WHITE PAPER

ZORRO

Red Teaming in de Zorg

Securify

Versterken van Cyberweerbaarheid bij het Antoni van Leeuwenhoek ziekenhuis op basis van het ZORRO Framework

In een tijd waarin cyberaanvallen en gegevensdiefstal gemeengoed zijn geworden, staat de gezondheidssector voor een uitdaging. Ziekenhuizen houden zich 24 uur per dag bezig met het verlenen van medische hulp, het waarborgen van de privacy en veiligheid van patiëntgegevens en het draaiende houden van de dagelijkse operaties, zodat ze voortdurend patiënten kunnen blijven bedienen. Het is inmiddels een feit geworden dat de gezondheidssector waakzaam moet zijn tegen cybercriminelen, continu moet innoveren op het gebied van IT en passende maatregelen moet treffen. Maar hoe beoordeel je de implementatie van preventie-, detectie- en responsmaatregelen en daarmee de weerbaarheid van een hele organisatie?

Het Antoni van Leeuwenhoek ziekenhuis (AVL) is hier enkele jaren geleden mee begonnen door zowel op het vlak van preventie, als detectie en response de algehele weerbaarheid tegen cyberaanvallen te verhogen. In 2021 heeft het AVL besloten om hun algehele weerbaarheid in kaart te brengen door het te toetsen middels een Red Teaming oefening. Hiervoor heeft het AVL zowel Securify als Stichting Z-CERT ingeschakeld om een Red Teaming oefening[1] uit te voeren volgens de richtlijnen van het toentertijd door Z-CERT nieuw ontwikkelde ZORRO-framework (Zorg Redteaming Resilience Oefening).

Actuele dreigingen in de zorg en toekomstige trends

Jaarlijks beschrijft Z-CERT de belangrijkste actuele gevaren voor de Nederlandse zorgsector in de vorm van een dreigingsbeeldrapport. Zo was dit jaar terug te vinden in het Cybersecurity Dreigingsbeeld voor de zorg (2023)[2], dat de gezondheidssector steeds vaker slachtoffer is van supplychain-aanvallen. Z-CERT hoopt dan ook dat met de komst van de strengere verplichtingen omtrent informatiebeveiliging door de Europese NIS2-wetgeving, zorginstellingen gaat helpen om leveranciers te verplichten een veiligere dienstverlening te leveren.

