Shared Research Programma Cybersecurity

Het is alweer meer dan twee jaar geleden dat dit magazine aandacht besteedde aan het Shared Research Programma Cybersecurity (SRP). In 2019 is het eerste SRP-lustrum gevierd met een event in Utrecht en is het tweede SRP-magazine verschenen (1). Het is nu een goed moment om een update te geven over hoe het SRP zich heeft ontwikkeld en om een drietal projectresultaten toe te lichten.

Door: Reinder Wolthuis (TNO)

In 2018 heeft ook de Volksbank zich aangesloten. TNO werkt dus met drie grootbanken (Rabobank, ABN AMRO en ING), Achmea en de Volksbank samen om de Nederlandse samenleving te wapenen tegen cyberaanvallen van vandaag en morgen. Het doel is het creëren van een veilige en veerkrachtige digitale samenleving door innovatie op het gebied van cybersecurity. De belangrijkste voordelen van de samenwerking in het SRP zijn een 'shared workload', 'shared data' en 'shared funding'. Met andere woorden: de partners zijn actief in de projecten betrokken, delen (geanonimiseerde) data om ontwikkelde innovaties te evalueren en hebben een aandeel in de financiering. Ook de Nederlandse overheid levert een aanzienlijke financiële bijdrage.

Menselijke factor

Nieuw sinds 2017 is dat de menselijke factor uitdrukkelijker in het onderzoeksprogramma aan bod komt. Aangezien de mens een belangrijke rol speelt in de cyberverdediging is het belangrijk om meer inzicht te creëren in hoe de mens (in de rol van slachtoffer, verdediger dan wel aanvaller) denkt, handelt en kan worden beïnvloed.

Wat gebleven is, zijn de mooie projecten met mooie resultaten die over een breed palet van securitygebieden de beheersing over cyberrisico's en -verdediging tegen aanvallen verbeteren. Die resultaten bestaan uit nieuwe en betere inzichten, methodieken of tools.

Deze resultaten worden zo breed mogelijk gedeeld.

Er wordt op dit moment gesproken over de programma-invulling in de komende jaren. Daarin ligt nog meer de nadruk op open samenwerking met andere partijen, snel kunnen acteren op ontwikkelingen in de omgeving, een structureel en continu innovatiemanagementproces en veel communicatie naar en zichtbaarheid in de maatschappij. Nadrukkelijk worden hierbij ook partijen uitgenodigd om aan te sluiten, expliciet ook uit andere sectoren dan de financiële sector.

Hieronder drie inhoudelijke resultaten vanuit het SRP-cybersecurity:

- het cybergedrag van bankmedewerkers;
- self-healing;
- threat landscaping.

Meer informatie is op de website te vinden (2).

Door: Rick van der Kleij (TNO)

Cybergedrag van bankmedewerkers

Banken nemen geavanceerde technische maatregelen om cybercriminaliteit buiten de deur te houden. In het verleden is gebleken dat technische maatregelen alleen niet voldoende zijn om criminaliteit of cyberincidenten te voorkomen. Incidenten vinden hun oorsprong veelal in het gedrag van medewerkers. Zo is bekend dat een groot deel van medewerkers hun wachtwoorden hergebruiken (50-

Medewerkers maken vaak bewust de keuze om bestanden niet te versleutelen

60%) of delen (30-95%). Dit maakt de banksystemen kwetsbaar voor hacking. Om de digitale veiligheid van banken te vergroten is het dus van belang dat er ook wordt gekeken naar het gedrag van de eigen medewerkers.
De meest gebruikte manieren om medewerkers te motiveren om zich cyberveilig te gedragen zijn het opstellen van gedragsvoorschriften of het houden van bewustmakingscampagnes. Voorschriften bepalen de verantwoordelijkheden van werknemers bij het voorkomen van incidenten. Deze voorschriften zijn echter vaak gebrekkig van opzet. Bijvoorbeeld omdat de verantwoordelijkheden van werknemers niet goed zijn afgestemd op de productiviteitsdoelen van werknemers. Dit leidt ertoe dat werknemers procedures omzeilen of minder veilig maar productiever beveiligingsgedrag aannemen. Ook bewustmakingscampagnes zijn veelal onsuccesvol. Meestal omdat zij zijn gebaseerd op onjuiste veronderstellingen over waarom mensen zich wel of niet veilig gedragen. Bewustmakingscampagnes worden bijvoorbeeld vaak gelanceerd vanuit de veronderstelling dat kennis over cybersecurity ontbreekt. Terwijl in feite andere factoren leiden tot niet-naleving van het beleid, zoals slecht ontworpen beveiligingsmaatregelen of een hoge werklast.

