Operatie POSITRON aflevering 1: Welkom in Cyberspace

JACOB

Het is niet uit te sluiten dat er landen actoren zijn die het echt als een middel gebruiken om te saboteren. En dan zou je kunnen denken aan het stilleggen van bankverkeer, dus dat je niet meer kan pinnen. Of het stilleggen van energiebedrijven, dat we geen energie meer hebben. Dus dat zijn zaken waar wij in dit land er allemaal van uitgaan, dat dagelijks... Dat dat gewoon goed werkt. Dat we een telefoon kunnen opladen. Dat we morgen gewoon geld kunnen pinnen.

LIESBETH

Ja.

JACOB

Maar als dat opeens wegvalt, dan zou dat vrij disruptief zijn.

LIESBETH

Het is bijna een jaar geleden dat ik voor het laatst het grote grijze gebouw van de AIVD uitliep, toen ik een contraterrorisme zaak had doorlopen die draaide om de mogelijke aanslag van Sander. En nu ben ik terug. Terug in Zoetermeer, terug bij de geheime dienst. COMPUTERSTEM Bezig met scannen van het document. Draai het document om alstublieft.

LIESBETH

Voor een nieuwe stage, ditmaal bij de Cyber Desk, met dus ook een nieuwe zaak.

JACOB

Een van de grote bedrijven in Nederland, één van de grote energieleveranciers is Elektron BV. We hebben informatie ontvangen dat zij het doel zijn van een hack.

LIESBETH

Ik mag vragen stellen aan mensen die nooit over hun werk praten, op een plek waar maar zelden mensen van buitenaf komen. Mijn naam is Liesbeth Rasker. Je luistert naar het nieuwe seizoen van de podcast van de AIVD. Welkom bij 'De Dienst'.

JACOB

Welkom.

LIESBETH

Dank je wel.

JACOB

Welkom terug, wij De Dienst.

LIESBETH

Ja, dat euh...

JACOB

Deel twee.

LIESBETH

Ja, precies. Dit is nu m'n tweede stage. Tegenover mij zit Jacob, het teamhoofd van mijn nieuwe afdeling. Bij binnenkomst moest ik de hele veiligheidsprocedure weer doorlopen, die staatsgeheim is. Mijn telefoon en laptop liet ik achter in een kluisje en een beveiliger bracht me door een wirwar aan lange gangen naar de kamer waar ik nu met Jacob zit.

JACOB

Ik ben Jacob. En ik ben een leidinggevende binnen de AIVD, bij één van de cyber teams.

LIESBETH

Kun je me uitleggen: hoe belangrijk is cyber voor de AIVD?

JACOB

Cyber is één van de speerpunten omdat het één van de grote dreigingen is op dit moment voor Nederland en haar bondgenoten. En het zal niet heel gek zijn als je hoort dat het alleen maar meer zal worden. Kijk maar naar hoeveel wij digitaal doen als privépersonen, maar ook bedrijven doen. Ja, het digitale domein is een nieuw werkveld, en daarmee dus ook voor de AIVD.

JACOB

De AIVD heeft meerdere taken, en één daarvan is zich ook begeven op het cyber domein. En daarvoor Nederland veilig houden, maar ook inlichtingen vergaren over onze actoren die een dreiging vormen voor Nederland en of haar bondgenoten.

LIESBETH

Kun je mij in in één zin uitleggen wat Cyber is?

JACOB

'Cyber' is echt een containerbegrip voor heel veel eigenlijk aan het internet gerelateerde zaken. Je kan heel kinderachtig zeggen: Cyber is alles wat aan het internet hangt. Wij kijken naar statelijke actoren die een dreiging, een digitale dreiging vormen voor Nederland en haar bondgenoten.

