Een robuustere cybersecurity

HSD CISO Whitepaper

The Hague Security Delta

Inhoudsopgave

1. Inleiding *2*
2. De CISO *3*
Werkzaamheden en verantwoordelijkheden 3
Het CISO spectrum 3
3. Intersectorale CISO intervisie *5*
High level CISO sessies 5
Thema's 6
4. Resilience en robuustheid bij langdurige ICT uitval *7*
Resilience versus robuustheid 7
Maersk 8
Digitale ontwrichting 8
Voorbeelden van robuustheid 8
5. Uitkomsten *10*
Directie 10
Oefenen 11
Techniek 11
Opleiden 12
Overheid 13
6. Conclusie *14*
7. Literatuur *15*
Bijlage: Vraagstelling en werkwijze *16*
Vraagstelling 16
Werkwijze 16
Bijlage: algemene bevindingen *18*

1. Inleiding

HSD is in de tweede helft van 2018 begonnen met de organisatie van intersectorale CISO/CIO intervisie-meetings. Hiervan hebben er bij het schrijven van dit whitepaper acht plaatsgevonden. Op deze meetings wisselen CISO's en CIO's ervaringen uit en leren ze van elkaar. Dit gebeurt aan de hand van een thema of door de deelnemers ingebrachte aandachtspunten. De deelnemende partijen aan deze meetings komen uit bedrijfsleven, overheid en onderzoeksinstellingen en willen van elkaar leren om gezamenlijk een bijdrage te leveren aan een veiliger wereld.

In dit whitepaper beschrijven we de gemene deler en lessons learned van deze intervisie-meetings. Gezien het vertrouwelijke karakter van de meetings zullen de in dit whitepaper opgenomen bevindingen niet herleidbaar zijn naar de bron. De bevindingen en aanbevelingen uit dit whitepaper zijn een samenvoeging van de uitkomsten van verschillende CISO-groepen. Meningen en uitspraken zijn steeds op persoonlijke titel gedaan en worden niet noodzakelijkerwijs door alle aanwezige CISO's ondersteund.

In hoofdstuk 2 wordt de rol van de CISO besproken, in hoofdstuk 3 behandelen we de opzet van de door HSD georganiseerde high level CISO intervisie-bijeenkomsten met in hoofdlijnen de onderwerpen die daar besproken worden of op de rol staan. In hoofdstuk 4 beschrijven we één van deze onderwerpen: de prangende en steeds relevantere vraag hoe we ons kunnen voorbereiden op het voor onbepaalde tijd uitvallen van de ICT infrastructuur. In dit hoofdstuk geven we achtergrond en voorbeelden bij dit vraagstuk, om vervolgens in hoofdstuk 5 de uitkomsten te beschrijven van de verschillende CISO-intervisiegroepen die over dit vraagstuk gesproken hebben. Dit hoofdstuk zoomt in op de verschillende facetten van het vraagstuk en bevate wensen, uitdagingen en aanbevelingen vanuit de verschillende CISO intervisiegroepen.

Tenslotte sluiten we in hoofdstuk 6 af met een korte conclusie. De bijlagen beschrijven de gekozen opbouw van de CISO-bijeenkomsten die over het thema van dit whitepaper gingen plus een aantal noemenswaardige algemene bevindingen.

2. De CISO

Het belang van information security in de sterk gedigitaliseerde wereld is in de afgelopen decennia sterk toegenomen en zal het komende decennium verder stijgen. Een continue stroom voorbeelden van cyberaanvallen die complete instellingen lamleggen onderstrepen dit belang. Het is dan ook niet verrassend dat steeds meer bedrijven en instellingen een CISO (Chief Information Security Officer) of zelfs een hele Information Security Office hebben.

Werkzaamheden en verantwoordelijkheden

De CISO is verantwoordelijk voor het opzetten en onderhouden van de visie, de strategie en het programma om de informatie en technologieën van de organisatie te beveiligen. Om risico's op het gebied van informatie en IT te verminderen stuurt de CISO organisatiebreed op het identificeren, ontwikkelen, implementeren en onderhouden van processen, standaards, policies en procedures. Daarnaast reageert hij of zij reageert op cyberincidenten. De CISO is in principe een senior executive met invloed door de gehele organisatie. De succesvolle CISO helpt, ondersteunt, signaleert, maar lost niet zelf de problemen op.

