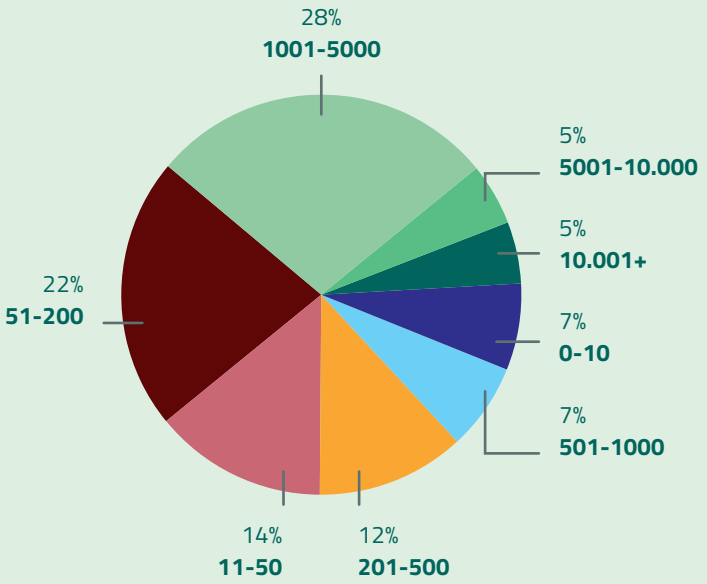
Op Europees niveau kregen vrijwel alle subsectoren te maken met ransomware-incidenten (zie bijlage figuur 1), zowel grote ziekenhuizen als kleine eerstelijns zorgpraktijken. De dreiging met ransomware is dus voor ieder type zorginstelling actueel.



Figuur 1

Hoeveelheid ransomware-incidenten in Europese zorgsector in 2022

Wat betreft grootte van de organisatie blijken ransomware-groepen niet selectief. Ook kleinere organisaties zijn interessant voor cybercriminelen. Sommige ransomware-groepen vallen liever tien kleine organisaties aan dan één grote organisatie, omdat deze vaak minder middelen hebben op security gebied en de ransomware-operator zich minder in het zicht speelt bij bijvoorbeeld inlichtingendiensten of de politiek.



Figuur 2

Percentage ransomware-incidenten per grootte van de zorginstelling (hoeveelheid personeel)

Impact

De impact kan per aanval anders zijn afhankelijk van de data waar de aanvaller toegang toe heeft gehad en het herstelvermogen van de instelling. Voor dit dreigingsbeeld hebben we een aantal feiten op een rij gezet die meer inzicht geeft over de mogelijke impact.

- In 2021 bleek uit een (internationaal) onderzoek naar ransomware bij zorginstellingen dat de kosten om te herstellen van een ransomware-incident ongeveer 1,85 miljoen dollar te zijn [3]. Daarbij is de zorg op één sector na de sector die de meeste kosten maakt om te herstellen.

- Uit hetzelfde onderzoek bleek dat het bij 44 procent van de zorgorganisaties een week duurt om volledig te herstellen. Bij een kwart duurt dat zelfs een maand [3].

- Van de 51 geobserveerde ransomware-aanvallen in de Europese zorgsector verschenen er 28 op zogenaamde datalek sites op het darkweb, waar gedreigd werd de buitgemaakte data te lekken.

Uit onderzoek naar ransomware incidenten in de zorg wereldwijd over de eerste 9 maanden van 2022 blijkt dat:

- In 50% van de gevallen waar het geregistreerd is, moesten patiënten uitwijken naar andere zorginstellingen.
- In iets meer dan de helft van de gevallen waar het bekend is, moesten afspraken afgezegd of verplaatst worden.
- In 93% van de gevallen waar het bekend is, was het resultaat dat IT-systemen niet beschikbaar waren.

Methoden

Een dreiging is pas effectief als uw organisatie vatbaar is voor de technieken die door de aanvaller gebruikt worden. Wat dat betreft is er goed nieuws. Alhoewel de groepen professioneler en dus effectiever zijn geworden, zijn de technieken die ransomware-groepen gebruiken de afgelopen jaren redelijk constant gebleven. Dat wil zeggen dat ze vaak misbruik maken van veelal dezelfde zwakheden en misconfiguraties [4].

De meest gebruikte technieken [5] [6] om een organisatie binnen te komen:

- Mail met malware (links naar malware of malafide bijlagen).
- Toegang tot thuiswerkoplossingen met gestolen of gelekte wachtwoorden, met name via RDP maar ook bijvoorbeeld de Citrix thuiswerkoplossing en VPN-oplossingen.
- Misbruik van kwetsbaarheden.

In 2022 waren met name kwetsbaarheden in firewall-oplossingen, de mailoplossing van Microsoft (Microsoft Exchange), online portalen en Log4j populair. Wat Z-CERT opviel, is dat ransomware-actoren ook kwetsbaarheden misbruikten in firewall-producten die gebruikt worden door kleine organisaties. In publieke nieuwsmedia werden deze niet genoemd.

Aanbevelingen

Het is belangrijk om de initiële toegang van een ransomware-actor zo moeilijk mogelijk te maken. Onder andere omdat in de praktijk blijkt dat het voor zorgorganisaties makkelijker is om hackers in deze fase van de aanval tegen te houden, dan wanneer hackers al het netwerk zijn binnengedrongen.

Ook zijn de maatregelen om initiële toegang te voorkomen vaak kosteloos in de aanschaf omdat het gaat om het gebruik van een functionaliteit die reeds aanwezig is in Windows.

Voor het voorkomen van de initiële toegang adviseert Z-CERT u prioriteit te geven aan het volgende:

- **Applicatie allowlisting**
  Hierbij wordt een oplossing zoals AppLocker gebruikt om te voorkomen dat programma's die niet goedgekeurd zijn door de organisatie, opgestart kunnen worden. Dit wordt gedaan door regels te definiëren. Bijvoorbeeld: alleen applicaties mogen opgestart worden die in "program files" staan. Op deze manier is het mogelijk middels simpele regels zelfs geavanceerde malware te blokkeren die nog niet herkend wordt door de antivirus-oplossing. Online zijn goede handleidingen beschikbaar om dit effectief in te richten [7].

- **Microsoft Office beveiligen tegen misbruik**
  Microsoft Office wordt zeer veel gebruikt en hackers gebruiken daarom graag kwaadaardige office-bestanden om organisaties binnen te dringen. Het is daarom belangrijk om Office zoveel mogelijk te beveiligen tegen dit soort aanvallen. Z-CERT raadt u daarom het volgende aan:

  - Faseer het gebruik van macro's uit. Als dit (nog) niet kan reguleer het gebruik van macro's dan (zie: [8]). Vaak zijn security specialisten bang dat het uitschakelen of managen van macro's tot veel klachten zal leiden. Zorgorganisaties hebben successen geboekt door dit gefaseerd in te voeren.

- Schakel "Attack surface reduction rules" in die betrekking hebben op Office. Uit de praktijk blijkt dat deze regelmatig in staat zijn om nieuwe aanvallen via Office-documenten tegen te kunnen houden.
- Gebruik de configuratie opties in Office die beschikbaar zijn en helpen tegen allerlei typen misbruik (zie [9]).

- Steeds vaker wordt malware aangeboden verpakt in een **cd-image bestand**. Dit wordt onder andere gedaan om de strengere regels van Microsoft wat betreft het opstarten van macro's te omzeilen. De mogelijkheid om de inhoud van deze bestanden te bekijken, kan uitgeschakeld worden [10]. Echter ook applicatie allowlisting kan ingezet worden om uitvoeren van malware vanaf deze cd-image bestanden te voorkomen.

- **Gebruik multifactorauthenticatie** voor alle services die toegang geven tot het netwerk en voor accounts met hoge rechten.

- **Geef prioriteit aan het patchen van systemen en software die ontsloten zijn aan het internet.** Maak een reële afweging of uw IT-afdeling de druk aan kan en kies anders voor een cloudoplossing, uitbreiding IT-afdeling, uitbesteding of uitfasering.

- **Geef prioriteit aan het patchen van veel gebruikte desktopsoftware** als webbrowsers, Microsoft Office en PDF-readers.

- **Indien u patchen heeft uitbesteed, voer regie uit op uw leverancier en stuur bij indien risicotoleranties overschreden worden.** Dit laatste is echt nodig, aangezien Z-CERT vele voorbeelden heeft van leveranciers die te laat zijn met patchen. De regievoering kan pas effectief uitgevoerd worden als er afspraken zijn gemaakt met de leverancier over patchen. Bijvoorbeeld dat kwetsbaarheden in een firewall-oplossing die als kritiek zijn ingeschaald en vanaf het internet te misbruiken zijn, binnen de afgesproken tijd gepatcht moeten worden.

Beschermen data

Voor de bescherming van data is het belangrijk een offline of immutable back-up van uw belangrijke data te hebben. Immutable back-ups zijn back-ups die niet veranderbaar zijn en dus ook niet door een ransomware-actor versleuteld kunnen worden. Niet elke offsite back-up is goed beschermd tegen ransomware omdat aanvallers in een volledig gecompromitteerde omgeving vaak ook toegang hebben tot de offsite back-up.

Meer literatuur

Voor meer literatuur over ransomware en wat u er tegen kunt doen, verwijst Z-CERT naar onze website waar we ingaan op de detectie van aanvallers in het netwerk [11] en een top 10 van de meest nuttige maatregelen [12]. Voor meer adviezen over incident response en preventie, verwijst Z-CERT naar de whitepaper *"Incidentresponsplan Ransomware"* van het NCSC [13].

dreiging

Ransomware in de leveranciersketen

Inschatting dreiging: hoog

Z-CERT schat het dreigingsniveau voor disrupties door ransomware in de leveranciersketen van zorginstellingen in als 'hoog'. Leveranciers van zorginstellingen worden vaker geraakt dan zorgorganisaties zelf. Het komend jaar verwacht Z-CERT een aantal ransomware-incidenten in de leveranciersketen die impact zullen hebben op Nederlandse zorginstellingen.

Naast de zorgsector hebben ook andere sectoren last van ransomware-incidenten. Uit onderzoek van Z-CERT blijkt dat in Europa bijvoorbeeld bij de bouw, bij IT-dienstverleners en de overheid waarschijnlijk meer ransomware-incidenten plaatsvonden dan in de zorg. In 2022 werd dit zichtbaar doordat er geregeld incidenten in de leveranciersketen plaatsvonden met impact op zorginstellingen (zie tabel 1). In 2022 werden er minder incidenten bij Z-CERT gemeld dan in 2021 en in de meeste gevallen viel de impact mee. Eén keer leidde een incident tot disrupties van belangrijke processen (zie tabel 1).

Z-CERT registreerde twaalf incidenten in de Europese farmaceutische industrie en zeven bij bedrijven die medische apparaten of andere medische producten maken. Dat is ongeveer vergelijkbaar met het jaar daarvoor. Ransomware-incidenten bij leveranciers van medische apparaten of IT-dienstverleners kunnen riskant zijn omdat zij soms ook toegang hebben tot de netwerken en systemen van zorginstellingen. Tabel 1 laat zien wat de impact was op Nederlandse zorginstellingen die in 2022 geraakt werden door ransomware via een leverancier.

Tabel 1

Impact op Nederlandse zorginstellingen door ransomware-aanvallen op leveranciers van zorginstellingen in 2022

Product/dienst geraakte bedrijf	Impact zorginstelling
Apothekerssoftware	Uitstel onderhoud
Crediteuren/facturatie	Enkele dagen niet factureren
Websitehosting	Website enkele uren niet online
Authenticatieoplossing	Datalek
Diagnostiek	Uitstel onderhoud
Vastgoed	Datalek
Eerstelijnszorg-automatisering	Bedrijf niet bereikbaar

Gespecialiseerde producten
Sommige bedrijven leveren gespecialiseerde producten, zoals dialyse-vloeistof en zuurstof. Indien deze leverancier lange tijd niet kan leveren door een ransomware-incident, kan het voor zorginstellingen spannend worden. Het is daarom rondom leveranciersmanagement belangrijk om niet alleen aandacht te besteden aan bedrijven die digitale diensten leveren, maar ook bedrijven die producten leveren die niet makkelijk te vervangen zijn door alternatieven.

