Operatie POSITRON aflevering 5 - Patatje troep

DAVID

Uiteindelijk zeg ik altijd: als je maar genoeg tijd en resources hebt, dan lukt het uiteindelijk wel een keer. Dus lukt het niet op afstand, dan wacht ik tot je straks naar het toilet gaat. En dan, ja, wie weet wat je dan allemaal kan doen?

LIESBETH

Ik moet wat bekennen. Heel veel jaren geleden, in een zwak moment, stond ik op het punt om in de telefoon van mijn toenmalige en niet erg te vertrouwen geliefde te gluren. Hij stond onder de douche en zijn telefoon lag op het nachtkastje. Er nog geen meter bij me vandaan. Zal ik? Ik denk dat veel mensen dit wel eens hebben gedaan of bijna hebben gedaan. Maar net toen ik mijn geweten aan de kant had gezet en van plan was toe te slaan, hoorde ik het water stoppen met lopen, de badkamerdeur opengaan en met een paar grote stappen stond hij weer in de kamer, wat gelukkig een voortijdig einde aan die missie bracht. Maar stel je voor dat je ongezien iemands telefoon in zou kunnen of iemands computer. Zou je dat dan doen?

DAVID

Ik denk dat er in de buitenwereld ook nog steeds plekken zijn om heel creatief heel veel hele toffe dingen met elkaar te maken, maar hier hebben we gewoon... Dit is jouw toestemming om op best wel spannende plekken te komen in de wereld.

LIESBETH

Mijn naam is Liesbeth Rasker. Dit is aflevering 5 van de podcast van de AIVD. Welkom bij De Dienst.

LIESBETH

Tom, goedemorgen.

TOM

Goeiemorgen, Liesbeth! Grote dingen gedaan, veel gebeurd. Zullen we even terugkijken op wat er allemaal gebeurd is en het even analyseren en waar we heen gaan?

LIESBETH

Er zijn inderdaad grote dingen gebeurd. Even een terugblik op onze zaak met de codenaam Operatie Positron. We hebben energiemaatschappij Elektron BV, die aangevallen wordt door een hackersgroep die we de codenaam Zuurkool hebben gegeven. Zuurkool heeft op twee plekken in het netwerk malware geplaatst. Die malware noemen we Rookworst. Elektron heeft een van de twee implants zelf verwijderd, wat betekent dat de actor waarschijnlijk weet dat ze gezien zijn. Het is dan dus wachten tot ze zich helemaal terugtrekken uit het netwerk en wij geen kans meer hebben te achterhalen wie ze zijn. Om dat te voorkomen, hebben we een kopie of een disk image gemaakt van de server waar pannekoekenpalazzo.nl op draait en hebben we een tap aangesloten. En dat levert nieuwe informatie op.

TOM

Ze hebben een wat verouderde methode gebruikt die, als we even technisch gaan, geen forward secrecy geeft, geen Diffie-Hellman gebruikt. En laten wij nou net op die disk image the private key van de server aangetroffen hebben.

LIESBETH

Dat is dus de sleutel.

TOM

Dat is de sleutel om dat verkeer te ontcijferen, dus dat hebben we gedaan. En daar zitten wel wat aardige stukken informatie in. Een kleine complicatie. De server staat niet in Nederland en dus met de WIV zijn we beperkt in de mogelijkheden die we hebben. Er is natuurlijk één ding dat we wel kunnen doen en dat is de

server gaan hacken. En ik denk dat we dat serieus moeten gaan overwegen. Omdat dit de enige weg voorwaarts is die we nog hebben.

LIESBETH

We gaan hacken en daarmee word ik naar mijn volgende gesprek gestuurd en wel met David. Hij is hacker bij de MIVD. Dat is de zusterdienst van de AIVD, zoals uitgelegd in de vorige aflevering. Niemand hier is eraan gewend om met iemand uit de buitenwereld over zijn of haar werk te praten, laat staan voor een microfoon. Maar een hacker al helemaal niet, zeker niet een hacker die voor de geheime dienst werkt. Het was dan ook tot vrij kort voor de opname onzeker of hij mee wilde doen aan deze podcast. We hebben zijn stem vervormd en uiteraard is David niet zijn echte naam.