Systematisch standpunt

Daarom moeten we eerst begrijpen waarom werknemers zich al dan niet veilig gedragen. Op basis van deze inzichten kunnen we dan interventies ontwikkelen die de oorzaken wegnemen van het onveilige gedrag. Het hebben van een systematisch standpunt over de verschillende soorten cybergedrag die werknemers wel of niet uitvoeren en de redenen daarvoor, is naar onze mening de eerste stap bij het tegengaan van incidenten en het bevorderen van cyberveilig gedrag op de werkvloer.
Samen met de SRP-partners hebben we gekeken naar het securitygedrag van hun medewerkers. Hiermee hebben we verschillende vragen beantwoord. Wat is cyber(on)veilig gedrag? Hoe (on)veilig gedragen medewerkers zich? Hoe meet je cyberveilig gedrag? Ook hebben we gekeken naar de bronnen die het cyberveilig gedrag van medewerkers frustreren. Dit met het oog op het ontwikkelen van interventies in een later stadium. De achterliggende vraag was: hoe kunnen we medewerkers helpen in het bereiken van hun zakelijke doelen op een veilige manier? Hierbij hebben we een gedragsmodel gebruikt dat stelt dat gedrag ontstaat door een samenspel tussen kennis van medewerkers, de gelegenheid voor veilig gedrag en de motivatie die medewerkers hebben om zich veilig te gedragen.
We hebben zeven clusters van cybergedrag geïdentificeerd via interviews en documentstudie. Een belangrijk cluster is 'omgaan met vertrouwelijke informatie'. Hierbinnen vallen specifieke gedragingen zoals 'het versleutelen van informatie met speciale software' en 'het waarborgen van correcte adressering van elektronische berichten'. We vroegen meer dan 2000 medewerkers binnen de banken vervolgens hoe zij omgaan met vertrouwelijke informatie. Daarnaast vroegen we ook naar hun kennis, motivatie en de gelegenheid die door de bank wordt geboden om op een juiste manier om te gaan met informatie.
Over het algemeen genomen zien we dat medewerkers zich veilig gedragen. Er zijn bovendien geen opmerkelijke verschillen tussen de banken. Alleen het versleutelen van vertrouwelijke informatie blijft achter. Medewerkers weten hoe ze dit moeten doen en encryptiesoftware is voor handen, maar, zo laten medewerkers ons weten, het versleutelen van bestanden is te moeilijk, het stoort te veel met het werk. Medewerkers maken vaak bewust de keuze om bestanden niet te versleutelen, bijvoorbeeld als deze gedeeld moeten worden met anderen. Een kansrijke oplossingsrichting lijkt dan ook te liggen in het (her)ontwerp van veiligheidsmaatregelen. Door security mensvriendelijker te maken kunnen we medewerkers helpen in het bereiken van hun zakelijke doelen op een meer veilige manier.

Door: Bart Gijsen (TNO)

Self-healing

Cybersecurityonderzoek zorgt ervoor dat organisaties beter bestand zijn tegen moderne cyberaanvallen. Dit neemt echter niet weg dat ook aanvallers hun technieken voortdurend vernieuwen. Ze ontdekken en misbruiken nieuwe

kwetsbaarheden (zero-day exploits) in de ICT-middelen van organisaties en maken steeds meer gebruik van geautomatiseerde aanvalstechnieken. Deze vicieuze cirkel van cyberaanval en -verdedigingstechnieken leidt tot een voortdurende toename van kosten en toenemende inzet van experts. Daarnaast vergen deze ontwikkelingen ook een steeds kortere reactietijd van de experts in de SOC's. In het SRP-onderzoek naar self-healing for cybersecurity (SH4CS) is daartoe de vraag op langere termijn geadresseerd op welke wijze deze vicieuze cirkel doorbroken zou kunnen worden.

De term self-healing werd geruime tijd geleden geïntroduceerd in een visie om ICT-systemen te ontwikkelen die autonoom (zonder menselijke interventie) in staat zijn om zich aan te passen aan factoren die de beoogde werking van het systeem verstoren. Inspiratie voor de ontwikkeling van self-healing-systemen komt voort uit de analogie met biologische mechanismen, zoals het menselijk immuunsysteem. In feite is het immuunsysteem ook verwikkeld in een vicieuze cirkel, vechtend tegen aanvallen van bestaande en muterende virussen, bacteriën, parasieten en schimmels. In het SH4CS-onderzoek is een parallel getrokken tussen het menselijk immuunsysteem en hedendaagse cyberdefensieve maatregelen. Daaruit zijn een aantal opvallende aspecten naar voren gekomen die nieuwe inzichten verschaffen hoe de cyberdefensieve maatregelen op een andere, meer autonome manier kunnen worden ingericht.