Het CISO spectrum

De exacte verantwoordelijkheden en taakinvulling van de CISO verschilt echter sterk van organisatie tot organisatie. Een aantal van de spectra die we binnen de CISO wereld aantreffen zijn weergegeven in de tabel hieronder. De voorbeelden links betreffen hier een minimale invulling, de voorbeelden rechts een volwassen volwaardige invulling van de rol. In de afgelopen jaren heeft een duidelijke verschuiving naar rechts plaatsgevonden.

Spectrum	Voorbeelden	
Fte	0,2 fte: "doe het er maar even bij"	CISO Office, groot team: "security is essentieel voor onze organisatie"
Plek in de organisatie	Rapporteert aan CIO	C-suite.
Verantwoordelijkheid	CISO is verantwoordelijk voor de security	Verantwoordelijkheden bij de uitvoerders, controle bij de CISO
Aandachtspunten	Techniek	Organisatie
Status	(tijdelijk) ingehuurd	Staande organisatie
Perceptie	De CISO is lastig	De CISO is ondersteunend

Omdat er een zekere mate van overlap is tussen de taken van de CISO en de CIO - wat in de ene organisatie onder de CISO valt, valt in de andere organisatie onder de CIO - nemen we in dit document én in de CISO meetings nadrukkelijk ook de CIO mee. De aandacht ligt daarbij wel steeds op information *security*.

Ondanks het belang voor en de invloed binnen de organisatie vervult de CISO vaak een ‘eenzame’ rol. Waar de rest van de organisatie ICT gebruikt om het werk uit te voeren of om nieuwe mogelijkheden na te streven is hij of zij de enige die zich druk maakt over de veiligheidsimplicaties. De CISO wordt vaak (terecht of onterecht) gezien als spelbreker of als het vermanende vingertje van de organisatie. Voor vragen of ideeën over de uitvoering van de eigen functie kan de CISO vaak niet binnen de eigen organisatie terecht. Er is dan ook vaak een behoefte om van gedachten te kunnen wisselen met CISO’s van andere instellingen.

3. Intersectorale CISO intervisie

De behoefte van CISO's vanuit verschillende achtergronden om met elkaar te delen en te groeien sluit aan bij de doelstelling van HSD om partijen uit overheid, onderzoek en bedrijfsleven bijeen te brengen om samen vernieuwend onze cybersecurity op een hoger plan te tillen. Er zijn reeds incidentele CISO-bijeenkomsten en de voor de CISO's uit de kritieke infrastructuur zijn de ISACs opgericht, maar een platform als dit, waar best practices, uitdagingen en ideeën met concollega's kunnen worden gedeeld, bestaat nog niet.

High level CISO sessies

HSD is medio 2018 dan ook begonnen met het organiseren en faciliteren van bijeenkomsten waarin we CISO's en CIO's van verschillende organisaties uit verschillende sectoren bijeenbrengen om van elkaar te leren. Dit gebeurt in de vorm van intersectorale CISO meetings met een groepsgrootte van rond de 8 CISO's/CIO's. Deze grootte is gekozen om het onderlinge vertrouwen snel op te kunnen bouwen. De meetings zijn georganiseerd rondom een specifiek thema of een door de groep aangegeven aandachtspunt, duren meestal 3 uur, en vinden plaats bij HSD of bij een van de deelnemende partijen.

Deelnemende partijen (per 01-01-2020)		
Brunel	Mammoet	RAI Amsterdam
Centric	MERUS	Rijk Zwaan
CISCO	Ministerie van Defensie	Rijksoverheid ICT
Cybersprint	Ministerie van Sociale Zaken en Werkgelegenheid	Rijkswaterstaat
De Nederlandsche Bank	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	TNO
Gemeente Den Haag	NN Investment Partners	TU Delft
Greenpeace	NS	Tweede Kamer
Hoogheemraadschap Rijnland	ONE-Dyas	Universiteit van Amsterdam
ICT Motiv	Openbaar Ministerie	Volker Wessels
KLM	Palo Alto	Vrije Universiteit Amsterdam
KPN	PGGM	

Deze sessies geven de deelnemende partijen de mogelijkheid om *best practices* te delen, elkaar vragen te stellen, als denktank te fungeren, het netwerk uit te breiden, interessante sprekers uit te nodigen, te reageren op actualiteiten, elkaar scherp te houden en de verdieping op te zoeken. Ze verschillen van bestaande gremia zoals de ISACs in het feit dat ze intersectoraal zijn en niet beperkt tot *vitale* sectoren. Het voordeel van deze aanpak is dat inzichten en oplossingen die binnen de ene sector bestaan makkelijker de oversteek maken naar andere sectoren. De algemene problematiek van CISO's blijkt ongeacht bedrijf of sector in grote mate identiek te zijn, wat deze meetings bij uitstek geschikt maakt om met elkaar te sparren.