DAVID

Wij zijn zuinig op onze identiteit, want het is bijvoorbeeld steeds populairder om naming en shaming te doen van buitenlandse hackers. Het is ook wel in het verleden gebeurd in de media dat diverse landen mediaberichten de wereld in sturen waarin ze zeggen: kijk, deze hackers hebben ons geprobeerd te pakken. Hier zie je: volledig met naam en toenaam en foto. En dat heeft aardig consequenties. Want dat kan betekenen dat het misschien voor je familie risico's met zich meebrengt, je reisbewegingen worden mogelijk beperkt. Het is gewoon geen pretje. Ik ben operator bij de afdeling Computer Network Exploitation, dus wat wij doen, is hacken van de targets die wij opgedragen krijgen om te hacken. Je moet je voorstellen, als wij ons werk doen, dat zijn operaties, die doen we heimelijk. Die doen wij in opdracht van een inlichtingenteam, dus een inlichting komt met een verzoek van: we willen graag informatie over een bepaald doel. Dat kan bij diverse targets zijn, de slachtoffers, om het maar zo te zeggen, die wij dan moeten gaan hacken om daar die informatie te verkrijgen. Het feit dat we dat doen moet dan geheim zijn, want er zijn wel degelijk potentieel diplomatieke gevolgen aan als het uit zou lekken, dat een land erachter komt, bijvoorbeeld als wij daar in een ministerie aan het binnendringen zijn voor informatie.

LIESBETH

Ah ja, oké, dat snap ik. En jij moet niet sporen achterlaten.

DAVID

Juist.

LIESBETH

Die te herleiden zijn naar de Nederlandse geheime dienst.

DAVID

Juist, ja.

LIESBETH

Hoe is de situatie bij jou thuis? Alle details graag.

DAVID

Alle details, alle details. Ik heb systemen die ik graag wat beter bescherm in mijn thuisnetwerk dan bijvoorbeeld m'n televisie. M'n televisie boeit me niet zoveel. Daar zit geen microfoon of niks in, dus dat maakt me niet zo gek veel uit. Dus dat hangt in een ander stukje netwerksegment dan de rest. En zo heb ik allerlei scheidingen aangebracht. Verschillende wifinetwerken om het een en ander los te koppelen van elkaar.

LIESBETH

Ja, precies. Dus jouw bereidheid om gebruiksgemak in te leveren, is natuurlijk een stuk groter dan de mijne.

DAVID

Ja en nee, want ik ben niet de enige in huis, dus ik moet ook rekening houden met andere gebruikers in het thuisnetwerk. Dus het moet wel gebruiksvriendelijk zijn.

LIESBETH

Worden die er weleens gek van?

DAVID

Ja, ja, als ik dan weer een of andere blacklist van systemen waar je dan niet naartoe zou mogen verbinden aan websites en dergelijke, weer toevoeg en in één keer werkt de webshop weer niet, dan ben ik de eerste die het weet.

LIESBETH

Binnen de afdeling Cyber is wat David doet wel zo'n beetje het meest spionnerige wat ik me kan voorstellen. Zijn verhaal en hoe alles wat hij doet in het grootste geheim gedaan moet worden, deed me ook denken aan vorig jaar, toen Harry vertelde over zijn geheime operaties waarbij hij met een ander paspoort en een tas vol spionagemateriaal, of een tas vol ellende zoals hij dat noemde, in het buitenland op missie ging.

DAVID

We hoeven inderdaad dus niet met een paspoort fysiek de grens over, maar we kunnen wel inderdaad alle grenzen... Er zijn voor ons geen landsgrenzen.

LIESBETH

Nee, precies, en waar hij een vals paspoort heeft, moet jij op een...

DAVID

Een valse online identiteit in feite hebben. Ja. Ja, zo zou je het kunnen zien inderdaad.

LIESBETH

Hoe is het dan nu voor jou om hier tegenover mij met deze microfoon, opnameapparatuur te zitten?

DAVID

Het is heel onnatuurlijk voor mijn gevoel, omdat ik heel erg gewend ben om stil te zijn over wat ik doe.

LIESBETH

Ja.