Ransomware-incidenten bij zorginstellingen door misbruik van leverancier accounts
In sommige gevallen vinden ransomware-incidenten plaats bij organisaties doordat een ransomware-actor meelift op de toegang die een leverancier heeft tot het netwerk van zijn klanten. Een aantal voorbeelden daarvan die Z-CERT afgelopen twee jaar tegenkwam:

- Een leverancier heeft een 'open verbinding' met een zorginstelling. Een aanvaller kan via de VPN-verbinding een fileserver van een zorginstelling bereiken en deze d.m.v. ransomware versleutelen.

- Bij een grote Europese producent komt de ransomware-actor het netwerk binnen via een leverancier. Deze leverancier heeft hoge rechten en veel bewegingsruimte in het netwerk, waardoor de hacker een groot deel van de IT-infrastructuur op slot kan zetten door ransomware te activeren.

- Een gemeente wordt slachtoffer van een groot ransomware-incident mede omdat multifactorauthenticatie ontbreekt op een gecompromit-teerd leveranciersaccount [14].

Aanbevelingen
Leveranciers zouden 'ransomware-resistent' moeten zijn en aanbevelingen volgen zoals Z-CERT die gedefinieerd heeft in hoofdstuk ransomware en de bronnen waar we naar verwijzen.

Wat betreft leveranciers die toegang hebben tot uw netwerk, zijn uit de hierboven beschreven incidenten een aantal lessen te trekken.

- Een gedegen privilege access managementoplossing en -proces is noodzakelijk indien u leveranciers toegang geeft tot uw netwerk. Bij een dergelijke oplossing kan een leverancier toegang aanvragen en krijgt hij alleen die toegang die nodig is en zo lang als het nodig is. Daarnaast worden de activiteiten gelogd.

  Uit ervaringen van zorginstellingen blijkt dat zij positieve resultaten hebben geboekt bij het migreren van hun leveranciers naar privilege access managementoplossingen. Dus indien uw organisatie nog niet op deze wijze werkt, is hier winst te boeken.

- Een aanvaller die via de leverancier binnenkomt moet niet in staat zijn om het netwerk verder te infiltreren. Z-CERT constateert dat er wel vaak netwerksegmentering aanwezig is, maar deze niet altijd zo is ingericht om een aanvaller tegen te houden.

- Leveranciersaccounts moeten niet gevrijwaard worden van multifactor-authenticatie.

dreiging

DDoS

Inschatting dreiging: medium

Z-CERT schat het dreigingsniveau voor DDoS-aanvallen op zorginstellingen in op 'medium' en verwacht binnen een jaar enkele DDoS-incidenten met weinig impact. Dit kan echter snel omslaan door de ontwikkelingen binnen het conflict tussen Rusland, Oekraïne en bondgenoten.

Incidenten

In 2022 werden bij Z-CERT drie incidenten gemeld die direct gericht leken op zorginstellingen. De DDoS-aanvallen hadden weinig impact. Er werden firewalls overbelast en er was tijdelijk geen toegang tot de webmail. Bij één zorginstelling was er geen internetverkeer mogelijk en bij een andere was de thuiswerkplek tijdelijk niet beschikbaar.

In vergelijking met andere sectoren heeft de zorgsector relatief weinig last van gerichte DDoS-aanvallen [15]. Wat is daarvoor de verklaring? Veel DDoS-aanvallen worden uitgevoerd door cybercriminelen met financieel gewin als motief. Voor een bedrijf dat diensten of producten via het internet aanbiedt, is de financiële impact van een DDoS-aanval mogelijk groot, maar voor zorgorganisaties is die impact vaak minder. Ze zijn daardoor een minder aantrekkelijk doelwit [16].

Een ander motief voor een DDoS-aanval kan 'wraak' zijn door een ontevreden cliënt, patiënt of (ex) medewerker. Een jeugdzorginstelling meldde aan Z-CERT een voorbeeld van een aanval die mogelijk geïnitieerd werd door een ontevreden client. Er zijn nauwelijks technische drempels om een DDoS aanval uit te voeren: iedereen kan op internet een DDoS-aanval kopen. Zeker als een website geen mitigerende maatregelen heeft, is een aanval goedkoop, zo'n 50 dollar voor een aanval van 24 uur [17]. Het gaat hier om relatief eenvoudige aanvallen waarbij de website een grote hoeveelheid verzoeken krijgt. De professionelere aanvallen waarbij zeer grote hoeveelheden dataverkeer verstuurd worden en waarbij mitigerende maatregelen op de proef gesteld worden, zijn veel duurder. Dit loopt in de duizenden euro's [18]. Dit soort aanvallen zullen minder snel voorkomen, omdat budget hier wel een barrière is.

Wat betreft DDoS kwam de grootste dreiging voor de zorgsector dit jaar vanuit pro-Russische hacktivisten. In het voorjaar 2022 begonnen zij met het uitvoeren van DDoS-aanvallen gericht op voornamelijk de NAVO-landen en Oekraïne. Vooral banken, luchtvaart, spoorwegen, de energiesector, logistieke bedrijven, technologiebedrijven en overheid waren doelwit.

Z-CERT constateerde dat er binnen deze hackersgroepen ook zorginstellingen en zorg gerelateerde organisaties als doelwit genoemd werden [19] [20]. Een ziekenhuis uit Oost-Europa bevestigde tegenover Z-CERT

dat er een DDoS-aanval werd uitgevoerd. Die aanval werd afgeslagen. Daarnaast werden er in september 2022 bedreigingen geuit naar acht ziekenhuizen uit het Verenigd Koninkrijk [19].

Onze analyse is dat de doelwitselectie vrij willekeurig lijkt. Aanvallen vinden vaak plaats als landen negatief in het nieuws komen in Rusland. Op het moment dat Nederland negatief zou opvallen in Russische media, is de kans aanwezig dat er DDoS-aanvallen worden uitgevoerd die ook gericht zijn op zorginstellingen. Daarnaast kunnen zorginstellingen overlast ervaren als IT-dienstverleners waar zij gebruik van maken, worden aangevallen.

> **“Het beeld bestaat dat de DDoS-aanvallen niet bijzonder krachtig zijn”**

Technieken

Wat betreft de pro-Russische hacktivistische groepen kan het niveau van de aanvallen en de gebruikte methoden verschillen, afhankelijk van de diensten of tools die gebruikt worden. Over het algemeen bestaat het beeld dat de aanvallen niet bijzonder krachtig zijn [21] en kunnen de aanvallen met de juiste middelen gemitigeerd worden. Gemiddeld hebben de aanvallen op de netwerklaag een volume tussen de 40-100 Gbps met een duur van één tot twee dagen [22]. Ook zijn er aanvallen op applicatieniveau waargenomen waarbij websites het doelwit waren [25]. Dit soort aanvallen vergen andere mitigerende maatregelen [26].

Voor meer technische details over de aanvallen die gezien worden vanuit pro-Russische hacktivistische groepen, verwijst Z-CERT naar de analyse van het nationale CERT van Italië [27] (vertaling: [24]).

Aanbevelingen

- Voor aanbevelingen op zowel organisatorisch en technisch niveau verwijst Z-CERT graag naar de volgende factsheets van het NCSC.
  - Factsheet Continuïteit van online diensten [28].
  - Factsheet Technische maatregelen voor continuïteit voor online diensten [26].

- Voor een voorbeeld van een basaal DDoS response-plan verwijst Z-CERT graag naar een voorbeeld van het NCSC UK [29].

dreiging

DDoS-aanvallen op leveranciers

Inschatting dreiging: medium

Z-CERT schat het dreigingsniveau voor DDoS-aanvallen op leveranciers in op 'medium' en verwacht binnen een jaar enkele incidenten met impact op zorginstellingen. Het dreigingsniveau kan echter snel stijgen als gevolg van geopolitieke ontwikkelingen binnen het conflict tussen Rusland en Oekraïne.

Incidenten en impact
Van de ondervraagde zorginstellingen heeft 9 procent overlast ervaren door DDoS-aanvallen die zijn uitgevoerd op leveranciers. Dit aantal is bijna de helft minder dan in 2021. De afgelopen jaren hebben zorginstellingen overlast ervaren van DDoS-aanvallen op de volgende typen leveranciers:

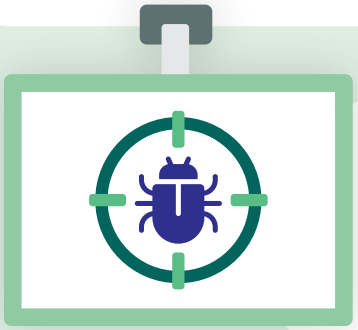
1. Authenticatieproviders
Patiënten of cliënten kunnen niet inloggen in de voor hen bestemde portalen omdat de vooraf benodigde authenticatie niet werkt. Bij sommige zorginstellingen kunnen patiënten daardoor niet bij de benodigde link voor het beeldbellen.

2. DNS-providers
Twee DNS-providers werden in 2022 geraakt door een DDoS-aanval. Voor een zorginstelling betekent dit dat diensten niet meer via hun domeinnaam te benaderen zijn. In de praktijk gaat het vaak om de website van de zorgorganisatie, het patiënten- of cliëntenportaal of de thuiswerkplek.

3. Leveranciers die webapplicaties hosten in de cloud (SaaS-leveranciers)
Steeds meer zorginstellingen nemen webapplicaties af in de cloud. HR-systemen, planning rond de zorgverlening, ERP-systeem en het elektronisch patiënten- of cliëntendossier. In twee gevallen was in de afgelopen twee jaar een elektronisch cliëntendossier een aantal uur niet beschikbaar door een DDoS-aanval op de leverancier.

4. Internet service providers (ISP's)
Aanvallen op dit type leveranciers heeft niet alleen consequentie voor de internetverbinding van een zorginstelling. Ook kunnen de effecten indirect zijn als bijvoorbeeld een internet service provider van een SaaS-leverancier wordt aangevallen.

24



Tabel 1

Type leveranciers van Nederlandse zorginstellingen die in 2022 een DDoS-aanval te verwerken kregen

Type organisatie	Impact
IT-provider	Tijdelijke traagheid van de systemen van de zorgorganisatie
Elektronisch cliënten portaal	Enkele uren applicatie niet bereikbaar
Internetprovider	Geen internet
DNS provider	Websites niet bereikbaar, patiëntenportaal niet bereikbaar
Authenticatieprovider	Ziekenhuisportaal niet beschikbaar, beeldbellen met patiënt niet mogelijk, niet mogelijk om in te loggen op website
SaaS-applicatie	Applicatie offline

Trends en technieken

In het kader van leveranciersmanagement is het goed om te weten welke sectoren vaak doelwit zijn van DDoS-aanvallen. Uit internationale dreigingsrapporten blijkt dat bepaalde sectoren een hoger risico lopen om slachtoffer te worden van DDoS-aanvallen op netwerkniveau. Voor de zorg relevante sectoren waar dit vaak voortkomt, zijn onder meer telecom- en IT-dienstverleners, webhostingbedrijven en dataverwerkingsdiensten [30] [31].

Voor Nederland heeft Z-CERT geen uitgebreid overzicht met DDoS-statistieken voor elke sector, echter wel voor ISP's. Daar waar Z-CERT slechts vier meldingen kreeg over gerichte DDoS-aanvallen voor de zorg, registreerde de Nationale Beheersorganisatie Internet Providers (NBIP) er 2001 [32]. Dit waren er wel minder dan het jaar daarvoor, maar meer dan in 2020. Het laat zien dat de kans dat bepaalde typen leveranciers van zorginstellingen worden aangevallen vele malen groter is dan dat de zorginstelling zelf direct aangevallen wordt.

Er is geen totaaloverzicht van de hoeveelheid DDoS-aanvallen wereldwijd. De meeste bronnen melden een toename van DDoS-aanvallen in 2022 ten opzichte van 2021 [33] [35]. Wat anders is dan in 2021, is dat er in 2022 ook veel meer DDoS-incidenten plaatsvonden die veroorzaakt zijn door pro-Russische en pro-Oekraïense hacktivisten. Dit maakt vergelijken met het jaar ervoor lastiger. Uit een analyse van dreigingsrapporten van Cloudflare lijkt het aantal meldingen van DDoS-aanvallen waarbij cybercriminelen geld eisen, redelijk stabiel te zijn gebleven ten opzichte van 2021 [34]. De hoeveelheid gerapporteerde aanvallen waarbij geld werd geëist door cybercriminelen, nam in 2022 elk kwartaal toe [34].