De sessies hebben een vertrouwelijk karakter. De deelnemende partijen worden in dit whitepaper wel genoemd, maar uitspraken zijn niet te herleiden tot individuele partijen. Ook moet opgemerkt worden dat niet elke partij het noodzakelijkerwijs eens is met de hier gepresenteerde uitkomsten en aanbevelingen.

Thema's

In de sessies zijn met de aanwezigen verschillende thema's besproken. Daarnaast is de behoefte uitgesproken om over andere thema's verder bijeen te komen.

Een van de meer prangende thema's, wat te doen bij langdurige ICT verstoringen, is in alle groepen aan bod gekomen en zal in dit whitepaper verder uitgewerkt worden. Andere thema's die aan bod zijn gekomen of waar behoefte aan bestaat zijn onder meer:

- Hoe betrek ik de board – nodig om ze de juiste risico-afwegingen te laten maken;
- Het opzetten van organisatiebrede cyberoefeningen – inclusief red-teaming;
- Verantwoordelijkheden: hoe leg ik de verantwoordelijkheid voor de security bij de afdelingen zelf;
- Groei van een van compliance based naar een risk based organisatie
- De rol van de overheid: welke concrete aanbevelingen kunnen we doen om de security in Nederland naar een hoger plan te tillen;
- Opleidingen en awareness, wat is nodig, wat is beschikbaar;
- Samenwerking met SOC's;
- Aansluiting op nationaal detectienetwerk

Daarnaast werd de wens uitgesproken om de sessie te verrijken door het uitnodigen van boardleden, experts, maar ook bijvoorbeeld de bakker om de hoek, om zo een helderder kijk te krijgen op visies, problemen en oplossingen.

4. Resilience en robuustheid bij langdurige ICT uitval

Eén thema dat in alle CISO intervisiegroepen aan bod is gekomen is de vraag hoe om te gaan met langdurige en ernstige ICT-verstoring. Achtergrond van deze vraagstelling is enerzijds de voorbeelden hiervan die ons in de afgelopen jaren bereikt hebben, anderzijds de aandacht die dit thema de afgelopen tijd van de overheid heeft gekregen.

Resilience versus robuustheid

Nederland digitaliseert steeds verder. Voor de meeste bedrijven en instellingen betekent een uitval van ICT een ernstige belemmering in de uitvoering van de (kern)activiteiten. De kans op uitval kan verkleind worden door allerhande beschermende maatregelen, maar het risico blijft. De impact van uitval is vaak groot. Om zich hiertegen te wapenen kunnen zowel de resilience als de robuustheid worden verhoogd.

De *resilience* van het systeem is het vermogen om ICT en netwerk snel te herstellen, zodat de normale operatie hervat kan worden.

De *robuustheid* van de organisatie is het vermogen van deze organisatie om de kerntaken ook zonder ICT-ondersteuning uit te blijven voeren.

Beide vallen in de *Respond fase* van het Gartner Predict Prevent Detect Respond framework (zie figuur - ze vallen ook onder de Respond fase van het NIST framework). Volledige uitval van de ICT is een speciaal geval van deze fase - de ernstigste mogelijkheid. De aandacht voor resilience en vooral robuustheid binnen cybersecurity blijft achter bij de aandacht voor preventie. Het voorbereiden op het omgaan met cyberfalen hoeft niet te wachten tot de organisatie getroffen wordt.

Het Gartner Predict Prevent Detect Respond framework

Maersk

In juni 2017 werden verscheidene bedrijven wereldwijd getroffen door de NotPetya malware. De malware, verspreid via Oekraïense accounting software M.E.Doc wordt verondersteld bedoeld te zijn geweest als aanvalswapen op Oekraïne, maar verspreidde zich ook tot ver daarbuiten. NotPetya vermomde zichzelf als ransomware en versleutelde zowel files als het Master Boot Record van geïnfecteerde computers met een willekeurige gegenereerde sleutel. Dit maakt herstel van het systeem onmogelijk. NotPetya was in staat zich razendsnel over het netwerk te verspreiden en leidde daarmee tot volledige ICT uitval van verschillende organisaties. Een van de getroffen organisaties was containervervoerder Maersk. Door een wereldwijde uitval van het systeem wist het bedrijf niet meer welke containers op welke locatie waren en naar welke klant ze op weg waren. Het herstel van het systeem duurde meer dan een week en vergde naast hard werk het nodige geluk. In de tussentijd probeerde de organisatie de kernoperatie draaiend te houden, zonder te weten hoe lang de uitval zou gaan duren.