DAVID

Zo weet bijvoorbeeld mijn familie ook niet precies wat ik doe, die zullen misschien een idee hebben van, maar die... Dus het voelt heel raar om hier te zitten tegenover jou en dit te doen. Maar ik denk wel dat ergens goed is om een stukje communicatie naar buiten te doen vanuit onze afdeling ook.

LIESBETH

Hoe word je hacker?

DAVID

Ik denk dat dat iets is... Ik denk dat het een houding is van mensen. Wat je over het algemeen ziet, stel, je zou een keer bij ons op de afdeling rondlopen... Wat je dan ziet, is dat het over het algemeen mensen zijn die heel intrinsiek gemotiveerd zijn om te snappen hoe iets werkt. Dus die luisteren niet naar: nee, dit is zo. Nee, die willen dan weten, die gaan uitzoeken: waarom werkt dat zo? Het zijn vaak mensen, niet allemaal, maar vaak ook mensen die al van jongs af aan ermee bezig zijn. Een jaar of 10, 14, en op die manier eigenlijk erin rollen. En dan kom je op allerlei plekken op het internet waar je met like-minded mensen erover

gaat praten. Je wordt steeds meer bedreven erin, totdat je uiteindelijk bijvoorbeeld een keer op een werkplek als deze komt. Omdat je naar de buitenwereld niet naar buiten kan treden, word je intern eigenlijk heel hecht en dat is wat je echt voelt. En daarnaast, ik kwam binnen in de veronderstelling dat ik redelijk wat wist. Toen kwam ik hier en toen dacht ik: nou, ik weet nog helemaal niks.

LIESBETH

Er ging ook op technisch gebied een wereld voor jou open.

DAVID

Ja, zeker. Ja.

LIESBETH

Er zijn uiteraard allerlei bedrijven waar ethical hackers en pen-testers werken en veel van hen maken gebruik van dezelfde technieken als David en andere CNE'ers. Maar zij mogen slechts een fractie van wat ze hier binnen doen en kunnen. En een geheime dienst is wat dat betreft een walhalla voor mensen die op dit niveau willen werken.

DAVID

Ik denk dat dat het vooral de plek voor dit soort dingen maakt. Dus het feit dat je dus eigenlijk als er eenmaal goedkeuring is, meer mag dan over het algemeen bij andere partijen. Daar zit denk ik het verschil. Ik denk dat er in de buitenwereld ook nog steeds plekken zijn om heel creatief heel veel hele toffe dingen met elkaar te maken. Maar hier hebben we gewoon... Dit is jouw toestemming om op best wel spannende plekken te komen in de wereld.

LIESBETH

Ja, als we het hebben over de, laten we het noemen, populaire media. Dan worden hackers natuurlijk altijd afgebeeld als gasten op een zolderkamer in een zwarte hoodie. Ik zal niet omschrijven hoe je eruitziet, maar ik kan wel vertellen dat je geen zwarte hoodie aan hebt. Hoe vind jij het wat voor beeld er wordt geschetst van een hacker?

DAVID

Inmiddels is volgens mij de media ook wel redelijk af van het zwarte hoodie-imago. Dat is op zich, ja goed, lig er niet zo wakker van, maar het is goed dat er een wat realistischer beeld wordt afgespiegeld. Wat ik wel lastig vind van de media is dat heel veel naar buiten wordt opgeblazen alsof de hele wereld in de fik staat. En iedereen bedoelt alleen maar kwaad. Terwijl eigenlijk volgens mij misschien wel het grootste deel van alle hackers in de wereld gewoon heel ethisch bezig is en echt probeert de wereld beter te maken tegen dat groepje dat het zo verpest voor de rest eigenlijk. Dus de goeden lijden onder de kwaden. De media die blaast dingen misschien iets te veel op. Maar aan de andere kant: er gebeuren ook gewoon gekke dingen. Ja.

LIESBETH

David heeft een kalme manier van praten en komt over als een man die niet meer zo snel ergens van onder de indruk is en bij mij begint inmiddels het beeld te ontstaan van iemand die werkelijk overal digitaal kan inbreken. Hoelang zou het bijvoorbeeld duren voordat hij in mijn Dropbox kan zitten?