Wat betreft de trends in technieken zijn hier uitgebreide verslagen voor beschikbaar die u eventueel aan uw leverancier kunt voorleggen [31] [34]. Een opvallende trend in het gebruik van aanvalstechnieken lijkt te zijn dat DDoS-aanvallen langer en krachtiger worden. NBIP geeft aan dat er een trend is waarbij meervoudige aanvalsmethodes gebruikt worden [36].

Gerichte DDoS-aanvallen op Nederland door pro-Russische hacktivisten heeft Z-CERT in 2022 niet gezien. Zoals is besproken in het vorige hoofdstuk, kan dit snel veranderen gelet op het conflict tussen Oekraïne en Rusland. Ook zijn in het verleden IT-dienstverleners aangevallen [20].

Aanbevelingen

- Beoordeel de weerbaarheid van externe leveranciers tegen verschillende typen DDoS-aanvallen. Zie voor vragen die u kunt stellen aan uw leverancier bijvoorbeeld de factsheet “Continuïteit van online diensten” van het NCSC [28].
- Leg afspraken over DDoS-mitigatie vast in een Service Level Agreement.
- Betrek DDoS-aanval scenario’s in uw business continuity plan.
- Stel vast voor welke diensten het raadzaam is om deze bij meerdere leveranciers af te nemen. Als uw internetverbinding bijvoorbeeld belangrijk is voor kritieke processen, kan het raadzaam zijn om een back-up internetverbinding te hebben.
- Sommige diensten kunt u optimaliseren tegen DDoS-aanvallen. Zie voor DNS bijvoorbeeld het artikel van SIDN genaamd “TTL-waarden voor DNS-records kiezen: hoe doe je dat?” [37].

“ Een opvallende trend in het gebruik van aanvalstechnieken lijkt te zijn dat DDoS-aanvallen langer en krachtiger worden ”

dreiging

Datalekken door malware, credential phishing of hacking

Inschatting dreiging: medium tot hoog

Z-CERT schat het dreigingsniveau voor datalekken in de zorg die veroorzaakt worden door malware en credential phishing in als 'medium' en actueel. Dit betekent dat er op korte termijn incidenten in deze categorie worden verwacht waarbij sprake is van een datalek. Z-CERT schat het dreigingsniveau voor datalekken in de zorg in 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 vaak hoger zijn dan bij een phishing-incident omdat er meer gevoelige data buitgemaakt wordt.

Er zijn verschillende manieren waarop datalekken plaatsvinden. In dit dreigingsbeeld zoomt Z-CERT in op de datalekken die plaatsvonden door de cyberincidenten: credential phishing, malware of hacking.

Incidenten

Het aantal datalekken dat via de uitgezette survey bij ons is gemeld en het gevolg was van credential phishing, malware of hacking, bleef beperkt. Slechts 5 procent van de respondenten meldde een datalek. Dit is relatief laag. Het lage percentage is te verklaren doordat veel zorginstellingen multifactorauthenticatie toepassen. Dit blijkt uit het feit dat 22 procent van de ondervraagde instellingen een incident meldde waarbij kwaadwillenden het wachtwoord of andere informatie wisten te stelen, maar waarbij het incident niet altijd leidde tot een datalek. Voorbereidende activiteiten die zouden kunnen leiden tot datalekken werden door de helft van de ondervraagde zorginstellingen gedetecteerd.

Daarnaast vermoedt Z-CERT dat niet elk datalek daadwerkelijk gedetecteerd wordt. Een succesvolle malware-infectie bijvoorbeeld, wordt niet door iedere IT-helpdesk geassocieerd met datalekken, waardoor niet altijd onderzocht wordt of er data gestolen is. Het stelen van de inhoud van e-mails is een basisfunctionaliteit van veel gebruikte malware [38]. Daarnaast moet er ook kennis en logging aanwezig zijn om een datalek te kunnen vaststellen.

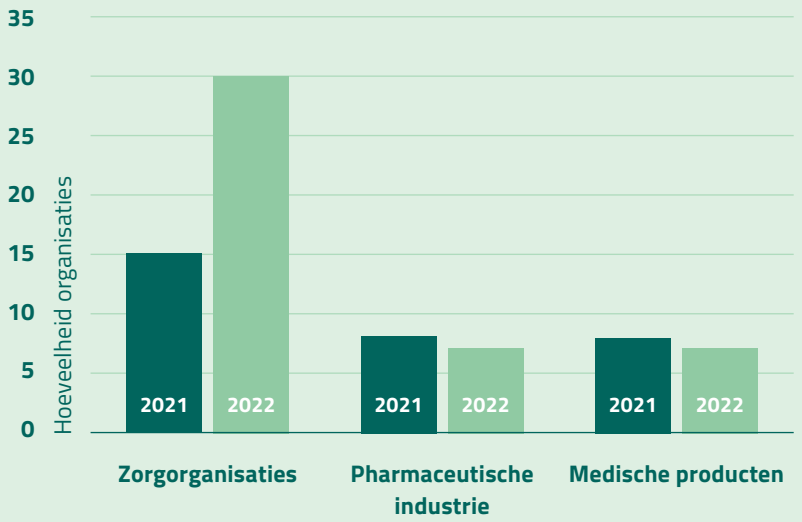
Afpersen door te dreigen met het lekken van data

Een grote zorg voor securityprofessionals zijn de groepen cybercriminelen die data stelen om organisaties af te persen. Ze dreigen met het lekken van gevoelige data als het slachtoffer niet tot betaling overgaat. Dit gaat vaak hand in hand met ransomware, maar niet altijd. Ook zijn er enkele groepen actief die ransomware geheel achterwege laten en alleen dreigen met het lekken van data.

28

Figuur 5

Hoeveelheid Europese organisaties die in 2022 op datalekwebsites verschenen



Zoals figuur 5 laat zien, leek de hoeveelheid incidenten bij Europese zorginstellingen toe te nemen, maar bleven deze voor de farmaceutische industrie en producenten van medische producten, redelijk constant. Ook van Nederlandse zorginstellingen is bij dit soort incidenten data gelekt.

Datalekken bij leveranciers en partners

Een bron van datalekken die niet bij de zorginstelling zelf plaatsvindt, zijn gehackte mailboxen van partners, leveranciers of collega-zorginstellingen. Indien een mailbox van zo'n relatie gehackt wordt, wordt vaak de mail gestolen. De inhoud van deze mail wordt door de cybercrimineel vervolgens gebruikt om phishingmail te sturen. Omdat er vertrouwde content in de phishingmail staat is de ontvanger eerder geneigd om op de malafide links te klikken of om de bijgevoegde malware op te starten.

Er werden bij Z-CERT maandelijks campagnes gemeld waarbij er malafide mails gestuurd werden naar soms tientallen zorginstellingen. Organisaties die nog steeds geen multifactorauthenticatie vereisen op hun mailtoegang, verhogen daarbij het risico op security-incidenten in de zorg. Volgens Z-CERT zouden dergelijke organisaties daarop geattendeerd moeten worden.

> **“Organisaties die nog geen multifactor-authenticatie vereisen voor toegang tot hun webmail, moeten hierop aangesproken worden”**

Dit type datalekken is er vaak niet op gericht om organisaties af te persen. Ze worden veroorzaakt door cybercriminelen die toegang tot systemen of gebruikersnamen en wachtwoorden verkrijgen, om die gegevens vervolgens te verkopen op het darkweb.

Script kiddies

Naast de cybercriminelen zijn er ook hackers die vallen in de categorie 'script kiddies'. Dit zijn vaak jonge mensen die het spannend vinden om te hacken. Dit liep in 2022 aardig uit de hand toen een 19-jarige jongen een kwetsbaarheid in een systeem van een digitaal zorgplatform [39] misbruikte en volgens nieuwsmedia toegang kreeg tot de gevoelige data van twintig zorginstellingen [40].

Script kiddies klinkt als term 'denigrerend', en kan daarom door sommige als een kleiner risico worden gezien, echter het niveau kan per individu erg variëren. Vaak opereren ze niet als een georganiseerd bedrijf zoals bij ransomware-operators, maar zijn het hobbyisten. De gevolgen van hun daden voor hun slachtoffers overzien ze doorgaans niet. En ze beseffen niet altijd dat ze strafbare feiten plegen.

Technieken en trends

Internationaal onderzoek laat zien dat datalekken in de zorg steeds vaker optreden door aanvallen op webapplicaties [15]. Dit zijn meestal basale aanvallen. De aanvaller gebruikt bijvoorbeeld gestolen wachtwoorden of misbruikt bekende kwetsbaarheden of misconfiguraties. Doordat zorgorganisaties steeds vaker hun webapplicaties afnemen in de cloud, is dit een aandachtspunt voor de zorg.

Hoe stelen deze actoren wachtwoorden? Natuurlijk zijn daar de standaardmethoden, zoals het uitproberen van wachtwoorden die bij datalekken van websites zijn uitgelekt (zoals het datalek bij Dropbox en LinkedIn). Echter niet iedereen weet dat veel van deze gestolen wachtwoorden zijn gestolen met behulp van malware. Uit onderzoek is in 2022 gebleken dat binnen zeven maanden 675.000 wachtwoorden gestolen werden van Nederlandse computers door gebruik te maken van malware [41].

De combinatie van slechte beveiliging tegen malware en het ontbreken van multifactorauthenticatie voor webapplicaties is een serieus risico. Daarnaast kan malware ook meeliften op bestaande sessies uit webbrowser door bepaalde cookies te stelen. Dit kan in sommige gevallen er zelfs toe leiden dat een cybercrimineel tijdelijk toegang krijgt tot een webapplicatie, zelfs al is multifactorauthenticatie ingeschakeld [42]. Een recent voorbeeld hiervan is de hack op een softwareontwikkelingsplatform, waarbij de hacker op deze manier toegang kreeg tot het platform ondanks het feit dat multifactorauthenticatie was ingeschakeld [43].

> **“De combinatie van slechte beveiliging tegen malware en het ontbreken van multifactorauthenticatie voor webapplicaties is een serieus risico”**

Multifactorauthenticatie

Multifactorauthenticatie werkt ontzettend goed tegen de meeste aanvallen waarbij er ingelogd moet worden met een gebruikersnaam en wachtwoord. Wel verschenen er dit jaar voorbeelden in de pers waarbij hackers erin slaagde traditionele multifactorauthenticatie methoden te omzeilen [44] [45]. Z-CERT heeft dit soort aanvallen in de Nederlandse zorgsector nog niet vastgesteld. Wel is het goed om op dit vlak de ontwikkelingen in de gaten te houden.

API's

Wat bij Z-CERT steeds vaker gemeld wordt zijn kwetsbaarheden en mis-configuraties in API's (application programming interface). Software zoals webapplicaties en mobiele apps communiceren met elkaar via deze API's. Als deze niet goed geconfigureerd zijn kan dit leiden tot datalekken.
In december 2022 kon een ethisch hacker via een slecht geconfigureerde API toegang kon krijgen tot meer dan 15.000 gebruikersnamen en andere gegevens van huisartsen [46]. Ook werden er bij Z-CERT incidenten gemeld waarbij er ook toegang verkregen kon worden tot patiënten data.

Aanbevelingen

- Wat betreft leveranciers van webapplicaties (SaaS leveranciers) raadt Z-CERT aan om softwareleveranciers van webapplicaties zorgvuldig te selecteren en met name leveranciers te selecteren die een gedegen Security Development Lifecycle (SDL) hebben. Als onderdeel van deze levenscyclus worden er onder andere pentests uitgevoerd en gebruikt een leverancier richtlijnen voor de veilige ontwikkeling van software. Bijvoorbeeld de richtlijn die het Nationaal Cyber Security Centrum (NCSC) heeft opgesteld [47].
  Een bekend model voor een SDL dat u kunt gebruiken, is het model dat Microsoft hiervoor heeft ontwikkeld [48].