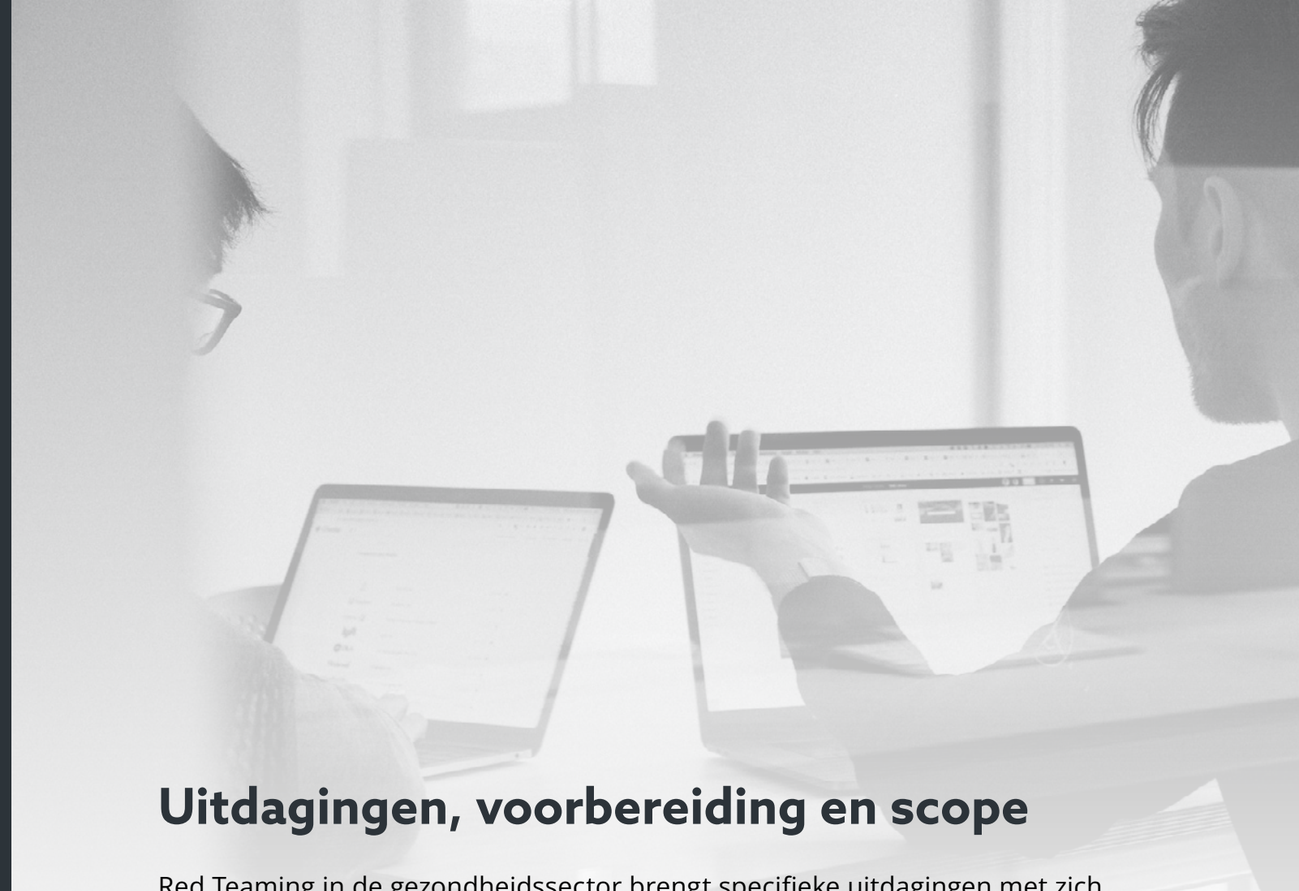
Tevens ziet Z-CERT dat het aantal succesvolle ransomware aanvallen, waarbij (medische) data gegijzeld wordt gehouden tegen losgeld, in de wereldwijde zorg in 2023 flink is toegenomen. Hoewel deze trend vooralsnog niet één-op-één vertaalt naar Nederland, verwacht Z-CERT dat de dreiging voor de gezondheidssector wel snel zal toenemen. Doordat aanvallers steeds sneller zijn in het misbruiken van kwetsbaarheden en nieuwe phishingtechnieken, welke mogelijk versterkt worden door de komst van generatieve AI, voorspelt Z-CERT vele ransomware pogingen en enkele grote incidenten voor 2024.

[1] https://z-cert.nl/eerste-red-teaming-oefening-antoni-van-leeuwenhoek-ziekenhuis-en-z-cert/
[2] https://z-cert.nl/cybersecurity-dreigingsbeeld-voor-de-zorg-2023/

TIBER VS. ZORRO

Het ZORRO-framework is een afgeleide van het succesvolle TIBER-framework (Threat Intelligence Based Ethical Red Teaming), dat al geruime tijd toegepast wordt in de financiële sector. Toch zien we wel een aantal verschillen tussen een ZORRO-oefening en een TIBER oefening. Bij TIBER speelt De Nederlandse Bank (DNB) als een onafhankelijke externe te allen tijde de rol als toezichthouder, waarbij Z-CERT deze rol op zich neemt voor bij ZORRO-oefeningen. Z-CERT levert ook het Threat Intelligence (TI) rapport waarbij de zorg specifieke dreigingsactoren onder andere worden omschreven, waarbij het TI-rapport bij een TIBER-oefening door een externe onafhankelijke leverancier opgesteld moet worden.

Verder zit er ook een verschil in de doorlooptijd door verschillende redenen. Bij een TIBER oefening zijn er minimaal twee verschillende scenario's verplicht, ten opzichte van één scenario bij een ZORRO-oefening. Tevens merk je dat zorginstellingen minder hevige of andere detectie en responsmaatregelen heeft ten opzichte van een financiële organisatie. Dit zorgt ervoor dat het Red Team over het algemeen sneller en efficiënter kan werken. Daarnaast kan de keuze worden gemaakt om sneller gebruik te maken van een zogeheten 'leg-up', wanneer de opdrachtgever het Red Team een stapje dichter bij het doel brengt en het proces versneld. Dit kan bijvoorbeeld door over te schakelen naar een 'assume breach' aanpak, waarbij wordt aangenomen dat een aanvaller uiteindelijk toch toegang (foothold) zal weten te verkrijgen.