DAVID

Interessante vraag. Uiteindelijk zeg ik altijd: als je maar genoeg tijd en resources hebt, dan lukt het uiteindelijk wel een keer. Dus lukt het niet op afstand, dan wacht ik tot je straks naar toilet gaat. En dan kijken of ik toevallig iets... dat ie unlocked is. En dan, ja, wie weet wat je daar allemaal kan doen.

LIESBETH

Maar waar zou je dan beginnen?

DAVID

Waar zou ik beginnen?

LIESBETH

Ik zal 'm er eens bij pakken. Kijk, daar komt ie. Dit is hem. Het is een MacBook en dit is het scherm waar ik dan mijn wachtwoord of mijn Touch ID invoer.

DAVID

Ja, ja, in principe zo direct aan de buitenkant als ie hier staat, zullen we allerlei hulpmiddelen moeten gebruiken om daar misschien wat mee te kunnen of niet.

LIESBETH

Wat voor hulpmiddelen?

DAVID

Bijvoorbeeld een aantal jaar geleden bij DEF CON heeft iemand een presentatie gedaan van ze noemen PCI Leech. Dat is een klein kastje, de exacte details maken niet uit, dat is denk ik nu iets te technisch voor het verhaal. Maar ja, dat is in ieder geval iets, dat stop je gewoon als USB in een laptop en dan probeert ie via een bepaalde manier eigenlijk de sleutels van de laptop of computer uit het systeem te vissen. En dat zou betekenen als je 'm zo aan laat staan en je bent al een keer ingelogd geweest en je sluit dat ding aan, dan zou het kunnen zijn dat ik het wachtwoord van jouw MacBook te pakken zou kunnen krijgen.

LIESBETH

En kan ik zo'n kastje ook kopen? Of is dat...

DAVID

Dit zijn publiekelijk beschikbare spullen, ja. Die zijn gewoon op het internet te verkrijgen.

LIESBETH

Ja. En dan, dan is dat dus al klaar.

DAVID

Ja, en dan is het afhankelijk van wat het doel is. Dus in dit geval heb je het over een enkel systeem. Dan moeten we kijken, als je zegt: je wil bij jouw Dropbox... waarschijnlijk staat ie nog gewoon ingelogd en kunnen we gewoon door je Dropbox gaan scrollen. Dan is het alleen de vraag: hoe
kunnen we het zo doen dat je het niet in de gaten hebt en dat dan eenmalig of periodiek gebeurt? Dat is natuurlijk wel de vraag: wil je één keer informatie of structureel? Vooral van het laatste moet je iets beter nadenken over: wat kan ik doen zodat jij het niet in de gaten hebt? Kijk, nu staat die laptop hier tegenover mij. Als ik ergens een pand binnen moet gaan lopen om dat te gaan doen, fysiek met iemands computer... Ik zit liever lekker achter mijn bureautje. Gewoon lekker achter de knoppen te bonken.

LIESBETH

Dat snap ik.

DAVID

Ja, maar over het algemeen... Als wij een operatie doen, gaat dat verder dan alleen een enkel systeem. We hebben ook een afdeling die enkele systemen target, maar de operators gaan over het algemeen op echt grote netwerken van bedrijven. Dan zijn het gewoon meer computers aan elkaar geknoopt.

LIESBETH

Uiteraard is mijn specifieke Dropbox over het algemeen niet de plek waar hackers van Davids statuur veel te zoeken hebben, maar toch wil ik graag weten wat ik nou kan doen om mezelf beter te beveiligen. Behalve mijn laptop niet achterlaten als ik een keertje naar de wc ga.

DAVID

Nou, dat is inderdaad, dus een stukje: waar laat je 'm liggen? Als je bij de Starbucks zit te computeren, laat je dan je computer daar staan als je even naar het toilet loopt? Of neem je 'm even mee? Anderzijds, altijd nadenken: waarvandaan haal je je software? Haal je het van de officiële vendor vandaan of denk je: nou, wat minder legale websites kunnen mij ook helpen. Of heb je antivirussoftware? Dat helpt toch altijd tegen de veel voorkomende, al bekende bedreiging. En heel eerlijk gezegd denk ik dat als iemand echt een gerichte aanval wil doen op jou, dan ga je het toch niet voorkomen.