- Besteed bij het beoordelen van de security van bijvoorbeeld mobiele en webapplicaties aandacht aan de API's die de applicaties gebruiken.
  Het komt regelmatig voor dat deze API endpoints onvoldoende beveiligd zijn. Een aandachtspunt hierbij is ook hoe de software om gaat met wachtwoorden en andere credentials. Z-CERT constateert dat sommige softwareleveranciers de credentials voor toegang tot deze API's in configuratiebestanden of in de broncode bewaren. In een aantal gevallen waren de credentials daardoor inzichtelijk vanaf het internet. Credentials dienen opgeslagen te worden op een daarvoor speciaal ontworpen beveiligde plek (vaak "vault" genoemd).

- Controleer of uw authenticatieprovider functionaliteit biedt die voorkomt dat hackers de gebruikte multifactorauthenticatie methode kan omzeilen. Microsoft heeft b.v. opties beschikbaar die zogenaamde "MFA fatigue attacks" bemoeilijken [49]. Daarnaast biedt Microsoft (en vele andere providers) zogenaamde "phishing resistente" MFA aan, een methode die bestand is tegen geavanceerde phishing-aanvallen waarbij de aanvaller ook MFA probeert te omzeilen [50].

  In de factsheet "Volwassen authentiseren" van het NCSC worden verschillende multifactorauthenticatie methoden naast elkaar gelegd en de voor en nadelen besproken [51]. Ook worden daarbij volwassenheidsniveaus gedefinieerd.

- Voor aanbevelingen die beschermen tegen malware verwijst Z-CERT u naar de aanbevelingen in het hoofdstuk ransomware.

dreiging

Cyberspionage door statelijke actoren

Inschatting dreiging: hoog

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, 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 zijn de defensieve vermogens van zorgorganisaties niet voldoende om dit type aanvallers buiten de deuren te houden.

Voor organisaties die geen wetenschappelijk onderzoek doen en geen cliënten of patiënten hebben die voor statelijke actoren interessant zijn, is de dreiging vooralsnog een potentiële dreiging. Een potentiële dreiging kan zich snel ontwikkelen naar een concrete dreiging. Op het moment dat uw organisatie - om wat voor reden dan ook - wel interessant wordt voor een statelijke actor.

Incidenten

Er is bij Z-CERT in 2021 één incident bekend geweest waarbij de digitale sporen wijzen op een Chinese statelijke actor. Nader onderzoek leek niet te wijzen op een gerichte aanval. Alhoewel Z-CERT geen digitale spionage-activiteiten heeft waargenomen, zijn er wel recente voorbeelden bekend uit andere landen [52]. Dit maakt dat dergelijke aanvallen voor ons land ook voorstelbaar zijn. Daarnaast zijn statelijke actoren zeer goed in het uitwissen van sporen en "onder de radar blijven" dus de kans is aanwezig dat zorginstellingen en Z-CERT niet alles detecteren.

Bent u een doelwit?

Er zijn een aantal doelen die statelijke actoren willen verwezenlijken:

- **Vergaren van kennis en technologie.**
  Dit kan hen economische voorsprong geven [53]. Daarnaast wil bijvoorbeeld China minder afhankelijk worden van het westen wat betreft kennis en kunde. Zij hebben de ambitie om wereldleider te worden op bepaalde vakgebieden zoals biotechnologie en neurowetenschappen. Organisaties die veel (toegepast) onderzoek doen zijn daarom interessant [54]. Recente waargenomen spionagecampagnes door Chinese statelijke actoren waren gericht op onderzoek naar infectieziekten, genomics en medische technologie [52]. In het verleden was er ook veel interesse in onderzoek naar chronische ziekten als kanker [55].

- **Vergaren van persoonsgegevens in bulk [53] [55].**
  Een grote dataset kan van pas komen bijvoorbeeld als een land onderzoek wil doen naar een bepaald doelwit die in de dataset voorkomt. Een recent voorbeeld van een dergelijke activiteit is de hack op het Rode Kruis waarbij gevoelige persoonsinformatie van 515.000 mensen werd buitgemaakt [56]. Hier lekte ook data van 4600 Nederlanders. Het is niet met 100 procent zekerheid te zeggen dat deze hack uitgevoerd is door een statelijke actor, maar het heeft er wel alle schijn van.

  De AIVD geeft aan dit type informatievergaring niet eerder te hebben gezien in Nederland, en noemt medische instellingen als voorbeeld van een aantrekkelijk doelwit [53].

- **Vergaren van informatie over (ex) burgers die zijn geëmigreerd naar een ander land.** Ze houden graag een vinger aan de pols en ondernemen zelfs beïnvloedings- en inmengingsactiviteiten [57]. Ook vluchtelingen en dissidenten uit het land kunnen interessant zijn. Een zorginstelling met informatie over belangrijke doelwitten zou interessant kunnen zijn.

- **Proactief toegang creëren tot organisaties waar wetenschappelijk onderzoek wordt gedaan.** Deze toegang kunnen ze op een later moment nog gebruiken als het de aanvallers goed uitkomt [54].

Methoden en technieken

- Een bekende methode van statelijke actoren is om kwetsbaarheden waar nog geen patch voor is (zero-day kwetsbaarheid) te misbruiken. Dit jaar werd bijvoorbeeld een kwetsbaarheid in Log4j gebruikt om toegang te verkrijgen tot organisaties [49].
- Het compromitteren van toeleveranciers is een veel gebruikte methode om op een snelle manier toegang te verkrijgen tot meerdere organisaties. Het bekendste voorbeeld is de hack op Solarwinds waarbij waarschijnlijk Russische statelijke actoren toegang kregen tot verschillende Nederlandse zorginstellingen, waaronder ziekenhuizen en GGZ-instellingen. Het lijkt er echter op dat deze zorginstellingen niet een direct doelwit waren, maar eerder bijvangst.

- Indien u op reis gaat naar een risicogebied, is het bekend dat data van gegevensdragers door statelijke actoren gestolen wordt. Loket kennisoverdracht heeft richtlijnen opgesteld die helpen dit soort scenario's te voorkomen [57].

Aanbevelingen

- Wilt u vaststellen of u kwetsbaar bent voor digitale spionage? De AIVD heeft een document gemaakt genaamd "handleiding kwetsbaarheidsonderzoek spionage" dat u hierbij kan helpen [58]. Het gaat hier niet louter om technische zaken maar ook om te identificeren wat mogelijk interessante informatie is voor een statelijke actor.
- Digitale spionage beperkt zich niet tot een hacker die vanaf de buitenkant probeert binnen te dringen in de IT-infrastructuur van een organisatie. Het is bekend dat staten ook doelgericht studenten, onderzoekers en medewerkers naar buitenlandse instellingen sturen met als opdracht spionageactiviteiten te ondernemen [57]. Voor vragen op gebied van internationale samenwerking en veiligheid kan contact opgenomen worden met het loket kennisveiligheid. Vanuit dit loket is er dit jaar ook het product "Nationale leidraad kennisveiligheid Veilig internationaal samenwerken" [57] verschenen dat u helpt kansen en de hieraan verbonden risico's tegen elkaar af te wegen.

dreiging

Financiële fraude

Inschatting dreiging: medium

Z-CERT schat het dreigingsniveau voor financiële fraude door gebruik te maken van digitale media als mail en WhatsApp in op 'medium'. Z-CERT verwacht op korte termijn pogingen van digitale fraude en dit jaar een aantal succesvolle fraudepogingen. De meeste deelnemers schatten de schade die zij als gevolg van financiële fraude via digitale middelen ondervinden in als 'beperkt'. Z-CERT benadrukt wel dat het soms om hoge bedragen kan gaan. In de vorige editie van het dreigingsbeeld noemden we een voorbeeld van een poging tot fraude waarbij men 150.000 euro probeerde te stelen.

Incidenten

In 2022 waren er 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 en sms werden gebruikt als medium.

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.

Malafide facturen of wijzigen van bankrekeningen

Van de ondervraagde deelnemers detecteerde 28 procent frauduleuze facturen of een frauduleuze poging om een rekeningnummer te laten wijzigen. 2 Procent van de ondervraagde deelnemers meldde een geslaagde poging.

Methoden en technieken

De personen achter deze fraudepogingen hanteren veelal dezelfde technieken. Er wordt aan medewerkers gevraagd om geld over te maken voor cadeaubonnen. Het komt voor dat aanvallen geavanceerder zijn. Dan wordt er bijvoorbeeld een nepdomeinnaam aangemaakt die lijkt op de domeinnaam van de zorginstellingen. Er kan vervolgens voor duizenden euro's artikelen besteld worden.

Vaak lijkt de aanvaller namen van mensen van LinkedIn te halen. Bijvoorbeeld: zoek op LinkedIn een directeur van een zorginstelling op en een HR-medewerker. Maak een mailadres aan en mail zogenaamd namens de directeur naar het echte mailadres van de HR-medewerker met het verzoek om vóór de volgende salarisbetaling de bankrekening aan te passen. Voor dergelijke aanvallen worden niet altijd social media als bron gebruikt. Dit jaar was er een enkel geval bekend waarin de nieuwe baan van een medewerker nog niet op social media bekend was. Ook werden voor het eerst CISO's nagebootst. Dit gaat verder dan de standaard 'cadeaubonnenfraude' omdat hierbij specifieke kennis gebruikt wordt.

Een veelvoorkomend probleem is dat vaak legitieme mailadressen worden gebruikt. Bijvoorbeeld een Gmail- of een Hotmail-adres. Een spamfilter haalt deze legitiem uitziende e-mails er over het algemeen niet uit omdat er geen malware aan vast zit en er geen malafide links in zitten. De kans dat de mail een zorgmedewerker bereikt, is daarom erg groot.

Aanbevelingen

- Implementeer e-mailstandaarden (SPF, DKIM en DMARC). Indien deze ontbreken wordt het voor een aanvaller heel makkelijk omdat zij dan kunnen mailen met het echte e-mailadres van een CEO. In 2021 gebeurde dit bij één organisatie omdat er een fout was gemaakt bij het implementeren van deze standaarden en een cybercrimineel zich kon voordoen als een collega. Voor meer informatie: [59].

- Monitor op 'look-a-like' domeinnamen die mogelijk misbruikt worden voor criminele doeleinden. Veel security-providers doen dit al en er zijn gratis tools beschikbaar die deze functionaliteit aanbieden. Zie bijvoorbeeld: [60].

- Registreer pogingen tot financiële fraude en neem deze op in de security-rapportages. Bij 4 procent van de ondervraagden werden CEO-fraude pogingen niet geregistreerd. Statistieken op dit vlak helpen bij security awareness trainingen en tonen het belang aan van het nemen van preventiemaatregelen tegen deze dreiging.

- Security awareness training over dit onderwerp is belangrijk omdat juist bij dit type fraude technische maatregelen niet veel uithalen. De financiële afdeling maar ook andere afdelingen waar betalingsbevoegdheden liggen, zijn daarbij belangrijk.
  Echter iedere medewerker zou hierin onderwezen moeten worden omdat vooral bij fraude met cadeaubonnen een medemerker verleid wordt om geld voor te schieten vanuit hun persoonlijk vermogen.

- Interne autorisatieprocedures en -processen moeten zo opgezet worden dat fraude voorkomen wordt. Bijvoorbeeld één zorginstelling meldde dat malafide pogingen tot het veranderen van rekeningen niet konden slagen, omdat werknemers dit zelf moeten doen in een daarvoor bestemd portaal. Het feit dat een financiële of HR-medewerker dit niet kan en mag, zorgt ervoor dat dit type fraude niet voorkomt bij deze organisatie.

- Creëer een procedure waarbij medewerkers pogingen tot financiële fraude kunnen melden. Daarnaast moet er ook een cultuur zijn dat bij twijfel of een melding legitiem is of niet, contact opgenomen kan worden met iemand binnen de organisatie of een leidinggevende. 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.

thema

Ontwikkelingen met kansen voor hackers én zorgaanbieders

In de maatschappij, maar zeker ook in de zorg, vinden ontwikkelingen plaats zoals de toename van thuiswerken of personeelstekort. In dit hoofdstuk nemen we een aantal trends onder de loep en onderzoeken we welke dreigingen gelinkt zijn aan deze ontwikkelingen. Het doel hiervan is dat zorgaanbieders zich bewust zijn van de kansen die een ontwikkeling kan bieden aan aanvallers. Ook kunnen zorgaanbieders deze inzichten zo meenemen in hun risicoanalyses en leveranciersmanagement. Sommige ontwikkelingen kunnen ook kansen bieden voor de zorginstellingen om de weerbaarheid te verhogen.