Digitale ontwrichting

Digitale netwerken zijn in toenemende mate verbonden en uitval in het ene netwerk kan door cascade-effecten propageren naar andere netwerken. Als hierbij vitale processen geraakt worden spreekt de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) over digitale ontwrichting. In het rapport “Voorbereiden op digitale ontwrichting” stelt het WRR: “Opvallend is echter dat vrijwel alle cybersecurity-maatregelen en ambities van de overheid en andere belangrijke partijen zijn gericht op preventie: op het *voorkomen* van incidenten dus.” De WRR pleit voor meer aandacht voor het omgaan met incidenten: voorbereiden op wanneer het mis gaat.

Het sluit hierbij aan bij de conclusie van het Cyber Security Beeld Nederland (CSBN) 2019, dat stelt: “Vrijwel alle vitale processen en diensten zijn volledig afhankelijk van ict. Omdat analoge alternatieven bijna helemaal verdwenen en terugvalopties afwezig zijn, is de afhankelijkheid van gedigitaliseerde processen en systemen zo groot geworden dat aantasting hiervan kan leiden tot maatschappij-ontwrichtende schade.”

Hierbij moet opgemerkt worden dat - hoewel WRR en CSBN het over vitale processen hebben - uitval van niet-vitale processen via keteneffecten invloed kan hebben op vitale processen. De aanval op DigiNotar in 2011 is een duidelijk voorbeeld van de potentiële invloed van niet als vitaal bemerkte processen op de vitale (overheids)processen.

Voorbeelden van robuustheid

Een pensioenfonds betaalt maandelijks pensioenen uit. Het bedrijf is volledig geautomatiseerd en de papieren administratie is reeds lang de deur uit. Het netwerk valt voor langere tijd uit. Op een apart ingerichte computer los van het netwerk worden de uitbetalingen van de afgelopen maand herhaald. Of aan de hand van een offline bewaarde basisadministratie en een aantal formules wordt een richtbedrag uitgerekend en dit wordt uitgekeerd. Daarnaast wordt een noodnummer opengesteld en heeft de directie bepaald dat in geval van twijfel eerder te veel dan te weinig wordt uitgekeerd. Deze oplossing werkt niet perfect voor alle klanten, maar levert wel een 95% oplossing. Na herstel van het systeem kunnen de fouten rechtgebreid worden.

Op 24 juni 2019 viel 112 uit. Door een storing bij KPN vielen alle noodsystemen gelijktijdig uit, ook het politie noodnummer. In de ideale situatie is hier een draaiboek voor en is er op getraind. Er is een lijst met nummers van alternatieve providers die direct verspreid kan worden. Deze nummers zijn up-to-date gehouden. Er zijn mogelijkheden om via sociale media zoals Whatsapp contact op te nemen met de noodcentrales.

De elektronische aansturing van sluizen en gemalen valt uit. Handbediening is nog mogelijk, maar er is onvoldoende mankracht. Er is een up-to-date lijst met pensionado's die voor deze situatie ingezet kunnen worden.

5. Uitkomsten

De volgende paragrafen beschrijven de belangrijkste uitkomsten en conclusies van de groepen CISO's naar aanleiding van deze discussies.

De CISO's herkenden het geschetste plaatje. Er zijn over het algemeen te weinig fall-back opties - met langdurige uitval van ICT wordt onvoldoende rekening gehouden. Er is een gat in response en recovery. Daar staat tegenover dat totale robuustheid, zoals alles ook op papier bijhouden, of faxen in de kast hebben staan, voor de meeste bedrijven en instellingen geen realistische optie is, en waarschijnlijk ook niet nodig.

Uit de discussies zijn verschillende inzichten en aanbevelingen naar voren gekomen, die we voor dit whitepaper in vijf categorieën zullen opdelen, drie categorieën (directie, oefenen, techniek) organisatie-intern, en twee categorieën (opleiden, overheid) organisatieoverstijgend. Daarnaast zijn nog een aantal algemene beschouwingen die de moeite van het opnemen waard zijn.

Disclaimer: het onderstaande is gedestilleerd uit de uitkomsten van discussies in vier verschillende CISO groepen. De CISO's spraken hier op persoonlijke titel, en de bevindingen en aanbevelingen worden niet steeds unaniem door alle CISO's gedeeld.