LIESBETH

Een terugkerend geluid. Ellen zei het ook al: als iemand echt je systeem in wil, dan lukt ze dat wel.

LIESBETH

Dan onze zaak. We willen de buitenlandse server hacken om erachter te komen waar die mee communiceert. En daarvoor kloppen we bij David aan. Wat kan hij voor ons betekenen in een onderzoek als dit?

DAVID

Het begint altijd met de vraag: wat wil je bereiken? Wat is het doel? Waarom moeten we dit gaan hacken? Hacken om te hacken doen we niet. In dit geval is het de informatie binnenhalen van die tweede C2-server. Dan willen we graag zo veel mogelijk informatie over dat systeem dat al bekend is. Dus hebben we toevallig al gegevens dat we weten of we al kunnen verbinden ermee, dat we ook kunnen authentiseren met dat systeem. Wat voor software draait daar? We gaan natuurlijk zelf ook enig onderzoek naar doen. En dan wachten we eigenlijk tot artikel 45 last geschreven is, de last waaronder wij werken. En dat moet dan een A en een B zijn voor het binnendringen en een A voor het vooronderzoek. En dan gaan we aan de slag. Ja, net als dat spreekwoordelijke huis, we gaan rammelen aan de deuren. We gaan even kijken: wat draait er? Wat is het aanvalsoppervlak? Dus we gaan scannen, we gaan in kaart brengen. Hoe beheren zij de server? En wat kunnen wij uiteindelijk met de gegevens die we hebben en wat we aantreffen bij die server? En de software die we hebben aangetroffen op het eerste niveau kunnen wij analyseren, dus we gaan bij CNE de software reverse engineeren. We gaan kijken wat andere afdelingen eventueel al met die software hebben gedaan. En dan gaan we kijken: kunnen we daar bijvoorbeeld misbruik van maken van die software en het gaan analyseren? Hoe praten de servers met elkaar? Kunnen wij patatje troep opsturen en dan crasht de server? Wat we ook wel fuzzen noemen. Dus we sturen gewoon allerlei input die kant op om te kijken: waar gaat het stuk en kunnen we analyseren waarop het stuk gegaan is? En wat betekent dat dan? Dus als ik heel veel A'tjes die kant op stuur en op een gegeven moment ligt dat ding op z'n gat... In de testopstelling kan ik dan terug traceren: waar is dit stuk gegaan en kan ik daar wat mee? Kan ik invloed krijgen over de flow van het proces om uiteindelijk dus uiteraard mijn code uit te voeren? En kan ik dus iets in die A'tjes stoppen wat uiteindelijk een payload is om uit te voeren? Als dat het geval blijkt, dan kunnen wij hopelijk de tools uitvoeren die we nodig hebben om volledige toegang te hebben en de informatie in beeld te halen die we nodig hebben.

LIESBETH

Is het een moeilijke, wordt het een moeilijke hack?

DAVID

In de praktijk valt wel te stellen dat als iemand een server huurt op het internet, het aanvalsoppervlak niet altijd groot is. Dus je zult heel goed je best moeten doen om binnen te komen. Maar elke situatie is anders.

LIESBETH

Omdat het huren van een server dusdanig veel moeite kost en dusdanig anoniem is dat je nog meer ongezien kunt blijven, is dat...

DAVID

Nee, wat ik bedoel te zeggen is dat over het algemeen de virtual private server, de VPS die gehuurd wordt door diverse mensen... Standaard staat eigenlijk alleen het beheerprotocol SSH, de Secure Shell, open. En dus is er heel weinig aanvalsoppervlak, je hebt eigenlijk maar één pootje binnen, zeg maar. En dan moet je wel net dat pootje kunnen gebruiken om je werk te doen.

LIESBETH

Want de rest is gewoon zo...