LIESBETH

Het domein Cyber is dus groot en breed, maar de dienst richt zich op de dreiging vanuit statelijke actoren. Een statelijke actor is typisch AIVD-jargon voor 'een land'. De AIVD doet bijvoorbeeld onderzoek naar Rusland, Iran, China en Noord-Korea. Een andere term die je vaak voorbij zal horen komen is 'attribueren', wat zoveel betekent als 'toekennen aan'. Je probeert dus een bepaalde actie te attribueren aan een bepaalde statelijke actor. En die acties, die zijn er voortdurend. Maar achterhalen wie erachter zit is lang niet altijd zo makkelijk.

JACOB

Waar wij heel erg mee te maken hebben binnen de dienst, is dat uhm... Cyber is een relatief makkelijk middel voor statelijke actoren om in te zetten om informatie te vergaren. En helemaal naar Nederland, want Nederland is een kenniseconomie is als land onderdeel van heel veel internationale gremia. Het is een open land, heeft een goeie infrastructuur, en het is heel makkelijk voor die statelijke actoren om vanaf een afstand te proberen informatie uit Nederland te halen, voor hun eigen belang. En dan kun je denken aan een economisch belang, een politiek belang. En dat willen wij voorkomen omdat dat ons schaadt. Dat is een risico voor onze neutraliteit, er loopt kennis de deur uit, onze politieke positie kan ondermijnd worden... En wij als AIVD hebben de opdracht om dat te onderkennen en op te acteren, op te handelen.

LIESBETH

Is het dan ook zo, dat jij naar het NOS Journaal kijkt en je hoort iets over, I don't know, verkiezingen in land X. Gaat er dan bij jou meteen ergens iets aan van: 'oh wacht. De verkiezingen gaan daar spelen, dat kan belangrijk zijn, zus en zo'?

JACOB

Ja, als we ons werk goed doen dan horen we het eigenlijk... Dan weten we het al. Dan kunnen we duiden wat er op het journaal komt.

LIESBETH

Ja precies, jij weet het voordat het...

JACOB

Nou, dat niet. Maar als er iets gebeurt waarvan je, hè... Verkiezingen is een prachtig voorbeeld als dat gaat spelen. Zeker in Nederland, verkiezingen. Dat weten we allemaal, want die staan al ver vooruit gepland. Maar als er iets in het nieuws komt, dan is dat meestal een extra duiding bij iets waar we hier intern al onderzoek naar doen of mee bezig zijn. Zeker als het betrekking heeft op het onderwerp waar we hier mee bezig zijn, waar ik mee bezig ben.

LIESBETH

Ja, en is er iets te zeggen over hoe lang een onderzoek duurt? Gemiddeld? Vast niet hè?

JACOB

Nee, dat dat varieert van 5 minuten dat we iets hebben kunnen duiden en hebben kunnen bepalen: 'Oké, dit is niet wat het is, dit hoort niet bij ons'. En dat kan tot heel lang, tot hele lange periodes van onderzoeken...

LIESBETH

Moet ik dan denken aan maanden of aan jaren?

JACOB

Jaren. Eigenlijk is het aan een touwtje trekken van een grote bol wol. En je trekt heel langzaam aan dat touwtje om dat bolletje wol te ontrafelen.

LIESBETH

En wat zit er aan het eind van het bolletje wol?

JACOB

Ehm dat is een goeie vraag.

JACOB

Bij een aanval staat nooit heel groot in de code die ze schrijven 'From Russia' of...

LIESBETH

With love.

JACOB

'With love' ja, of 'hacked by Iran'. Dat zal nooit, dat zal nooit naar voren komen. Dus het zijn heel vaak hele kleine puzzelstukjes tezamen die duidelijk maken waar de actor van komt. Maar heel vaak is het ook dat we een heel groot en heel sterk vermoeden hebben, maar dat we niet... Een smoking gun vinden, is een hele grote uitdaging.

LIESBETH

Is er eigenlijk... Zitten er consequenties aan verbonden aan zo'n actie? Ik bedoel, jullie gaan niet Iran aanklagen, hè? Als in... Jullie zouden dat sowieso natuurlijk niet doen. Maar wat zijn de consequenties van dat soort hacks als je ze zo goed als zeker, of helemaal zeker, wèl kunt attribueren aan een bepaalde actor?