Ontwikkeling/Dreiging	Ransomware	Ransomware leveranciers	DDoS	DDoS leveranciers	Datalekken	Financiële fraude	Spionage
Transitie naar de cloud		x	x	x	x		x
Professionalisering van cybercrime	x	x		x	x		
Conflict Rusland en Oekraïne			x	x			x
Personeelstekort	x				x	x	x
Gebrek aan security awareness	x				x	x	x
Personeelstekort IT en security	x		x		x	x	x

Tabel 1

Overzicht van de ontwikkelingen en dreigingen die hier aan gelinkt zijn

Trend: transitie naar de cloud

De zorg digitaliseert en is in toenemende mate afhankelijk van de cloud. Deze groeiende afhankelijkheid viel met name op in de volgende categorieën:

1. Consultaties op afstand

Veel zorginstellingen zetten in op consultaties op afstand waarbij cloudoplossingen worden gebruikt. De Nederlandse Vereniging van Ziekenhuizen (NVZ) meldde bijvoorbeeld dat in het eerste kwartaal van 2022, bijna 28 procent van alle poliklinische zorg digitaal werd afgehandeld [61]. Veel zorginstellingen hebben zich als doel gesteld om meer consulten door middel van beeldbellen uit te voeren [62]. Naast beeldbellen, kan men ook vaak vragen stellen via een portal, app of beveiligde mail [63].

> **“Veel zorginstellingen zetten in op consultaties op afstand waarbij cloudoplossingen worden gebruikt”**

2. Telemonitoring

Veel ziekenhuizen zetten vol in op telemonitoring [62]. De verwachting is dat de mondiale markt die in 2021, een waarde had van 1,2 miljard dollar in 2028 een waarde zal hebben 4,1 miljard dollar [64]. Omdat bij telemonitoring patiënten op afstand gemonitord worden, is de oplossing vaak afhankelijk van de cloud. De patiënt kan zelf met behulp van een medisch apparaat metingen uitvoeren en deze samen met een vragenlijst via een app versturen. Ook kunnen middels sensoren bepaalde zaken gemonitord worden en meetresultaten automatisch doorgestuurd worden naar behandelaars [65].

3. Zorgdomotica

De zorgdomotica markt is groeiende [66]. Het ‘middleware’-gedeelte van domotica-oplossingen wordt steeds vaker in de cloud afgenomen. In het middleware-gedeelte wordt data opgeslagen en worden alarmeringen gerouteerd [66]. Veel zorgdomotica oplossingen spelen dagelijks een rol in de zorg voor vaak tienduizenden cliënten [66].

Domotica wordt bijvoorbeeld veel ingezet in de ouderenzorg, gehandicaptenzorg en GGZ ten behoeve van de veiligheid of het gemak van de patiënt of cliënt. Het is een technologie die een taak vervult in en om het huis. De toepassingen zijn eindeloos. Zo kan worden gemonitord of medicijnen zijn ingenomen, gaat er een alarm als iemand valt en wordt gemonitord waar een persoon met dementie zich bevindt. Ook rookmelders en camera’s zijn voorbeelden van domotica.

4. Migratie naar clouddiensten

De meeste organisaties in de zorg stappen steeds meer over op clouddiensten voor de applicaties die zij gebruiken. Dit zijn vaak bedrijfsondersteunende applicaties maar ook elektronische cliëntendossiers. Vooral bij de jeugdzorg, GGD, gehandicaptenzorg en de ouderenzorg is daar vaak het beleid ‘cloud tenzij’ waarbij vooral ingezet wordt op Software as a Service (SaaS-diensten). Ziekenhuizen zijn vaak wat behoudender, maar ook daar worden steeds meer clouddiensten afgenomen. Bovendien wordt veel infrastructuur verplaatst naar de cloud. Soms voelt de zorginstelling zich zelfs gedwongen om naar de cloud te gaan omdat de applicatie in kwestie alleen nog in de cloud af te nemen is. Ook ervaren zorginstellingen grote ‘druk’ vanuit grote leveranciers om naar de cloud te gaan.

ontwikkelingen met kansen voor hackers én zorgaanbieders

Kansen voor aanvallers:

- De markt voor digitale producten en diensten in de cloud groeit. Dit betekent dat er kansen liggen en er nieuwe bedrijfjes opgericht worden om gespecialiseerde diensten voor bijvoorbeeld het leveren van telemonitoring of domotica. Daarnaast zijn er softwareleveranciers die zich gedwongen voelen door de markt om hun applicatie in de cloud aan te bieden. Zonder dat zij ervaring hebben met het managen en beveiligen van een clouddienst.

  In de praktijk blijkt de volwassenheid wat betreft informatiebeveiliging en cybersecurity niet altijd voldoende te zijn voor dit soort bedrijven, wat de kans op cyberincidenten verhoogd.

- Het concentreren van data van zorgverleners bij dezelfde leveranciers zorgt dat één incident impact kan hebben op meerdere zorginstellingen en soms duizenden cliënten. Dit maakt deze leveranciers een aantrekkelijk doelwit voor cybercriminelen. Voor een dergelijke leverancier is een hoge volwassenheidsniveau op het gebied van cybersecurity, essentieel. De Verenigde Staten, het Verenigd Koninkrijk, Canada, Australië en Nieuw-Zeeland waarschuwden in mei 2022 dat er verhoogde aandacht is van dreigingsactoren voor managed service providers die bijvoorbeeld cloudoplossingen beheren [67].

- Zorginstellingen zijn door het afnemen van cloudapplicaties in hoge mate afhankelijk van hun internetverbinding. Indien de internetverbinding niet functioneert b.v. door een DDoS-aanval op de externe firewall, kan het zijn dat de zorginstelling geen toegang heeft tot de applicaties in de cloud.

- Software die gehost wordt in de cloud, levert nieuwe risico's op zoals kwetsbaarheden en misconfiguraties die in deze nieuwe situatie ook vaak vanaf het internet te misbruiken zijn. Met name slecht beveiligde API's zijn een punt van zorg.

- Een softwareoplossing die in de cloud draait is vaak afhankelijk van meerdere leveranciers. Voor bijvoorbeeld een beeldbeloplossing moet soms worden ingelogd op een portaal. Voor het inloggen wordt gebruik gemaakt van een identiteitsprovider. Daarnaast is er een DNS-provider nodig om naar de URL te surfen en is er een leverancier die de hosting en connectiviteit verzorgt. Op al deze punten in de keten heeft Z-CERT afgelopen jaar incidenten gezien, waardoor er niet of verminderd gebruik gemaakt kon worden van een digitale dienst van een zorgaanbieder.

Kansen voor zorginstellingen:

- Daar waar snel patchen voor een zorginstelling soms een uitdaging is, is dit bij cloudoplossingen door grote cloudleveranciers vaak op orde.

- Sommige cloudoplossingen bieden uitgebreide functionaliteit op het gebied van informatiebeveiliging en cybersecurity.

- Volwassen clouddiensten kunnen een hoge staat van volwassenheid bereiken wat betreft de security van hun eigen infrastructuur, hoger dan een zorginstelling zelf zou kunnen leveren.

Professionalisering van cybercrime

Cybercrime-groepen zijn goed georganiseerd en werken samen om de effectiviteit te verhogen. Dit leidt ertoe dat deze cybercrime-groepen tientallen en soms meer dan honderd ransomware-incidenten kunnen afwerken per maand. Omdat digitale munten anoniem geïncasseerd kunnen worden, blijft dit ecosysteem van cybercrime bestaan. Daarnaast werkt een georganiseerde "ransomware as a service" groep erg drempelverlagend om als nieuwe cybercrimineel aan de slag te gaan. De grote bedragen die verdiend worden hebben ook een aanzuigende werking op nieuwe rekruten.

Cybercriminelen creëren gebruiksvriendelijke tools om kwetsbaarheden automatisch te misbruiken, vaak verkopen ze deze toegang door. Automatisering betekent dat een zorginstelling die niet op tijd is met patchen vaak automatisch gecompromitteerd wordt. Dit geldt ook voor de distributie van malware en misbruik van gestolen wachtwoorden. Daar waar multifactor-authenticatie en bescherming tegen malware niet optimaal is, loopt een zorgorganisatie de kans dat een hacker toegang krijgt tot systemen van de organisatie. De verkregen toegang kan voor verschillende doeleinden misbruikt worden.

Gebrek aan security awareness bij medewerkers

Veel deelnemers melden dat bewustwording een punt van zorg is. In de zorg werken veel medewerkers die van nature geneigd zijn om te helpen. De uitspraak 'ik houd van mensen niet van computers' is er één die veel zorgmedewerkers herkennen. Een onderliggend probleem voor een gebrek aan security awareness is dat sommige medewerkers beperkt digitaal vaardig zijn. Werken aan digitaal vaardig maker en security awareness gaan vaak hand in hand.

Daarnaast is er onder zorgpersoneel soms een hoog verloop of wordt er gewerkt met tijdelijke krachten. Door de werkdruk, in combinatie met de tijdelijke aard van het dienstverband, is er geen tijd of capaciteit om deze medewerkers voldoende op te leiden wat betreft security awareness.
Een gebrek aan security awareness genereert kansen voor cybercriminelen op het gebied van financiële fraude, datalekken en ransomware.

Geopolitieke ontwikkelingen

Het conflict tussen Rusland en Oekraïne heeft het afgelopen jaar geen impact gehad op de zorg in Nederland. Wel hadden verschillende zorginstellingen in Europa last van DDoS-aanvallen die ondernomen werden vanuit Pro-Russische hacktivisten. In het hoofdstuk DDoS gaan we hier verder op in.
Stel dat het conflict escaleert en Nederland direct bij het conflict betrokken wordt, verwacht Z-CERT voor de zorg vooral een actuele dreiging vanuit pro-Russische hacktivisten. Z-CERT verwacht niet dat de Nederlandse zorg direct een doelwit zal worden voor statelijke actoren. Bij aanvallen geïnitieerd door statelijke actoren zal er wel het risico zijn op nevenschade die bijvoorbeeld kan ontstaan als internet service providers of energieleveranciers worden aangevallen. Het gaat hier met name om DDoS-aanvallen, aanvallen met ransomware en wipersoftware. Ook malware die door aan Rusland gelieerde statelijke actoren verspreid wordt en onbedoeld terechtkomt bij zorgorganisaties zou incidenten kunnen veroorzaken. Voorbeelden uit het verleden daarvan zijn de aanvallen met de NotPetya malware die waarschijnlijk onbedoeld ziekenhuizen raakten in de VS [52] en de Solarwinds hack die onbedoeld impact had op verschillende Nederlandse zorginstellingen.

De leverancierskеten bleek in 2022 kwetsbaar doordat verschillende pro-Oekraïense hacktivisten malafide code introduceerden in veel gebruikte open-source softwarecomponenten [68]. In één geval leidde dit onbedoeld tot verlies van data bij een hulporganisatie die zijn servers gehost had in Wit-Rusland. Het managen van deze 'third party components' is een onderwerp voor leveranciersmanagement met software leveranciers. Ook buiten het conflict tussen Rusland en Oekraïne waren er voorbeelden waarbij open-source componenten aangepast werden met malware [69] [70] of waarbij nepversies van bestaande componenten verspreid werden.

Thuiswerken

Sinds corona is thuiswerken heel normaal geworden. Thuiswerken heeft een aantal zaken veranderd.

- Sommige medewerkers hebben autorisaties gekregen die zij voor corona niet hadden, maar nu vanwege het thuiswerken wel nodig hebben. De autorisaties zijn na corona niet ingetrokken omdat de manier van werken permanent veranderd lijkt te zijn. In geval van een security incident heeft een aanvaller mogelijk meer toegang tot gevoelige data dan voorheen.

- Meer mensen maken gebruik van remote toegang oplossingen als voor corona. De kans dat een aanvaller credentials voor remote toegang kan krijgen, neemt daardoor toe. Ook zal in geval van een DDoS-aanval er impact zijn op meer gebruikers als voorheen.