DAVID

Dichtgezet. En daar draait ook niks, want dat is gewoon een kale server, dus het is net afhankelijk van wat dus de eigenaar daarop gaat draaien. Gaat ie er een webserver op draaien? Heeft hij een of ander eigen pakketje geschreven die de C2-server-software bijvoorbeeld die er standaard draait, waar wij misschien wat mee kunnen? Het is net afhankelijk van: wat doet de eigenaar met de server wat ons potentieel meer aanvalsoppervlak geeft? Dan koppelen we dat soms terug naar het team van: Nou, we verwachten dat de kans van slagen klein, middelhoog is. En dan maken we een inschatting van: wat is het laagste risico binnen de aanvalsmethodiek? Als de voordeur open staat, ga ik natuurlijk niet een ruit aan de achterzijde van het huis inslaan, dus dan ga ik gewoon kijken: is het goed om de voordeur te gebruiken? We maken natuurlijk afwegingen van: o, weten we wie de gebruikers zijn? Op welk moment zijn die actief? Gaan we dan juist ook op dat moment naar binnen? Of gaan we daarbuiten naar binnen? Dus moeten we onze werktijden verschuiven? Hoe moet onze infrastructuur eruitzien? Dat zijn allemaal zaken waar we dan zo mee gaan lopen puzzelen. Dan hopelijk als we goed hebben geïnvesteerd op die open deur, dan zijn we eindelijk binnen.

LIESBETH

Is het ook weleens gebeurd dat jij bijvoorbeeld wel dus gezien bent en dat je dat dan weet? Dat je dus weet: o shit, we zijn erbij.

DAVID

Uiteraard doen wij ons best om ons werk zo heimelijk mogelijk te doen. Het kan zijn dat je een keer tegen de lamp loopt. Ja, daar doe je dan niks aan. Soms heb je dat in de gaten. Soms is je verbinding ineens weg.

LIESBETH

Maar is het dan stress? Zit je dan bezweet achter je bureau of...

DAVID

Als zoiets gebeurt, dan kan dat vrij stressvol zijn, want je gaat gelijk je stappen terug traceren van: ligt dit aan mij? Is dit een tijdelijke hick-up wat hier nu gebeurt als mijn verbinding in één keer wegvalt? Het kan ook zomaar zijn dat er een keer ergens onderhoud werd gepleegd en dat er niks aan de hand is. Dan ben ik aan het stressen voor niks, zeg maar.

LIESBETH

Tot slot vraag ik David wat hij van een zaak als deze vindt.

DAVID

Het is een... Ik zou willen zeggen een spannende zaak, omdat natuurlijk een klein beetje onduidelijk is wat nou de uiteindelijke intentie is van de actor, maar we wel een klein beetje durven te gokken misschien voorzichtig.

LIESBETH

Ja, dat begint toch ernstig op sabotage te lijken?

DAVID

Nou ja, inderdaad. Dus ja, daar wil je toch graag zicht op krijgen van: wie is dit aan het doen? En zijn we de enigen of niet?

LIESBETH

Ik zou best wel eens een dag naast hem aan het bureau willen zitten wanneer hij in zijn woorden 'achter de knoppen zit te bonken', maar helaas, dat deel van de dienst is ook voor mij verboden terrein. Hij gaat in ieder geval verder met de operationele kant van de case en ik ga terug naar analist Anouk. Want ook al speelt alles zich af in computers, een hack van deze omvang heeft wel degelijk effecten op de buitenwereld. Wanneer wordt die ingelicht? En hoe doen we dat?

ANOUK

Toen we hoorden dat die malware aangepast was en dus op zoek ging naar SCADA ICS-systemen, toen ging er bij ons wel een belletje rinkelen van: hé, het lijkt erop alsof het spionageoogmerk van die malware die we eerder hebben gezien, omgeslagen is in een sabotageoogmerk. Dat moet de buitenwereld wel weten. Althans, onze Haagse partners.

LIESBETH

Zaken als dit worden niet via een mailtje even naar Den Haag gestuurd. Anouk heeft de zaak al besproken met Erik Akerboom, de hoogste baas van de AIVD. Dit is de directeur-generaal, afgekort met DG. Hij zal uiteindelijk de betrokken ministers op de hoogte stellen.