Directie

De directie (board / raad van bestuur) is vaak nog te naïef als het om cyberincidenten en de daaruit mogelijk voortvloeiende gevolgen gaat. Ze denken er vaak liever niet over na en willen het niet weten. Dit is deels te verklaren uit het feit dat ICT security als ongrijpbaar en onbegrijpbaar wordt beschouwd en deels uit het feit dat security een negatief image heeft - in plaats van kansen gaat het alleen maar over risico's en gevaren. Security wordt dan ook graag uitbesteed aan CISO of ICT afdeling, maar blijft uiteindelijk een board verantwoordelijkheid. Van dat laatste is de directie zich niet altijd bewust.

Om hier verandering in te brengen zal de CISO de taal van de board moeten spreken. Dat betekent onder andere dat cybersecurity van context moet worden voorzien en vertaald moet worden naar de business.

AANBEVELING: Laat een business impact analyse uitvoeren naar de gevolgen van een langer durende uitval van ICT systemen. Wat zijn de kosten? Waar liggen de verantwoordelijkheden? Wat zijn de kroonjuwelen? Volwassen bedrijven beschikken over een Business Continuity Management framework. ICT gerelateerde rampen dienen hierin opgenomen te worden.

Ook spraken verschillende CISO's de wens uit om de board op te leiden zodat ze over voldoende kennis en tools beschikken om de juiste beslissingen te nemen om cyberincidenten te voorkomen of het hoofd te bieden. Zo zouden ze de board graag eens meenemen naar een bijeenkomst als deze om over dit onderwerp te praten en te ondervinden dat het geen ICT problematiek maar een management issue is.

Tenslotte wordt in verschillende groepen genoemd dat veel bedrijven nog te veel op *compliance* inzetten, maar dat een lijstje met vinkjes niet hetzelfde is als een veilig bedrijf. Compliance is te veel een papieren werkelijkheid, en daarnaast vaak het absolute minimum aan maatregelen dat moet worden genomen. Echte security is risk based en biedt de mogelijkheid om te reageren op echte dreigingen.

AANBEVELING: Neem geen genoegen met compliance, maak de stap naar risk based ICT security.

De CISO's zouden graag een soortgelijke sessie als deze over dit onderwerp doen, en daarbij de board uitnodigen.

Oefenen

Er is de afgelopen jaren veel aandacht besteed aan awareness. Het is een open discussie in de cybersecurity community in hoeverre dit effectief is. Ook in de bijeenkomsten worden voorbeelden aangehaald van awareness campagnes die succesvol zijn tot phishingcampagnes die niet tot meetbare verbetering leiden.

Dit kan mogelijk verklaard worden door het gegeven dat veel campagnes een rationele insteek hebben. De medewerkers kennen de risico's, weten wat ze zouden moeten doen, maar *voelen* het niet.

Ook is in de bijeenkomsten geconstateerd dat er nog een gat zit in de response en recovery. De nadruk in cybersecurity ligt nog op preventie, en dan vaak ook nog technisch, terwijl de response het cyberdomein overstijgt en bij een groter incident de hele organisatie kan raken. Bij volledige uitval van het netwerk is dat zeker het geval. De hele organisatie moet dan ook getraind zijn.

Oefeningen vangen beide punten af: ze maken awareness emotioneel door de deelnemers te betrekken en onder te dompelen in een scenario. En ze maken de gaten in de response-organisatie zichtbaar, zodat de rampenplannen navenant aangepast kunnen worden. Ook eventuele cascade effecten worden zichtbaar. Daarnaast kunnen ze het negatieve image van cybersecurity helpen verbeteren.

Over de vorm van de oefeningen geven de groepen geen aanbeveling: table top oefeningen, grootschalige rampenscenario's, red teaming - ze lijken allen te werken. Wel belangrijk is dat de oefeningen serieus worden genomen, vooral ook door de directie. Een goed voorbeeld van een succesvolle oefening is TIBER van DNB, die op een van de sessies uitgebreid werd gepresenteerd.

AANBEVELING: Meer cyber-oefeningen. Betrek de directie. De gevolgen van veel cyber-incidenten zijn fysiek; sluit op bestaande fysieke oefeningen aan. Leg de verbanden tussen ICT rampen en fysieke gevolgen.

De oefeningen hoeven overigens niet goed te gaan. Ze zijn immers bedoeld om gebreken aan het licht te brengen. Een oefening waarin iedereen de juiste beslissingen neemt is een mislukte oefening.

Techniek

Daar waar technische oplossingen te implementeren zijn verdient het aanbeveling om dit ook te doen. Het is echter een fout om te denken dat dit voldoende is om rampen te voorkomen of op te lossen. Toch kunnen technische maatregelen bijdragen aan een grotere robuustheid van de organisatie.