- Op de werkvloer zijn contactfrequenties groter en worden er sneller zaken met elkaar gedeeld. Wanneer mensen thuiswerken, is het minder vanzelfsprekend om even een collega mee laten kijken naar een verdacht mailtje of het delen van informatie over phishing-campagnes. Dit vergroot de kans dat een phishing-aanval of poging tot CEO-fraude slaagt.

Personeelstekort IT en security

Zorginstellingen melden dat het moeilijk is om IT- en security-personeel te krijgen door krapte op de arbeidsmarkt. Ook zijn ze niet altijd in staat concurrerende lonen te bieden. Dit betekent dat zorginstellingen niet altijd over genoeg gekwalificeerd security-personeel bezitten. Dit kan er onder andere toe leiden dat security-meldingen niet tijdig opgepakt worden, patchen niet op tijd wordt uitgevoerd en de groei in volwassenheid stagneert. Sommige zorginstellingen hebben hetzelfde probleem geconstateerd bij leveranciers en maken zich hierover zorgen.

De aanvalsmogelijkheden die personeelskrapte geeft kan per instelling variëren. Echter omdat het vaak impact heeft op meerdere aspecten van de weerbaarheid van een organisatie, zal het risico op verschillende typen incidenten verhoogd zijn.

“ Omdat personeelskrapte vaak impact heeft op meerdere aspecten van de weerbaarheid van een organisatie, zal het risico op verschillende typen incidenten verhoogd zijn ”

thema

Evaluatie Log4j-crisis

Log4Shell, de kwetsbaarheid in de loggingstool Apache Log4j, behoeft bijna geen inleiding meer. Deze kwetsbaarheid bracht de gemoederen behoorlijk in beweging eind 2021 en in 2022. De kwetsbaarheid maakte misbruik van functionaliteit in Log4j die loggingsdata probeerde te verrijken. Hierdoor kon een aanvaller de Log4j module 'instrueren' om malafide commando's op te halen en uit te voeren. Om het wiel niet telkens opnieuw uit te hoeven vinden, gebruiken veel softwareontwikkelaars Log4j om het loggingsgedeelte af te handelen. Hierdoor was Log4j in erg veel applicaties aanwezig en het aanvalsoppervlak groot.

Impact

Vanwege het grote aanvalsoppervlak was de kans op misbruik hoger en het risico dus groter. Er werd dan ook rekening gehouden met grootschalig misbruik. In de praktijk bleek dit echter gelukkig mee te vallen. Hoewel er door zorginstellingen incidenten gemeld zijn met Log4Shell als aanvalsvector, bleef dit bij enkelen. Er was één incident die een aanzienlijke impact had en bij een ander serieus incident was de impact beperkt omdat men er op tijd bij was.

Veel cybersecurity partijen maakten zich grote zorgen over de mogelijke impact van de kwetsbaarheid in Log4j. De hoeveelheid applicaties die gebruikmaken van Log4j is groot, en de kwetsbaarheid stelde een aanvaller in staat om aan 'Remote Code Execution' te doen. Hierbij kan een aanvaller commando's geven aan een computer alsof hij er voor zou zitten. Daar nog bovenop kwam de onzekerheid over welke applicaties, welke versies van Log4j gebruikten. Deze combinatie van factoren creëerde de omstandigheden voor een 'perfect storm'.

Waarom is grootschalig misbruik uitgebleven?

Misbruik is beperkt gebleven omdat veel zorginstellingen adequaat hebben gereageerd door snel preventief maatregelen te nemen en te patchen. Veel zorginstellingen zetten een crisisorganisatie op om de situatie te controleren. Daarnaast werd het uitbuiten van de kwetsbaarheid bemoeilijkt doordat de kwetsbaarheid in een loggingsmodule zat. Logging wordt, afhankelijk van de inrichting van systemen, lang niet altijd op het systeem waar de applicatie draait afgehandeld. Omdat de daadwerkelijk kwetsbare, achterliggende, systemen veelal niet aan het internet ontsloten waren, kon de kwetsbaarheid niet misbruikt worden. In andere gevallen kregen aanvallers wel signalen terug dat een aanval of verkenning was gelukt, maar kwam dit pas vele uren later, vanuit onverwachte plekken. Dit zorgde in veel gevallen dat aanvallers belemmerd werden.

Wel bleek een aantal oplossingen op zo'n manier in elkaar te zitten dat deze zeer geschikt waren voor misbruik als ze ontsloten waren aan het internet.

In de loop van de tijd werd er bij gebruikers van deze producten wereldwijd op grotere schaal misbruik geconstateerd door zowel ransomware als statelijke actoren. Dit leidde tot security-incidenten in zowel buitenlandse zorginstellingen als bij de twee genoemde incidenten in Nederland.

Lessons learned

Hoewel Log4j in veel applicaties wordt gebruikt, was dit niet vaak erg duidelijk. Applicaties worden meestal gebouwd met hergebruik van componenten, maar inzicht in welke componenten allemaal gebruikt worden, is nog lang niet altijd een gewoonte. Er is hier daarom sprake van supply chain risico's. Gelukkig wordt er hard gewerkt aan oplossingen hieromtrent. Een van de beste kandidaten hiervoor is de zogeheten Software Bill of Materials (verder, SBoM). Deze standaard schrijft een lijst voor van gebruikte componenten in een gestructureerd, afgesproken formaat. Het gebruik van deze standaard kan erg nuttig zijn in het kader van kwetsbaarhedenmanagement.

Z-CERT roept daarom ook ontwikkelaars van soft- en hardware op om gebruik te maken van de SBoM, en motiveert zorginstellingen om in de relatie met leveranciers te verzoeken gebruik te maken van de SBoM.

Evaluatie

In de afwezigheid van een hoge graad van adoptie van de SBoM was de inspanning van het NCSC en haar partners een welkome toevoeging tijdens de Log4j-crisis. Door middel van een publiek beschikbare Github-pagina werd bijgehouden welke leveranciers wel en niet gebruik maakten van Log4j. Bij reguliere soft- en hardware was dit echter gemakkelijker dan bij leveranciers van medische soft- en hardware. Het is daarom wenselijk om de banden met deze partijen verder aan te halen om zorginstellingen specifieker te kunnen ondersteunen.

Naast de meldingen van leveranciers zelf werd er door diverse partijen gescand naar kwetsbare systemen. Dankzij een steeds toenemende mate van informatiedeling onder cybersecurity partijen in Nederland, die Z-CERT als zeer positief waardeert, konden zorginstellingen sneller geïnformeerd worden over kwetsbare systemen. Om hieraan nog actiever te kunnen bijdragen, is Z-CERT bezig met de implementatie van scantooling.

> **"Dankzij een steeds toenemende mate van informatiedeling konden zorginstellingen sneller geïnformeerd worden over kwetsbare systemen"**

Samenvatting

De grootste dreiging voor de zorgsector schuilt in verstoringen door ransomware-besmettingen bij een zorginstelling zelf of bij een IT-leverancier van de zorgorganisatie. Leveranciers van zorginstellingen worden vaker geraakt dan zorgorganisaties zelf. Het komend jaar verwacht Z-CERT een aantal ransomware-incidenten in de leverancierssketen die impact zullen hebben op Nederlandse zorginstellingen.

Z-CERT registreerde afgelopen jaar 65 procent meer ransomware-incidenten bij Europese zorginstellingen dan een jaar eerder. In Nederland heeft Z-CERT tenminste vijf ransomware-incidenten bij zorgorganisaties gezien. Dat zijn er evenveel als in 2021. Een verschil is wel dat de impact op de totale hoeveelheid zorginstellingen die in Nederland overlast ondervonden, in 2022 veel groter was.

Ook bestaat er een grote kans op datalekken in de zorg als gevolg van hacking. Vooral datalekken die optreden door aanvallen op webapplicaties komen vaak voor. De aanvaller gebruikt hiervoor bijvoorbeeld gestolen wachtwoorden of misbruikt bekende kwetsbaarheden of misconfiguraties. Doordat zorgorganisaties steeds vaker hun webapplicaties afnemen in de cloud, is dit een aandachtspunt voor de zorg. De meeste aanvallen waarbij er ingelogd moet worden met een gebruikersnaam en wachtwoord, kunnen goed worden tegengehouden door het gebruik van multifactorauthenticatie.

Data in de zorg is vaak gevoelig. Securityprofessionals maken zich daarom zorgen om de groepen cybercriminelen die data stelen om organisaties af te persen. Ze dreigen met het lekken van gevoelige data als het slachtoffer niet tot betaling overgaat. Vaak gaat dit om aanvallen met ransomware, maar het kan ook gaan om afpersen waarbij cybercriminelen dreigen een organisatie plat te leggen met een DDoS-aanval.

Het risico van uitval van systemen of diensten in de zorg door DDoS-aanvallen lijkt echter niet zo groot. Z-CERT kreeg slechts drie meldingen over gerichte DDoS-aanvallen voor de zorg. Wel bestaat er een risico dat zorginstellingen last krijgen van DDoS-aanvallen die zijn uitgevoerd op leveranciers, zoals cloudaanbieders of hosting- en internet service providers. Opvallend is dat het conflict tussen Rusland en Oekraïne het afgelopen jaar nauwelijks impact heeft gehad op de zorg in Nederland.

Een andere dreiging is cyberspionage door statelijke actoren. Dit is vooral een risico voor zorgorganisaties waar veel wetenschappelijk onderzoek wordt gedaan dat bovendien relevant is voor statelijke actoren. Voorbeelden daarvan zijn grote hoeveelheden persoonsgegevens of specifieke kennis en technologie.

Tot slot vormt financiële fraude een reële dreiging voor de zorg. De bekendste vorm daarvan is CEO-fraude. Hoewel veel van deze fraude-pogingen op tijd worden geblokkeerd, meldt 2 procent van de door Z-CERT ondervraagde zorginstellingen dat een poging tot CEO-fraude is geslaagd. De bedragen die organisaties daardoor verliezen, kunnen snel oplopen tot soms wel 150.000 euro. Omdat technische maatregelen niet altijd voldoende zijn om dergelijke aanvallen tegen te houden, is aandacht voor security awareness training van groot belang.

De toenemende digitalisering van de zorg en het verhuizen van applicaties naar de cloud biedt nieuwe mogelijkheden voor zorginstellingen en patiënten en cliënten. Dit is een goede ontwikkeling zolang zorgaanbieders zich bewust zijn van de beveiligingsrisico's en voldoende mitigerende maatregelen treffen.

Bibliografie

[1] **Colloseum Dental**, *"Informatiepagina cyberincident augustus 2022,"* [Online]. Available: https://www.colosseumdental.nl/mededeling-cyberincident.

[2] **Secutec**, *"Hackers show remorse after attack on Flemish facility for people with disabilities,"* 1 Maart 2022. [Online]. Available: https://secutec.eu/hackers-show-remorse-after-attack-on-flemish-facility-for-people-with-disabilities/.

[3] **Sophos**, *"The State of Ransomware in Healthcare 2022,"* Sophos, 31 Mei 2022. [Online]. Available: https://news.sophos.com/en-us/2022/06/01/the-state-of-ransomware-in-healthcare-2022/.

[4] **Microsoft**, *"Cyber Signals: 3 strategies for protection against ransomware,"* 30 Augustus 2022. [Online]. Available: https://www.microsoft.com/security/blog/2022/08/30/cyber-signals-3-strategies-for-protection-against-ransomware/.

[5] **Coveware**, 26 Oktober 2022. [Online]. Available: https://www.coveware.com/blog/2022/10/26/q3-2022-quarterly-report.

[6] **Kaspersky**, *"Common TTPs of modern ransomware groups,"* 23 Juni 2022. [Online]. Available: https://go.kaspersky.com/rs/802-IJN-240/images/Common-TTPs-of-the-modern-ransomware_low-res.pdf.

[7] **Sami Laiho**, *"AppLocker whitelisting vs. blacklisting,"* 10 Juni 2020. [Online]. Available: https://4sysops.com/archives/applocker-whitelisting-vs-blacklisting/.

[8] **ACSC**, *"Microsoft Office Macro Security,"* Oktober 2021. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/publications/microsoft-office-macro-security.

[9] **ACSC**, *"Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016,"* Januari 2022. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-365-office-2021-office-2019-and-office-2016.