Uitdagingen, voorbereiding en scope

Red Teaming in de gezondheidssector brengt specifieke uitdagingen met zich mee, aangezien de continuïteit van de bedrijfsvoering van een zorginstelling, in dit geval een ziekenhuis, te allen tijde moet worden gehandhaafd. Om dit te bewerkstelligen zijn nauwe communicatielijnen tussen het White Team en het Red Team van uiterst belang. Het is in dergelijke exercities zaak dat veel acties die het Red Team op elk moment uitvoert, eerst zijn besproken en goedgekeurd door het White Team, zodat het ziekenhuis operationeel blijft.

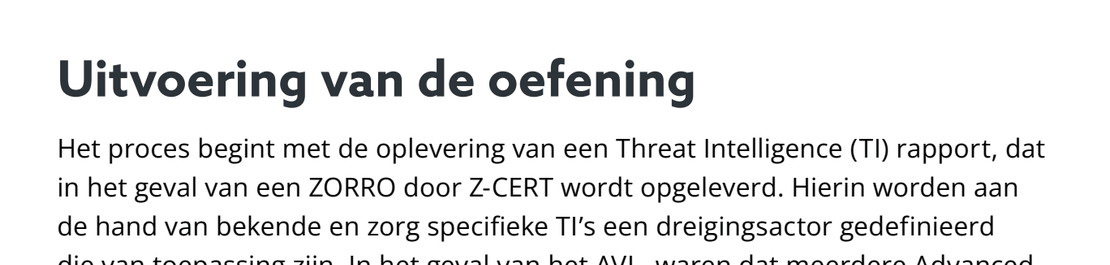
Een voorbeeld hiervan is dat er bij de exercitie met het AVL zogeheten Subject-Matter Experts (SME) van elke afdeling werden aangesteld. Op het moment dat het Red Team bepaalde acties zou uitzetten die invloed kon hebben op bijvoorbeeld specifieke apparatuur, zou er een specifiek tijdslot worden afgestemd voor het uitvoeren van deze acties binnen een sector of technologie.

Een ander belangrijk onderdeel binnen dit proces is het afstemmen van de scope (reikwijdte en afbakening) in samenwerking met de zorginstelling. Zo waren bij de exercitie enkele afdelingen buiten scope gesteld in verband met de gevoeligheid en geheimhouding van bepaalde data of de continuïteit en beschikbaarheid van deze afdelingen. De scope omvatte niet alleen welke onderdelen binnen of buiten de reikwijdte van de test vielen, maar ook welke specifieke bevindingen direct gemeld moesten worden aan het AVL.

Uitvoering van de oefening

Het proces begint met de oplevering van een Threat Intelligence (TI) rapport, dat in het geval van een ZORRO door Z-CERT wordt opgeleverd. Hierin worden aan de hand van bekende en zorg specifieke TI's een dreigingsactor gedefinieerd die van toepassing zijn. In het geval van het AVL, waren dat meerdere Advanced Persistent Threat (APT) actoren, zoals een georganiseerde criminele organisatie of een groep aanvallers die uit naam van een staat of een staatgefundeerde groep opereren. Aan de hand van deze actor(en) worden de bijbehorende tactieken, technieken en procedures (TTP's), die omschreven worden in het MITRE ATT&CK-framework[3], door het Red Team gehanteerd. Dit maakt een Red Teaming oefening zo realistisch mogelijk omdat bestaande en actuele dreigingen en mogelijke aanvalsscenario's realistisch gesimuleerd worden.

Een ZORRO-oefening omvat meerdere gestructureerde fasen die door het Red Team worden gehanteerd om een inzicht te krijgen in zowel de technische als organisatorische beveiligingsmaatregelen. Binnen die fasen worden specifieke acties die overeenkomen met het verloop van acties van een daadwerkelijke cyberaanval, ook wel bekend als de Unified Kill Chain[4] (zie hiervoor onderstaande afbeelding).



CHAIN MODEL: UNIFIED CYBER KILL

Het Red Team van Securify speelt de rol van de aanvaller en test zowel de technische als organisatorische beveiligingsmaatregelen van het Blue Team, in dit geval het AVL en het Security Operations Center (SOC). Waarbij onder andere de Elektronische Patiënten dossiers (EPD) het doelwit waren. De uitwerking van bovenstaande fasering bij een ZORRO-oefening kan er uitzien zoals de afbeelding op de volgende pagina:

[3] https://attack.mitre.org/
[4] https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf

Ter aanvulling op de Unified Kill Chain maakt Securify gebruik van één additionele fase, namelijk een kennisoverdracht fase. Deze fase wordt gezien als het afronden van het onderzoek, maar is misschien wel het belangrijkste onderdeel van de gehele exercitie. In deze fase worden de ruwe logging van het Red Team en het eindrapport opgeleverd en kunnen er onderdelen nog worden herhaald in het bijzijn van het Blue Team. Het Red Team zal vervolgens de opgedane kennis overdragen aan het Blue Team om zo de zorginstelling te helpen bij het verhogen van de algehele weerbaarheid tegen cyberaanvallen op het gebied van preventie, detectie en respons.