ANOUK

Schriftelijk zou dus al niet handig zijn, want dan, ja, dan gaat het toch wel wat onrust veroorzaken. Dus het is ook heel belangrijk dat we dit warm overdragen. Goeie uitleg erbij geven en dat we een heel goed onderscheid maken tussen: wat weten we, wat weten we zeker en wat hebben we uit de inlichtingen gehaald? En hoe duiden we dat? Omdat het natuurlijk allemaal heel technisch is, moeten we ze heel goed meenemen in: wat weten we en hoe beoordelen wij dat? En omdat we het mondeling willen doen en het ook belangrijk is dat het op het hoogste niveau gebeurt, moeten wij ook aan de AIVD-kant daar onze hoogste persoon voor inzetten. En vandaar dat ik DG heb gevraagd of hij het mee wil nemen naar de RVI.

LIESBETH

De RVI is de Raad voor de Veiligheid en Inlichtingendiensten. Dit is een onderraad van onze ministerraad die in politieke zin sturing geeft aan de geheime diensten en bestaat uit de volgende personen.

ANOUK

Nou, sowieso natuurlijk onze eigen minister van Binnenlandse Zaken en de minister van Defensie, want dat is het departement waar de MIVD toe behoort. Maar daarnaast heb je natuurlijk het ministerie van JenV dus de minister van JenV. De minister van Buitenlandse Zaken. Die zitten dus ook allemaal in die RVI. En de RVI wordt voorgezeten door de minister-president.

LIESBETH

En al die mensen zitten dan bij elkaar in een kamer?

ANOUK

Zeker. En zij bespreken dan zaken die er in de inlichtingenwereld spelen en die voor hun eigen portefeuilles van belang zijn.

LIESBETH

En wat gaan zij daar dan mee doen? Wordt er dan een scenario gemaakt voor wat er gaat gebeuren als het de actor wel lukt?

ANOUK

Ja, iedereen binnen de veiligheidsketen heeft natuurlijk z'n eigen rol die hij moet vervullen. Onze rol is dat we ze moeten informeren van hetgeen dat er speelt en zij hebben binnen hun eigen ministerie natuurlijk een eigen rol te vervullen. Wie welke rol exact heeft, is denk ik ook niet aan mij om helemaal uit te leggen. Maar de NCTV zal waarschijnlijk wel iets van scenario's gaan opstellen.

LIESBETH

Nationaal Coördinator Terrorismebestrijding en Veiligheid, ofwel NCTV. Zij spelen een belangrijke rol. Het is een instantie die samen met partners binnen overheid, wetenschap en bedrijfsleven ervoor zorgt dat de Nederlandse vitale infrastructuur veilig is en blijft. Dan Anouk begint met het schrijven van een inlichtingenbericht en weegt goed af wat er wel en niet in wordt verteld.

ANOUK

Wat ik er wel uitlaat en waar best wel eens een discussie over bestaat, is Elektron BV. Ik zal die niet noemen in m'n inlichtingenbericht. Dat is namelijk best wel naming and shaming en dat is onnodig in dit geval.

LIESBETH

Het lijkt me juist heel nodig.

ANOUK

Waarom? Waarom vind je het nodig?

LIESBETH

Je moet toch vertellen wat er aan de hand is? Als in, het gaat er toch om dat Elektron BV mogelijk uit kan vallen en dat alle mensen die daarop aangesloten zitten daar dus problemen van gaan hebben?

ANOUK

Het kan eigenlijk lezers triggeren om acties te ondernemen die we niet wenselijk vinden. Zo zou een lezer bijvoorbeeld kunnen denken: ik ga ernaartoe, want wij van ons ministerie zijn verantwoordelijk voor wat dan ook en in dat kader willen wij toch wel graag even met het slachtoffer zelf gaan praten. Dan kunnen dingen toch een soort van... ja, uitlekken is misschien niet zo'n mooi woord. Het kan wel breder bekend worden dan wenselijk is. Het is voor hoogambtelijk en ministerieel niveau van belang om dit te weten, zodat zij hun eigen rol ook kunnen vervullen. Maar zij hoeven niet per se te weten welk bedrijf het precies is. Want het kan bij Elektron BV gebeuren, of daar hebben wij het nu gezien, maar wie zegt dat ze niet ook al ergens anders binnen zitten?

LIESBETH

O ja, o ja, dat had ik me echt nooit bedacht. Ik dacht dat het daarmee zou beginnen bijna, dat je zou zeggen: we hebben iets gevonden bij Elektron BV, maar juist niet dus.