[10] **Redcanary**, *"Why so, ISO? Mark-of-the-Web, explained,"* 3 November 2022. [Online]. Available: https://redcanary.com/blog/iso-files/.

[11] **Jan Hanstede**, *"Detectie van ransomware,"* 2020. [Online]. Available: https://www.z-cert.nl/kennisbank/ransomware-logging/.

[12] **Z-CERT**, *"Tien gouden tips tegen ransomware,"* 12 Oktober 2021. [Online]. Available: https://www.z-cert.nl/wp-content/uploads/2021/02/Z-CERT_FactsheetRansomware_2560x1920px_04-1.pdf.

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

[14] **Hunt & Hackett BV**, *"Red Mudnester: Rapportage,"* 4 Juli 2022. [Online]. Available: https://openpub.buren.nl/wp-content/uploads/2022/07/20220701_Red-Mudnester_Report_v3.0_Publiek.pdf.

[15] **Verizon**, *"2022 Data Breach,"* 2022. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/.

[16] **NBIP**, *"DDoS-aanvallen steeds vaker onderdeel van bredere aanval,"* Juli 12 2022. [Online]. Available: https://www.nbip.nl/nieuws/ddos-aanvallen-q2-2022/.

[17] **Privacy Affairs**, *"Dark Web Price Index 2022,"* 19 September 2022. [Online]. Available: https://www.privacyaffairs.com/dark-web-price-index-2022/.

[18] **Netscout**, "*findings from 2nd half 2021 - netscout threat intelligence report,*" 2021. [Online]. Available: https://www.netscout.com/sites/default/files/2022-03/ThreatReport_2H2021_WEB.pdf.

[19] **Z-CERT**, Telegram kanaal van de pro-Russische hacktivisme groep Phoenix, 2022.

[20] **Z-CERT**, Telegram kanaal van de Pro-Russische hacktivisme groep *"Killnet"*, 2022.

[21] **FBI**, *"Hacktivists Use of DDoS Activity Causes Minor Impacts,"* 4 November 2022. [Online].

[22] **SingCERT**, *"Dangers and implications of Hacktivism during the Russia-Ukraine Conflict,"* 7 April 2022. [Online]. Available: https://www.csa.gov.sg/singcert/Publications/dangers-and-implications-of-hacktivism-during-the-russia-ukraine-conflict.

[23] **B. Toulas**, *"Russian hacktivists launch DDoS attacks on Romanian govt sites,"* 29 April 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/russian-hacktivists-launch-ddos-attacks-on-romanian-govt-sites/.

[24] **Digital shadows**, *"Killnet: The Hactivist Group That Started A Global Cyber War,"* 8 juni 2022. [Online]. Available: https://www.digitalshadows.com/blog-and-research/killnet-the-hactivist-group-that-started-a-global-cyber-war/.

[25] **Sysdig**, *"2022 Sysdig Cloud Native Threat Report,"* 2022. [Online]. Available: https://sysdig.com/wp-content/uploads/2022-cloud-native-threat-report.pdf.

[26] **NCSC**, *"Factsheet Technische maatregelen voor continuïteit voor online diensten,"* 14 Maart 2016. [Online]. Available: https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-technische-maatregelen-voor-continuiteit-van-online-diensten.

[27] **CSIRT-ITA**, *"Attacco DDoS ai danni del sito istituzionale dello CSIRT Italia.,"* 31 Mei 2022. [Online]. Available: https://www.csirt.gov.it/contenuti/attacco-ddos-ai-danni-del-sito-istituzionale-dello-csirt-italia-del-30-maggio-2022-analisi-preliminare-bl01-220531-csirt-ita.

[28] **NCSC**, *"Factsheet Continuïteit van online diensten,"* 14 Maart 2016. [Online]. Available: https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-continuiteit-van-onlinediensten.

[29] **NCSC UK**, *"A minimal Denial of Service (DoS) response plan,"* 20 Januari 2019. [Online]. Available: https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection/a-minimal-denial-of-service-response-plan.

[30] **O. Yoachimik**, Cloudflare, 12 Oktober 2022. [Online]. Available: https://blog.cloudflare.com/cloudflare-ddos-threat-report-2022-q3/.

[31] **Netscout**, *"DDoS THREAT INTELLIGENCE REPORT (1st half 2022),"* 2022. [Online]. Available: https://www.netscout.com/threatreport/.

[32] **NBIP**, [Online]. Available: https://www.nbip.nl/nieuws/. [Accessed https://www.nbip.nl/nieuws/ Januari 2023].

[33] **Imperva** , *"81% Increase in Large-Volume DDoS Attacks,"* 27 September 2022. [Online]. Available: https://www.imperva.com/blog/81-increase-in-large-volume-ddos-attacks/.

[34] **Cloudlare**, *"Cloudflare DDoS threat report for 2022 Q4,"* 10 Januari 2022. [Online]. Available: https://blog.cloudflare.com/ddos-threat-report-2022-q4/.

[35] **Cloudflare**, *"Cloudflare threat rapports of Q1, Q2, Q3 and Q4 2022,"* 2022.

[36] **NBIP**, *"Cijfers DDoS-aanvallen in het vierde kwartaal 2022,"* 18 Januari 2022. [Online]. Available: https://www.nbip.nl/wp-content/uploads/2023/01/NBIP%20-%20Infographic%20-%20DDoS%20data%20-%20Q4%202022%20%5BNL%5D.pdf.

[37] **G. Moura**, *"TTL-waarden voor DNS-records kiezen: hoe doe je dat?,"* SIDN, 17 September 2019. [Online]. Available: https://www.sidnlabs.nl/nieuws-en-blogs/ttl-waarden-voor-dns-records-kiezen-hoe-doe-je-dat.

[38] **Kaspersky**, *"QakBot technical analysis,"* 2 September 2021. [Online]. Available: https://securelist.com/qakbot-technical-analysis/103931/.

[39] **Nedap**, *"Beveiligingsincident Carenzorgt.nl,"* 2022 Oktober 2022. [Online]. Available: https://nedap.com/wp-content/uploads/2022/10/Persbericht-Beveiligingsincident-Carenzorgt.nl_.pdf.

[40] **Security.nl**, *"Zorginstellingen melden datalek na inbraak bij digitaal zorgplatform Carenzorgt,"* 2 November 2022. [Online]. Available: https://www.security.nl/posting/773253/Zorginstellingen+melden+datalek+na+inbraak+bij+digitaal+zorgplatform+Carenzorgt.

[41] **Security.nl**, *""Criminelen stelen 675.000 wachtwoorden van Nederlandse computers","* 23 November 2022. [Online]. Available: https://www.security.nl/posting/775361/%22Criminelen+stelen+675_000+wachtwoorden+van+Nederlandse+computers%22.

[42] **Sophos**, *"Cookie stealing: the new perimeter bypass,"* 28 Augustus 2022. [Online]. Available: https://news.sophos.com/en-us/2022/08/18/cookie-stealing-the-new-perimeter-bypass/.

[43] **Security.nl**, *"Inbraak CircleCI via gestolen '2FA-backed' SSO-sessie van laptop engineer,"* 16 Januari 2023. [Online]. Available: https://www.security.nl/posting/781495/Inbraak+CircleCI+via+gestolen+%272FA-backed%27+SSO-sessie+van+laptop+engineer.

[44] **Bleepingcomputer**, *"MFA Fatigue: Hackers' new favorite tactic in high-profile breaches,"* 20 September 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/mfa-fatigue-hackers-new-favorite-tactic-in-high-profile-breaches/.

[45] **Bleepingcomputer**, *"Microsoft accounts targeted with new MFA-bypassing phishing kit,"* 3 Augustus 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/microsoft-accounts-targeted-with-new-mfa-bypassing-phishing-kit/.

[46] **J. Bouman**, 22 December 2022. [Online]. Available: https://twitter.com/JonathanBouman/status/1603158320365420544.

[47] **NCSC**, *"ICT-beveiligingsrichtlijnen voor webapplicaties,"* 1 September 2015. [Online]. Available: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties.

[48] **Microsoft**, *"What are the Microsoft SDL practices?,"* [Online]. Available: https://www.microsoft.com/en-us/securityengineering/sdl/practices. [Accessed 7 December 2022].

[49] **Microsoft**, *"Defend your users from MFA fatigue attacks,"* 28 September 2022. [Online]. Available: https://techcommunity.microsoft.com/t5/

microsoft-entra-azure-ad-blog/defend-your-users-from-mfa-fatigue-attacks/ba-p/2365677.

[50] **Microsoft**, *"Conditional Access authentication strength (preview),"* 12 Januari 2023. [Online]. Available: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-strengths.

[51] **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.

[52] **American Hosptial Association**, *"Agencies alert health care sector to commonly exploited cyber vulnerabilities,"* 7 Oktober 2022. [Online]. Available: https://www.aha.org/news/headline/2022-10-07-agencies-alert-health-care-sector-commonly-exploited-cyber-vulnerabilities.

[53] **2022**, *"Dreigingsbeeld Statelijke Actoren 2 November 2022,"* 28 November 2022. [Online]. Available: https://www.rijksoverheid.nl/documenten/rapporten/2022/11/28/tk-bijlage-dreigingsbeeld-statelijke-actoren-2.

[54] **M. N. AIVD**, *"Dreigingsbeeld statelijke actoren,"* 3 Februari 2021. [Online]. Available: https://www.rijksoverheid.nl/documenten/rapporten/2021/02/03/dreigingsbeeld-statelijke-actoren.

[55] **FireEye**, *"Beyond Compliance: Cyber Threats and Healthcare,"* 2020. [Online]. Available: https://content.fireeye.com/cyber-security-for-healthcare/rpt-beyond-compliance-cyber-threats-and-healthcare.

[56] **ICRC**, *"Cyber-attack on ICRC: What we know,"* 16 Februari 2022. [Online]. Available: https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know.

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

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

[59] **NCSC**, *"Factsheet Bescherm domeinnamen tegen phishing,"* 28 Oktober 2015. [Online]. Available: https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-bescherm-domeinnamen-tegen-phishing.

[60] **CIRCL**, *"typosquatting finder,"* [Online]. Available: https://typosquatting-finder.circl.lu/.

[61] **ICThealth**, *"Factsheet NVZ: 28% poliklinische zorg is digitaal,"* 26 Juli 2022. [Online]. Available: https://icthealth.nl/nieuws/factsheet-nvz-28-poliklinische-zorg-is-digitaal/.

[62] **NVZ**, *"NVZ Factsheet digitale zorg,"* Juni 2021. [Online]. Available: https://nvz-ziekenhuizen.nl/sites/default/files/2022-10/NVZ%20Factsheet%20Digitale%20Zorg%20juni%202021.pdf.

[63] **Zorgenablers**, *"Remote Consultation,"* 24 November 2021. [Online]. Available: https://zorgenablers.nl/remote-consultation/.

[64] **Zorg Enablers**, *"Remote Monitoring,"* 23 11 2022. [Online].

Available: https://zorgenablers.nl/remote-monitoring/.

[65] **VGZ**, *"Explosieve groei opschaling digitale zinnige zorg,"* 2021. [Online]. Available: https://www.cooperatievgz.nl/cooperatie-vgz/nieuws-en-media/nieuwsoverzicht/explosieve-groei-opschaling-digitale-zinnige-zorg.

[66] **M&I/Partners**, *"Domotica-leveranciers in perspectief,"* 2022. [Online]. Available: https://mxi.nl/uploads/files/publication/domotica-leveranciers-in-perspectief-2022.pdf.

[67] **CISA**, *"Protecting Against Cyber Threats to Managed Service Providers and their Customers,"* 11 Mei 2022. [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/aa22-131a.

[68] **Bleepingcomputer**, *"BIG sabotage: Famous npm package deletes files to protest Ukraine war,"* 9 Januari 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/big-sabotage-famous-npm-package-deletes-files-to-protest-ukraine-war/.

[69] **Bleepingcomputer**, *"Dev corrupts NPM libs 'colors' and 'faker' breaking thousands of apps,"* 9 Januari 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/dev-corrupts-npm-libs-colors-and-faker-breaking-thousands-of-apps/.

[70] **ITPro**, *"Open source packages with millions of installs hacked to harvest AWS credentials,"* 24 Mei 2022. [Online]. Available: https://www.itpro.co.uk/security/hacking/367776/open-source-packages-hacked-to-harvest-aws-credentials.