Een van deze inzichten is de constatering dat bij ICT-systemen en netwerken de disposability eigenschap ontbreken waarover menselijke cellen wél beschikken: een lichaam blijft gezond als (in beperkte mate) zijn cellen sterven. Het immuunsysteem gebruikt deze eigenschap door voortdurend cellen te vernietigen, met een voorkeur voor cellen die geïnfecteerd zijn of zich niet-lichaam-eigen gedragen. De meeste ICT-systemen missen deze disposibility eigenschap. Ze zijn niet ontworpen om voortdurend (en zonder specifieke reden) systeemonderdelen te termineren en nieuwe onderdelen op te starten. Dit strookt ook niet met de traditionele opvatting over ICT-beheer. Met recentere DevOps-methoden en -technieken dient zich echter wel de mogelijkheid aan om 'regeneratieve ICT-infrastructuur' te realiseren.

In het SH4CS-onderzoek is op basis van Kubernetes technologie een experiment ontwikkeld om het concept van regeneratieve containers (die gebruikt worden om IT-applicaties uit te voeren) te demonstreren en beproeven. Dit experiment demonstreert hoe het container-opstartproces en container-terminatieproces de verspreiding van malware-infecties van de containers kan beperken en de detecteerbaarheid kan verhogen (doordat de infectie steeds opnieuw verspreid moet worden naar 'geschoonde' containers). In geval van een detecteerbare infectie kan de verspreiding zelfs autonoom (dat wil zeggen: zonder betrokkenheid van experts) beëindigd worden door een versnelling van het container-terminatieproces.

Dit vooralsnog eenvoudige experiment is de eerste stap richting het ultieme doel om de benodigde, schaarse cyberdefensieve expertise in de vicieuze cirkel te minimaliseren. Uiteraard is SH4CS geen wondermiddel dat alle cybersecurityproblemen oplost, maar zal het eerder een bruikbare aanvulling zijn op andere oplossingen. Ook wordt momenteel onderzocht onder welke omstandigheden het middel wellicht erger kan zijn dan de kwaal, zoals er ook door het menselijk immuunsysteem gezondheidsrisico's op kunnen treden. Verder onderzoek zal uitwijzen of en hoe de toepassing van SH4CS zal bijdragen aan de 'battle of the cyber fittest'.

Door: Richard Kerkdijk(TNO) en Maarten Jak (ING)

Threat landscaping

Met de term 'threat landscape' (dreigingslandschap) wordt in essentie gedoeld op een naar prioriteit gerangschikt overzicht van (cyber)dreigingen waarop een organisatie zich moet voorbereiden. In dit project is een methode ontwikkeld om een dergelijk dreigingslandschap af te leiden uit (cyber)dreigingsinformatie en incidentgegevens die een organisatie in de loop der tijd heeft verzameld. Belangrijk uitgangspunt was om daarmee tot een dreigingslandschap te komen dat specifiek is toegespitst op de individuele organisatie die het samenstelt. Dit vanuit de filosofie dat organisaties als ABN AMRO, ING, Rabobank en Volksbank vanuit hun uiteenlopende bedrijfsprofielen een evenzo uiteenlopende waardering van (het belang van) specifieke dreigingen zullen hebben.

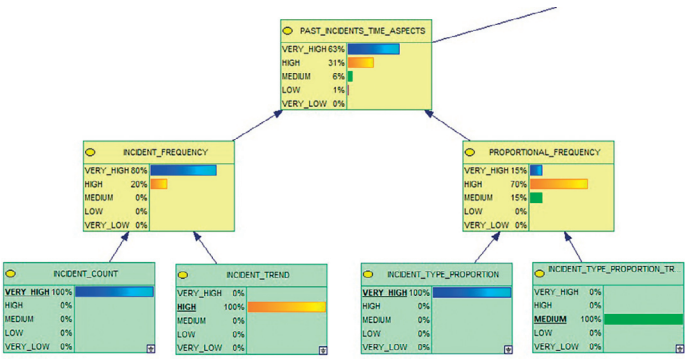
Het concept van een dreigingslandschap is niet nieuw, verscheidene leveranciers en ook organisaties als ENISA publiceren met enige regelmaat overzichten van (ontwikkelingen in) cyberdreigingen die zij belangwekkend achten. Dergelijke rapportages bieden weliswaar nuttige informatie, maar zijn in de regel te generiek om richting te geven aan de cybersecurityaanpak van een individuele organisatie. Bovendien is het begrip 'dreiging' niet altijd eenduidig afgebakend, hetgeen leidt tot inconsistente overzichten van actoren, aanvalsmethoden en meer algemene trends op het gebied van technologie en (cyber)security. Om hier meer lijn in te brengen, is vroeg in het project besloten om het top level dreigingslandschap met zogeheten campaigns (3) te bevolken en deze consis-