Genoemde opties zijn compartimentaliseren, standaardiseren en simplificeren. Alle drie de methoden verlagen de complexiteit van het systeem en daarmee de kwetsbaarheid. Compartimentalisatie kan er bij grootschalige uitval voor zorgen dat onderdelen van het systeem blijven draaien. Standaardisatie vergroot de beheersbaarheid van het systeem, en simplificatie heeft te maken met het feit dat veel systemen organisch gegroeid zijn en er verbanden zijn die allang niet meer nodig of wenselijk zijn.

Overigens is wel opgemerkt dat standaardisatie niet te ver doorgevoerd moet worden. Er is een belangenafweging met de innovatiekracht van de organisatie. Een van de deelnemers merkte zelfs op dat bij grootschalige uitval van onbeperkte duur het wel eens de shadow IT zou kunnen zijn die de organisatie draaiend houdt.

AANBEVELING: Verhoog de robuustheid van de organisatie door systemen en processen goed onder de loep te nemen: kan er worden gecompartimentaliseerd, gestandaardiseerd, gesimplificeerd? Maar blijft het daarbij dan wel werkbaar? Besteed hierbij vooral aandacht aan scheiding van IT en OT.

Opleiden

In een maatschappij die sterk leunt op automatisering is het tekort aan specialisten, capaciteit en kennis op cybersecurity gebied een ernstig risico op de langere termijn. Mede door het tekort wordt het bestaande personeel vaak zwaar belast. Volgens een door Nominet in begin 2019 gepubliceerd onderzoek is de kans op burn-out bij CISO's hoog. De werkdruk is overigens hier niet de enige oorzaak van. Om de capaciteit te verhogen zijn er grofweg drie opties:

- Aantrekken vanuit het buitenland
- Beter omspringen met beschikbare capaciteit
- Meer mensen opleiden

Om Nederland aantrekkelijker te maken voor buitenlandse specialisten is een cybersecurity delta nodig waar innovatie, onderzoek en hoogwaardig werk samenkomen. Dit valt buiten het aandachtsgebied van dit whitepaper.

We gebruiken in Nederland nog maar een fractie van ons potentieel. Op termijn kan door opleiding en anders denken dit percentage verhoogd worden. Zo zijn vrouwen nog sterk ondervertegenwoordigd in deze sector, wordt nog te veel geleund op universitair geschoolden en is er een groep goede ICT'ers die helemaal geen diploma heeft. Ook is er een groep goede kandidaten die moeilijk in de klasieke kantooromgeving te plaatsen is, en dient aandacht besteed te worden aan het op het goede pad houden van jeugdig talent (project Hackright is hier een goede aanzet voor). Een beter gebruik maken van het beschikbare potentieel betekent dat werkgevers anders zullen moeten gaan werven, en overheid en onderwijsinstellingen het studieaanbod moeten verbreden en aantrekkelijker maken voor meer doelgroepen.

Het tekort in de sector is niet weg te werken zonder actieve stimulans van het onderwijs. Dit betekent verbreden van het aanbod, en het aantrekkelijker maken van het vakgebied voor meer groepen. Dit houdt overigens ook in dat de afnemers van nieuw talent, zowel bij overheid als bedrijfsleven, zelf een investering moeten doen in het onderwijs, bijvoorbeeld door hun experts (gast)colleges te laten geven, door bij te dragen aan curriculum en ontwikkeling middels leeropdrachten, afstudeer- en stageprojecten.

AANBEVELING: Verbeter het cybsersecurity onderwijs op HBO en MBO niveau. Stimuleer onderwijs aan vrouwen en ouderen. Ondersteun vanuit bedrijfsleven en overheidsorganisaties dit onderwijs actief.

Naast specialisten is er ook behoefte aan een hoger niveau van algemene ontwikkeling op het gebied van cybersecurity. Met ICT dermate verweven in onze samenleving zou security een standaardonderdeel van het curriculum op voortgezet onderwijs én basisscholen moeten zijn. Om dit te kunnen bewerkstelligen zullen eerst de onderwijzers onderwezen moeten worden.

Overheid

Uitval komt zelden alleen. Een volledige ICT uitval bij een bedrijf of instelling heeft gevolgen bij andere bedrijven en instellingen. In veel gevallen zal de overheid er daarom mee te maken krijgen. Daarnaast speelt de overheid een belangrijke rol als het gaat over de preventie van grote cyberincidenten en de voorbereiding op het omgaan met dergelijke incidenten, mochten ze toch plaatsvinden.