LIESBETH

Stel, de minister van Buitenlandse Zaken hoort dit op maandag en heeft een vermoeden uit welke richting dit komt en heeft op dinsdag een afspraak met de ambassadeur van dat land. Hoe werkt dat?

ANOUK

Nou, hij kan hier niks over zeggen. Hij zal hier ook niks over zeggen. Maar in het achterhoofd kan het natuurlijk wel meegenomen worden. Je bent natuurlijk wel extra alert en voorzichtig misschien in een dergelijk gesprek. Wij zullen ook in het inlichtingenbericht schrijven dat Elektron BV of tenminste de energieleverancier bij ons heeft aangegeven de malware inmiddels uit het systeem verwijderd te hebben. Dus dat is dan de feiten die we daar in zullen schrijven, dat wat we gehoord hebben. Dat kunnen we zelfs ook geverifieerd hebben of dat klopt. Maar onze duiding kan dan zijn: ondanks dat ze aangeven dat ze de actor uit hun systeem verwijderd hebben, betekent niet dat de actor er niet meer in zit. Zelfs als ze nu helemaal uit het systeem zouden zijn, dan nog is er een redelijke kans dat ze weer terug gaan komen en opnieuw in het systeem proberen te komen.

ANOUK

En wat we natuurlijk ook moeten doen, is de sector op de hoogte brengen. Ik denk niet dat de statelijke actor per se deze energieleverancier heeft willen raken. Hij heeft bij deze partij een ingang gevonden om binnen te komen, maar het had misschien ook een andere partij kunnen zijn. En om Nederland veilig te houden, willen we eigenlijk dat ze niet binnen komen bij de andere.

LIESBETH

De zaak is nu dus deels in politiek Den Haag en ik ga terug naar Tom.

TOM

Liesbeth, wat vond je ervan en heb je je eigen zwarte hoodie al besteld?

LIESBETH

Nou, bijna wel eigenlijk, moet ik zeggen. Ik vond het wel vet. Kun jij dat ook, hacken?

TOM

Niet op het niveau waarop hij het kan, nee, absoluut niet. Maar ik ga niet ontkennen dat ik niet die interesse ook heb en daar ook wel stiekem, soms thuis een beetje op oefen.

LIESBETH

En wat betreft onze zaak. Wat gaat er gebeuren. Wat doen we nu?

TOM

Nou, we gaan vol spanning om te beginnen maar gewoon wachten. David is begonnen. Het verkennen is gestart...

LIESBETH

Met de hack, bedoel je?

TOM

Met de hack, zeker. En nu is het gewoon de vraag of het allemaal gaat lukken. En ja, stiekem hoop ik gewoon dat ik op werk kom en nog even in de chat kijk en dan zie: Last message van David, 4 uur 33. Dat is meestal een goed teken dat dingen geslaagd zijn. Dus daar gaan we heel hard op hopen. En ja, wat we gaan aantreffen precies, daar durf ik bijna geen voorspellingen over te doen nog. Want ik weet het gewoon niet.

LIESBETH

Oké, we hebben David die de server probeert te hacken. Meerdere ministers houden de case nu rechtstreeks in de gaten via de hoogste baas van de AIVD. En ook al zei Tom dat het attribueren het moeilijkste is in zijn werk, ik voel dat we dichterbij komen. In de volgende en laatste aflevering: wat komt er uit de hack? En wat dan? Voor wie meedoet met ons onderzoek heeft Tom vandaag een heel bijzondere challenge.

TOM

Als je zelf wil laten zien hoe goed je bent en of je het niveau hebt om bij de AIVD te komen hacken, kijk dan vooral even op operatiepositron.nl, want daar kun jij ook inbreken in deze server. Veel succes.

LIESBETH

Dit was de vijfde aflevering van De Dienst, een podcast van de AIVD, gepresenteerd door mij, Liesbeth Rasker, en geproduceerd door Het Podcast Kantoor in samenwerking met Werk Merk.

Abonneer je nu, zodat je niets van dit nieuwe onderzoek hoeft te missen. En laat ons vooral weten wat je van deze serie vindt in een recensie in je favoriete podcastapp.