tent als (campaign) by (threat actor (type)) te formuleren. Deze ontwerpkeuze legt de focus op het eindspel van aanvallers en leidt tot items als (targeted ransomware) bij (Gogalocker) en (manipulation of payment applications) by (Carbanak Group). Onderliggende kenmerken zoals de capaciteiten en werkmethoden van een threat actor zijn daarbij uiteraard wel van belang, enerzijds om de ernst van een dreiging op waarde te schatten en anderzijds om in de informatiebehoeften van specifieke belanghebbenden te voorzien. Met het oog op het laatste zou het dreigingslandschap bijvoorbeeld ook een rangschikking van meest relevante aanvalsmethoden kunnen bieden.

FAIR

De grootste uitdaging in dit onderzoek was om observatiegedreven en bij voorkeur rekenkundig vast te stellen welke prioriteit aan de verschillende dreigingen in het dreigingslandschap moet worden toegekend. De in het FAIR (4) (Factor Analysis of Information Risk)-raamwerk beschreven taxonomie voor cybersecurityrisico's bleek hier een geschikt vertrekpunt voor te bieden. In samenwerking met de betrokken banken zijn de verschillende elementen van FAIR vertaald naar de context van een (cyber)dreigingslandschap. Hiertoe is onder meer gekeken naar enkele historische campaigns en de factoren die verschillende banken mee hebben gewogen bij het beoordelen daarvan. Op basis hiervan is een eerste set van 26 threat metrics gedefinieerd aan de hand waarvan een algehele threat score voor specifieke campaigns kan worden bepaald. In lijn met de FAIR-structuur reflecteren deze metrics niet alleen de kans dat een organisatie met een campaign te maken zal krijgen (5), maar ook de mate waarin weerstand tegen die dreiging kan worden geboden (6) en de impact van een eventueel incident. Voor het berekenen van de threat score is een zogeheten Bayesian Belief Network (7) samengesteld (zie figuur 1). Veel van de gedefinieerde threat metrics hebben een organisatie-specifiek karakter, waarmee het doel om het dreigingslandschap op individuele organisaties toe te spitsen is gerealiseerd. In totaliteit is de structuur van threat metrics wel relatief complex geworden. Het idee is echter om kwantificeren van deze metrics verregaand te automatiseren, niet in de laatste plaats om de threat score met enige regelmaat te kunnen verversen. Veranderingen op specifieke metrics kunnen immers tot een herschikking van dreigingen en daarmee een heroverweging van prioriteiten leiden. Punt van aandacht is dat voor de hand liggende bronsystemen (denk aan CTI-platformen (8), incidentregistratiesystemen en SIEMs (9)) niet vanzelfsprekend op deze automatiseringsslag zijn voorbereid. In samenspraak met de betrokken banken zal moeten worden nagegaan hoe de benodigde brongegevens structureel en maximaal efficiënt verzameld kunnen worden.

Parallel aan dit SRP-project liep vanuit de grootbanken het zogeheten '1-FTNL-initiatief' om tot een eenduidig (cyber)-dreigingslandschap voor de financiële sector als geheel te komen. Met dit traject is nauw samengewerkt, onder meer om onderlinge consistentie in terminologie en formats te garanderen. De in SRP verband ontwikkelde structuur van threat metrics wordt naar alle waarschijnlijkheid ook door dit sectorale initiatief omarmd, hetgeen de onderlinge synergie nog verder kan verstevigen.



Figuur 1 - De figuur toont een selectie van de totale set aan threat metrics.

Referenties

(1) https://www.tno.nl/media/14237/srp_magazine_-_editie_2019.pdf).

(2) https://www.tno.nl/srpcybersecurity

(3) Met campaign wordt gedoeld op een set van activiteiten (feitelijk incidenten) die een threat actor met specifieke aanvalstechnieken verricht om een bepaald doel te bereiken

(4) Zie https://www.fairinstitute.org/

(5) Dit wordt onder meer afgeleid uit de (veronderstelde) doelstellingen van de threat actor en de frequentie en geografische kenmerken van recente incidenten.

(6) Deze metrics appelleren onder meer aan detectiemogelijkheden en de mate waarin sprake is van specifieke kwetsbaarheden die de threat actor kan misbruiken.

(7) Een wiskundige methode om met kansverdelingen te redeneren, zie https://en.wikipedia.org/wiki/Bayesian_network

(8) Cyber Threat Intelligence

(9) Security Information and Event Management