Regulering is een middel waarmee bedrijven en instellingen gedwongen kunnen worden om hun cybersecurity naar een hoger niveau te tillen. Veel van de op de bijeenkomsten aanwezige CISO's hebben in de praktijk het nut van regulering gezien. Daarnaast waarschuwen ze echter wel dat regulering het risico meebrengt dat bedrijven en instellingen inzetten op compliance, terwijl security risk-based zou moeten zijn. De overheid zou misschien een tweede stap kunnen aanbieden in de vorm van een risk management framework.

De overheid kan ook een rol spelen in een nationale samenwerking op het gebied van cybersecurity. Op security zou niet geconcurreerd moeten worden. Maar samenwerken vergt vertrouwen, en in het opbouwen van dit vertrouwen kan de overheid een aanjagende rol spelen.

Tenslotte zouden de CISO's graag een duidelijkere visie van de overheid willen zien.

AANBEVELING: Met het toenemen van grote cyberdreigingen is er behoefte aan een nationaal ICT Deltaplan. De overheid zou hierin het voortouw moeten nemen, maar het onderwijs en bedrijfsleven dient nadrukkelijk meegenomen te worden.

6. Conclusie

Behoefte

Een gremium als de intersectorale CISO/CIO intervisie-meetings bestond nog niet. De deelnemers hebben aangegeven de bijeenkomsten zinvol te vinden. HSD gaat dan ook op zoek naar de mogelijkheden om deze meetings voort te zetten en uit te breiden met nieuwe groepen. Op de meetings hebben de deelnemers ook aangegeven waarover ze in toekomstige sessies graag van gedachten zouden wisselen. Dit heeft een lijst opgeleverd van CISO interesse-punten waarmee HSD aan de slag kan. Het betreft zeer gevarieerde thema's zoals onderwijs, cybercrisisoefeningen, schaarste van expertise en regelgeving.

Bevlogen

Wat opvalt bij de CISO's in hun bevlogenheid – niet alleen voor het veilighouden van hun eigen organisatie, maar ook voor de samenleving. CISO's gaan door als anderen de deur al lang achter zich dichtgetrokken hebben en hebben een hoge mate van corporate social responsibility

Aanbevelingen

De gekozen vraagstelling heeft geleid tot nuttige discussie waarin de deelnemers aanknopingspunten hebben gekregen om zelf aan de slag te gaan, maar ook aanbevelingen te kunnen geven voor collega's in den lande.

De robuustheid van veel bedrijven en instellingen behoeft extra aandacht. Totale uitval van de ICT is denkbaar - ransomwaregevallen geven dit keer op keer aan. De mogelijkheid op totale uitval zou meegenomen moeten worden in het Business Continuity Plan. Meer in het algemeen dient cybersecurity beter aan te sluiten op de business, en de board zich meer bewust te zijn van het belang van cybersecurity.

Hoe nu verder?

Er zijn verschillende modellen denkbaar waarbij deze intersectorale intervisiesessie voortgezet en uitgebreid kunnen worden. HSD is deze modellen aan het onderzoeken.

Veel van de aanbevelingen uit dit document bieden aanknopingspunten voor HSD om samen met CISO's en partners aan de slag te kunnen: samenwerking, opleidingen en matchmaking komen op verschillende plaatsen terug en zijn de core business van de Hague Security Delta.

7. Literatuur

CIP - Enquete CISO's binnen de Nederlandse Overheid, oktober 2019

DNB - TIBER NL Guide, How to conduct the TIBER NL Test, November 2017

Streefland, Fred (Palo Alto), Budgeting for Cybersecurity: Are You Doing It Right?, oktober 2019

Greenberg, Andy - The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Wired, augustus 2018

Inspectie Justitie en Veiligheid - Crisiscommunicatie bij de uitval van 112 op 24 juni 2019

NCSC - Coordinated Vulnerability Disclosure: the Guideline, oktober 2018

NCTV - Cybersecuritybeeld Nederland 2019, juni 2019

Nominet - Life inside the perimeter - understanding the modern CISO, februari 2019

Secure Link - The CISO File, mei 2019

Shomo, Paul (DarkReading), 5 Cybersecurity CISO Priorities for the Future, november 2019

WRR - Voorbereiden op digitale ontwrichting, augustus 2019

Bijlage: Vraagstelling en werkwijze

Vraagstelling

Om voorbereid te zijn op een situatie waarin de volledige ICT uitvalt moeten zowel resilience als robuustheid geregeld zijn. Resilience is hoofdzakelijk een ICT uitdaging. Een goede resilience zorgt ervoor dat de kans op langdurige uitval beperkt blijft. Het biedt echter geen garantie, en zonder de robuustheid om gedurende de uitval op een alternatieve manier de kernoperatie te kunnen blijven uitvoeren ontstaan bij langduriger uitval ernstige risico's, waaronder de mogelijkheden van faillissement en digitale ontwrichting

Over robuustheid van organisaties bij langdurige ICT uitval is nog weinig geschreven. Daarom is voor dit thema gekozen voor de CISO meetings. Daarnaast is resilience veel ter sprake gekomen, aangezien de twee met elkaar verbonden zijn.