JACOB

Nou, volgens mij kan je dat van elkaar loskoppelen. De acties die daaraan kunnen liggen als je een aanval ziet, en dat is eigenlijk wat de actor is als... Welke staat er achter een attack zit, is dan nog niet eens zo heel belangrijk. En de acties die er aan kunnen zitten is dat wij willen dat de weerstand in Nederland, de digitale weerstand van Nederland omhoog gaat. Dus je kan informeren en alerteren bij partijen die mogelijk geraakt zijn van: weet dat dit in je systeem speelt. Daar kun je handel links perspectief aanbieden. Aan de andere kant kun je ook, als er niet direct een slachtoffer is, kan je wel in in meer algemene zin informeren over de dreiging die uitkomt. De Dienst publiceert er ook wel geregeld stukken over. Aan de andere kant, hè, waar je misschien meer naar doelt, is dat in het fysieke domein kun je natuurlijk, als land, kun je personen persona non grata maken. Dat is een heel... Dat is dan heel concreet. Dan, dan.. Een groepje diplomaten, meestal diplomaten, die kan je dan het land uitzetten.

LIESBETH

Bij de terrorisme zaak van vorig jaar, hadden we te maken met een geradicaliseerde scheikunde student die naar een IS trainingskamp afreisde en vervolgens met een tas vol explosieven op een Nederlandse snelweg achterover werd getrokken. Het gevaar en de dreiging van die zaak, en van andere onderzoeken naar terrorisme, dat hoef ik aan niemand uit te leggen. Maar het domein waar we ons nu bevinden is abstracter. En daardoor, voor een leek als ik, lijkt het dan ook misschien minder dreigend.

JACOB

Ook nu, ook in dit domein ook, waar jij nu stage gaat lopen, hebben te maken met een dreiging die consequent aanwezig is. De vorm en de uitkomst is alleen minder zichtbaar. Hè, de casus rond Sander [...] is natuurlijk heel... Is heel tastbaar, is heel... Dat spreekt heel erg voor zich, wat de consequenties voor het land, maar ook voor de direct betrokkenen kunnen zijn.

LIESBETH

Ja.

JACOB

Die consequenties zijn in in dit domein ook heel groot. Alleen ze zijn niet tastbaar. Het is heel abstract. Misschien om het wat concreter te maken is, wat je kan voorstellen is dat: Nederland is een is een rijk land in meerdere opzichten. We zijn onderdeel van grote internationale verbanden. De EU, de NAVO, de VN. We beschikken over heel veel economische kennis. We beschikken over heel veel politiek kennis door, ook door die verbanden. En dat is voor andere actoren heel erg interessant. Ehm, en die hebben het ook echt wel op ons gemunt. Dus die zitten... Ja, mijn inschatting is, maar dat is dan ook maar soms hoe ik er over nadenk... Die zitten ook in een soort bureaucratisch systeem waarbij ze Nederland, of de instanties die hier werken, als doelwit het hebben gemunt. En die zetten om acht uur de computer aan, en die zijn gewoon... Ja, hun hele werkdag bezig om te kijken of ze in een in een Nederlands systeem kunnen binnendringen.

LIESBETH

Ja.

JACOB

En dat gaat, dat gaat dagen, weken gaat dat door, om maar net informatie naar boven te halen voor hun eigen gewin.

LIESBETH

Ja.

JACOB

Het is niet uit te sluiten dat er landen actoren zijn die het echt als een middel gebruiken om te saboteren. En dan zou je kunnen denken aan het stilleggen van bankverkeer, dus dat je niet meer kan pinnen. Of het stilleggen van energiebedrijven, dat we geen energie meer hebben is. Dus dat zijn zaken waar wij euh, in dit land er allemaal van uitgaan dat dagelijks... Dat dat gewoon goed werkt. Dat we een telefoon kunnen opladen. Dat we morgen gewoon geld kunnen pinnen. Maar als dat opeens wegvalt, dan zou dat vrij disruptief zijn.