IN

Initial Foothold

Een aanvaller onderzoekt welke medewerkers mogelijk toegang hebben tot gevoelige gegevens en probeert daarvan via één of meerdere technieken toegang tot de inloggegevens te krijgen.

THROUGH

Network Propogation

De aanvaller gebruikt de inloggegevens op meerdere online diensten, waarmee uiteindelijk toegang wordt verkregen tot een systeem met gevoelige informatie. Dit ondanks de beveiliging met 2FA. Bijvoorbeeld door op logische tijden in te loggen, waarbij een medewerker onterecht op akkoord klikt op een authenticatieverzoek.

OUT

Action on Objectives

De aanvaller maakt een kopie (als voorbeeld) van deze gegevens en stuurt een dreigingsbericht naar de organisatie waarin staat deze te publiceren wanneer er niet ingegaan wordt op het betalen van losgeld.

Lessons learned

Securify is van mening dat met de komst van ZORRO er een goede start is gemaakt om de gezondheidssector weerbaarder te maken tegen realistische cyberaanvallen. Wij verwachten dat er veel organisaties in de komende jaren zullen volgen en dat staat Securify klaar om hen daarbij te helpen. Deze eerste oefening van het ZORRO framework bij het AVL is dan ook naar ons idee het perfecte bewijs daarvan. Met behulp van de resultaten van de oefening die het Red Team van Securify in kaart heeft gebracht, kon het AVL de nodige stappen ondernemen om het algehele beveiligingsniveau tegen cyberaanvallen te verhogen. De waardevolle TI-informatie, expertise binnen de gezondheidssector en de continue begeleiding van Z-CERT hebben ook een grote rol gespeeld in het succesvol maken van deze exercitie.

Desondanks zullen aanvalsactoren/dreigingsactoren blijven binnen proberen te komen in de gezondheidssector. En gezien de gevoeligheid en essentie van de sector, zullen ZORRO-oefeningen nog door veel meer instanties moeten worden uitgevoerd.

LESSONS LEARNED VOOR HET AVL

Voor het AVL was de uitslag van de oefening duidelijk en wisten ze waar ze goed in waren bij het verdedigen tegen een daadwerkelijke aanval en waar nog verbetering in lag. ”De waarde van een Red Teaming oefening zit hem er juist in dat je een realistisch beeld krijgt van hoe de organisatie reageert als ze écht wordt aangevallen. Red Teaming is dan ook een waardevolle toevoeging in de Cyber-security-gereedschapskist”, aldus Joost Boele, CISO (Chief Information Security Officer) bij het AVL.

WAT IS DE TOEKOMST VAN ZORRO?

De ZORRO oefening bij het AVL was de eerste die was uitgevoerd. Inmiddels zijn er enkele ander zorginstellingen die ook een ZORRO-oefening hebben laten uitvoeren. Het framework is de afgelopen jaren aanzienlijk doorontwikkeld en is woensdag 10 april 2024 officieel gepubliceerd door Z-CERT. Wij kunnen stellen dat Z-CERT een adequaat framework heeft neergezet waar de gezondheidssector de komende jaren de vruchten van gaat plukken. Het is een goed middel dat specifiek afgestemd is op de sector en in ons optiek cruciaal vanwege de gevoeligheid van de (medische)gegevens en het belang van de continuïteit van de bedrijfsvoering.

Met de opkomst van nieuwe EU-wet- en regelgeving, zoals de Digital Operational Resilience Act (DORA), hebben verschillende instanties gewerkt aan de ontwikkeling van een vergelijkbaar framework dat toegankelijker moet zijn voor kleinere instellingen dan het TIBER-framework. Dit heeft geleid tot de ontwikkeling van het Advanced Red Teaming framework (ART)[5]. Door de minder strenge regelgeving en toezichthouding is ART ook aanzienlijk goedkoper, waardoor het een haalbare optie wordt voor kleinere instellingen.

[5] https://www.digitaleoverheid.nl/wp-content/uploads/sites/8/2023/03/75856-BZK-Red-Teaming-ART-raamwerk_PDFUA.pdf