Besproken is onder andere:

- Of langdurige ICT uitval realistisch is en wat de impact is - in het bovengenoemde voorbeeld zijn zowel Maersk als Oekraïne er redelijk snel bovenop gekomen;
- Wat de oorzaken zijn van gebrek aan robuustheid, en hoe deze weggenomen zouden kunnen worden;
- Welke acties nu ondernomen zouden moeten worden om bij een groot incident de kernactiviteiten te kunnen blijven uitvoeren terwijl de ICT er voor onbepaalde tijd uit ligt.

Werkwijze

De CISO's van de verschillende groepen waren unaniem van mening dat een Maersk-type incident in elke organisatie *kan* voorkomen, al is het risico daarop kleiner naarmate de volwassenheid van de security van de organisatie toeneemt. Uitgangspunt voor discussie was of we een dergelijk incident met onze huidige oplossingen *aankunnen*.

De stelling voor discussie luidde:

> Onze huidige cybersecurity aanpak (o.a. middelen, technieken, kennis) is in de toekomst niet langer opgewassen tegen het groeiend aanvals- en verstoringsgeweld.

Met *huidige aanpak* bedoelen we hier antivirus, firewalls, network intrusion detection, SOC, wachtwoordbeleid, awareness, financiële en personele middelen, kennis etc.

De cybersecurity aanpak kan vergeleken worden met een dijk die we verhogen om stijgend water te kunnen keren. Het water zou echter sneller kunnen rijzen dan we de dijk verhogen: welke (cascade)effecten heeft dat? wat is het plan voor als de dijk toch overstroomt? Is er een plan? Is een plan nodig?

De groep werd in tweeën gesplitst:

Groep 1 (voor de stelling) “we gaan eraan” (met de huidige aanpak) besprak en prioriteerde de knelpunten, en besprak wat en wie nodig is om deze knelpunten op te lossen.

Groep 2 (tegen de stelling) “we kunnen het aan” beschreef de oplossingen, prioriteerde deze, en beschreef wat en wie nodig is om deze oplossingen te implementeren.

Aan de hand van de antwoorden van beide groepen werd verder gediscussieerd om te komen tot analyse en aanbevelingen.

Bijlage: algemene bevindingen

Het thema ‘langdurige uitval van ICT systemen’ is slechts een van de onderwerpen die in de CISO intervisiesessies aan bod is gekomen. Er zijn met een aantal groepen ook bijeenkomsten geweest met andere thema’s. Daar waar we denken dat dit toegevoegde waarde kan hebben kunnen ook hierover whitepapers gepubliceerd worden. In deze bijlage willen we ons beperken tot het opsommen van een aantal bevindingen die meermaals terug zijn gekomen, soms terloops, soms uitgebreid besproken, maar die niet direct met het onderwerp van dit whitepaper te maken hebben.

Rampen zijn nuttig. Omdat het effect van goede cybersecurity niet zichtbaar is zal het af en toe mis moeten gaan als gevolg van slechte cybersecurity om de focus en het budget te blijven behouden. En dat misgaan moet dan het liefst elders plaatsvinden, maar wel bij een herkenbare organisatie. Een goede ramp is nooit weg. Diginotar bewijst nog steeds zijn nut.

Veiligheid van OT (Operational Technology) is onderbelicht. Er zijn nog steeds teveel legacy systemen die ongepatcht en onbeschermd aan het internet hangen. Op dit gebied is meer awareness nodig.

De mindset binnen de security zou meer richting kansen moeten gaan om interessanter te worden voor directie en instromers.

Nederland heeft een uitstekende positie in de wereld als het gaat om coordinated vulnerability disclosure (voorheen vaak responsible disclosure genoemd). Dit draagt bij aan de algemene cyberveiligheid. Hier kan nog flink op uitgebouwd worden.

The Hague Security Delta
Wilhelmina van Pruisenweg 104
2595 AN Den Haag
070 204 51 80

info@thehaguesecuritydelta.com
www.thehaguesecuritydelta.com
@HSD_NL