[71] **Kaspersky**, *"DDoS attacks in Q3 2021,"* 7 November 2022. [Online]. Available: https://securelist.com/ddos-report-q3-2022/.

[72] Overzicht cyberincidenten, 2022. [Online]. Available: https://www.datalekt.nl/home/overzicht-cyberincidenten/.

[73] **M. Ulikowski**, *"dnstwist,"* 2022. [Online]. Available: https://github.com/elceef/dnstwist.

[74] **FBI**, *"Hacktivists Use of DDoS Activity Causes Minor Impacts,"* 4 November 2022. [Online]. Available: https://www.ic3.gov/Media/News/2022/221104.pdf.

[75] **Enisa**, *"ENISA Threat Landscape for Ransomware Attacks,"* 29 Juli 2022. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks.

[76] **CIS**, *"CIS Benchmarks,"* [Online]. Available: https://www.cisecurity.org/cis-benchmarks/. [Accessed 14 December 2022].

[77] **R. Janssen, H. Prins, A. van Hout, J. Nauta, M. Hettinga, L. van der Krieke and S. Sytema**, *"Videoconferencing in Mental Health Care,"* in eTELEMED 2015 : The Seventh International Conference on eHealth, Telemedicine, and Social Medicine, 2015.

[78] *"U.S. Declares Start of Russia's Invasion of Ukraine, Introduces Sanctions; "Cyber Shields Up," Says CISA,"* The American Hospital Association, 23 Februari 2022. [Online]. Available: https://www.aha.org/advisory/2022-02-23-us-declares-start-russias-invasion-ukraine-introduces-sanctions-cyber-shields.

Begrippenlijst

2FA
(Zie tweefactorauthenticatie)

Aanval
Actie waarbij iemand met opzet de beveiliging probeert uit te schakelen of te omzeilen om in een digitaal systeem te komen.

Aanvaller
Iemand die met opzet de beveiliging probeert uit te schakelen of te omzeilen om in een digitaal systeem te komen.

Aanvalsoppervlak
Het gedeelte van IT-systemen dat een aanvaller kan bereiken om zijn aanvallen op te richten.

Actor
Persoon, groep of organisatie die een digitaal systeem dreigt aan te vallen. Voorbeelden zijn: script kiddie, hacktivist, kwaadwillende medewerker, vijandige staat (statelijke actor) of een cybercrimineel (criminele actor).

Administrator
Beheerder van een computersysteem of computernetwerk. Deze persoon heeft meer rechten dan een gewone gebruiker. Zo kan hij bijvoorbeeld instellingen aanpassen en hij bepaalt wat gebruikers in een computernetwerk mogen doen en wat niet.

AI
Artificial Intelligence (ook wel kunstmatige intelligentie, K.I.)

API
Application Programming Interface. Een programma waarmee applicaties onderling kunnen communiceren zonder dat mensen dit aansturen. Veelgebruikte methodes over het internet zijn bijvoorbeeld SOAP en REST.

APT
Advanced Persistent Threat, oftewel de voortdurende dreiging van een geavanceerde tegenstander. Dit zijn met name vijandige staten (statelijke actoren). Er wordt gebruik gemaakt van cyberaanvallen waarbij de aanvaller langere tijd in een informatiesysteem zit, zonder te worden opgemerkt. Of hij probeert langere tijd op allerlei manieren bij bepaalde informatie in het systeem te komen. Vaak wil de aanvaller hiermee informatie stelen of op een zeker moment het netwerk stilleggen. Een APT verschilt van een gewone dreiging door het motief, de vasthoudendheid en soms ook de gekozen middelen van de aanvaller.

BEC
Business E-mail Compromise, oftewel een incident waarbij de aanvaller is doorgedrongen tot de mailomgeving van een organisatie. De aanvaller kan deze toegang gebruiken om vertrouwelijke informatie te stelen of om nieuwe aanvallen mee uit te voeren, zogenaamd uit naam van (iemand van) een organisatie. Een voorbeeld daarvan is CxO-fraude.

Botnet
Een netwerk van computersystemen die zelfstandig kwaadaardige taken uitvoeren, zoals het versturen van spam of het uitvoeren van een DDoS-aanval. Een command-and-control server stuurt dit netwerk aan.

CEO-fraude (ook wel CxO fraude)
Vorm van fraude waarbij een aanvaller e-mails verstuurt aan een financiële afdeling zogenaamd uit naam van de CEO of CFO van een bedrijf. De aanvaller wil hiermee een medewerker van de financiële afdeling overtuigen of onder druk zetten om geld over te maken.

CISM
Certified Information Security Manager. Dit is een certificering voor professionals in informatiebeveiliging.

CISO
Chief Information Security Officer.

Code injection
Een bepaald type aanval op een onveilige plek in een applicatie. Daarbij verandert de aanvaller iets in de code van het systeem waardoor het programma anders werkt. Voorbeeld van een code injection is SQL-injection.

Credentials
De gegevens waarmee een gebruiker of ander computersysteem bij een computersysteem kan aantonen dat hij is wie hij zegt dat hij is. Bijvoorbeeld een gebruikersnaam in combinatie met een wachtwoord of een via SMS opgestuurde code.

Cross site scripting
Veel voorkomende fout in een website waardoor een aanvaller toegang kan krijgen tot gegevens of functionaliteit die niet voor hem bedoeld is.

CVE
Cybersecurity Vulnerabilities and Exposures - lijst van publieke kwetsbaarheden. (https://cve.mitre.org/cve/).

Cybersecurity
Het geheel aan maatregelen om relevante risico's tot een aanvaardbaar niveau te reduceren. De maatregelen kunnen zijn gericht op het voorkomen van cyberincidenten of op het ontdekken van cyberincidenten, het beperken van de schade of het eenvoudiger herstellen na een incident.

CxO-fraude
Zie CEO-fraude.

DDoS
Distributed Denial-of-Service. Aanvallen waarbij digitale diensten onbereikbaar worden gemaakt voor gebruikers. DDoS-services kunnen makkelijk en goedkoop worden afgesloten via het internet (dark web) en maken veelal gebruik van zogenaamde botnets bestaande uit IoT-apparaten.

Defacing
Het bekladden van een website om een eigen bericht te plaatsen. Wordt veelal gebruikt door hacktivisten.

Digitale veiligheid
Het ongestoord functioneren van informatie-en procesbesturingssystemen, daardoor verwerkte en opgeslagen informatie en daarvan afhankelijke diensten en processen.

Digitaal proces
Een proces dat geheel of gedeeltelijk wordt uitgevoerd door de complexe en onderling samenhangende interactie tussen mensen en vele componenten zoals hardware, software en/of netwerken. Volledig geautomatiseerde processen, zoals procesbesturingssystemen, vallen ook onder dit begrip.

Dreiging
Een cyberincident dat zich kan voordoen of een combinatie van gelijktijdige of opeenvolgende cyberincidenten.

Endpoint security
Beveiliging van eindsystemen (PCs, laptops, tablets et cetera) – niet beperkt tot antivirus, maar ook bijvoorbeeld data-leak protection (DLP).

Exploit
Methode (programma of code) die hackers gebruiken om een kwetsbaarheid te misbruiken.

Hacking
We spreken van 'hacking' wanneer het een actor gelukt is de beveiliging te doorbreken en acties uit te voeren op het systeem waarvoor de actor niet geautoriseerd.

Hacktivist
Iemand die digitale aanvallen uitvoert om een bepaalde ideologie te promoten.

Immutable back-up
Een back-upbestand die niet veranderd kan worden zodat een aanvaller deze niet kan versleutelen.

Incident
Een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of via netwerk- en informatie-systemen, in gevaar brengt.

Initial access (initiële toegang)
De aanvaller krijgt een eerste toegang bij het slachtoffer, vaak een account van een medewerker van een organisatie binnen een specifieke applicatie of op een specifieke server. Hiertoe wordt gebruik gemaakt van instrumenten die automatisch scannen op zwakheden in systemen. Ook wordt er veel gebruik gemaakt van (spear)phishing.

Kunstmatige intelligentie
Ook wel AI genoemd, artificial intelligence. Technologie waardoor een systeem het menselijk denkvermogen kan nabootsen zodat het zelfstandig bepaalde menselijke taken kan uitvoeren.

Malware
Kwaadaardige software die aanvallers op een digitaal systeem zetten om er op afstand bij te kunnen, het te vernielen of informatie te stelen. Malware is een samentrekking van het Engelse 'malicious' en 'software'.

Multifactorauthenticatie (MFA)
Zie tweefactorauthenticatie (2FA).

Patch
Nieuwe versie van software of firmware door de producent. Repareert bekende kwetsbaarheden, zorgt eventueel voor nieuwe beveiliging en extra functies.

Phishing
Aanval waarbij de aanvaller iemand verleidt om belangrijke informatie te geven, zoals bijvoorbeeld inloggegevens of creditcardgegevens. Phishing gebeurt vaak via e-mails. Maar aanvallers doen het ook via de telefoon, een sms of een app-bericht.

Privileged Access /account
Account op een digitaal systeem dat meer rechten geeft om bepaalde dingen te doen. Bijvoorbeeld bestanden en instellingen veranderen.
In Windowssystemen heet dit account de administrator of beheerder, in Unix- en Linux-systemen de root.

Responsible disclosure
Actie waarbij een of meer gevonden beveiligingslekken op een verantwoorde manier bekend worden gemaakt. Meestal meldt men het lek eerst bij de eigenaar van het systeem waar het is gevonden zodat de kwetsbaarheid kan worden verholpen.

Risico
De kans dat een dreiging leidt tot een cyberincident en de impact van het cyberincident op belangen, beide in relatie tot het actuele niveau van digitale weerbaarheid.

SaaS (Software-as-a-Service)
Een vorm van het uitbesteden van diensten. Bij SaaS wordt software aangeboden als een online dienst. Op een zelfde wijze spreken we ook van bijvoorbeeld IaaS (Infrastructure as a Service) , PaaS (Platform as a Service) en DRaaS (Data Recovery as a service).

SBoM
Software Bill of Materials (SBoM). Een lijst van welke versie van componenten in de software zit.

Security-by-design
Het afdwingen, zowel technisch als organisatorisch, van een zorgvuldige omgang met gegevens vanaf de ontwerpfase van een systeem.

Spear phishing
Een phishing-aanval die gericht is op een bepaald persoon. Soms is de aanval ook speciaal aangepast voor deze persoon. Daardoor is het heel moeilijk om te herkennen dat het een phishing-aanval is.

Statelijke actor
Een land dat digitale aanvalsmiddelen inzet voor spionage en sabotage en/of voor het verspreiden van desinformatie.

Uitval
Een situatie waarin één of meer digitale processen zijn verstoord als gevolg van natuurlijke of technische oorzaken of als gevolg van menselijke fouten.

Verstoring
Een belemmering in de beschikbaarheid, integriteit of vertrouwelijkheid van informatie(verwerking). Met andere woorden: uitval van digitale processen of onderdelen daarvan.

Tweefactorauthenticatie (2FA), ook wel multifactorauthenticatie (MFA) genoemd
Methode om vast te stellen of een gebruiker of digitaal systeem wel is wie of wat hij zegt te zijn. Je gebruikt hiervoor verschillende manieren. Bijvoorbeeld een wachtwoord en een code die de gebruiker per sms krijgt. Of een combinatie van een vingerafdruk en een wachtwoord.

Vulnerability scan
Kwetsbaarheden scan - Een geautomatiseerde controle die zwakke plekken in een systeem opspoort.

Wipersoftware
Een variant van malware die essentiële bestanden op een computer beschadigt of verwijdert waardoor de computer niet meer werkt.

Zero-day aanval
Aanval of aanvalsmethode die misbruik maakt van een kwetsbaarheid (de zero-day kwetsbaarheid) die nog niet bekend is bij anderen (zoals een leverancier of gebruiker), waardoor er nog geen patch beschikbaar is.

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.

Ook zijn we een speciale dank verschuldigd aan de **Financial ISAC en TNO** voor het gebruik van hun model, dat is gebaseerd op het FAIR (Factor Analysis of Information Risk) framework (https://www.fairinstitute.org).

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

Vragen of opmerkingen?
info@z-cert.nl
033 737 06 09

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

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