LIESBETH

Maar Nederland speelt nog om een andere reden een belangrijke rol als het gaat om cyber. Misschien herinner je je nog van het vorige onderzoek dat in ons land veel belangrijke internet kabels samenkomen. De Amsterdam Internet Exchange is een van de grootste internetknooppunten van de hele wereld. Dat maakt het aantrekkelijk om via Nederland digitale aanvallen uit te voeren.

JACOB

legt het verder uit.

JACOB

Er komen letterlijk heel veel kabels vanuit euh, vanuit heel de wereld komen op dat punt samen. Daar gaat dus ook heel veel internetverkeer over langs. En aan de andere kant hebben wij in Nederland, doordat we een heel welvarend land zijn, een hele goeie infrastructuur. Ehm. En we hebben een heel stabiel land. En die twee tezamen zorgt ervoor dat we hier heel veel infrastructuur hebben. Wat eigenlijk nooit uitvalt, wat heel snel is en wat heel interessant is voor andere actoren om gebruik van te maken. Ten behoeve van hun, digitale aanvallen op andere landen. Wat je nooit zult zien is dat iemand in Moskou op zijn computer inlogt en direct vanuit zijn eigen computer met een internetverbinding, naar, naar zijn doelwit gaat, wat dat dan ook mag zijn. Dat dat gebeurt doormiddel van heel veel stapjes en op verschillende wijzen is over het internet heen. En heel vaak is... Of, het gebeurt geregeld dat Nederland een van die, van die stapjes is. Dus dat ze via Nederland en misschien nog zes andere stappen ergens proberen binnen te komen. En waarom is Nederland dan heel interessant om te gebruiken? Omdat Nederland een heel stabiel netwerk heeft. Dus je hoeft je niet zorgen te maken dat opeens 's avonds de elektriciteit wegvalt en dat jouw, een onderdeel van jouw aanvalsroute, een onderdeel van jouw digitale aanvalsroute opeens offline is. Je hoeft je ook geen zorgen te maken dat hier morgen opeens een staatsgreep is, waardoor ook het internet er hier wordt uitgetrokken. Uhm is het is dus een hele... Het is een hele prettige omgeving om...

LIESBETH

Vanuit hier kun je dus vrij makkelijk...

JACOB

...overal terecht.

LIESBETH

Ook al zijn digitale dreigingen minder zichtbaar, ze zijn dus wel degelijk aanwezig. En veel ook. Om je een idee te geven: er werden de afgelopen jaren 300 hack-pogingen per uur ondernomen op de Belastingdienst. Ter voorbereiding op de gesprekken die volgen heb ik uiteraard mijn research gedaan. Maar om nou te zeggen dat ik echt helemaal tot in details snap hoe mijn e-mails verzonden worden? Nee. Maar de impact van cyber en juist de grote rol die het in mijn dagelijks leven speelt maken me wel nieuwsgierig en leergierig. Tijd om te beginnen.

JACOB

Wat jij hier kan verwachten de komende periode is dat je een tijdje mee gaat lopen met Tom. Dus is een bewerker in mijn team hem. De rol van bewerker is eigenlijk onderzoeksleider. Tom is de spil van het onderzoek en die zorgt ervoor dat de juiste vragen worden gesteld, de juiste middelen worden ingezet. En daar ga jij in meedenken.

LIESBETH

Dus Bart nam me vorig jaar op sleeptouw, ditmaal heb ik Tom aan mijn zijde.

TOM

Ja, goedemorgen. Nou, ik ben Tom en ik ben op het moment bewerker bij de AIVD, en op een cyber onderzoek. We hadden begrepen dat je jezelf wilde verbreden in je bewerkersvak en zodoende ben je bij mij terechtgekomen.

LIESBETH

Ja.

TOM

Ja, het wordt wel heel anders, ja.

TOM

Het feit dat alles met elkaar verbonden is, dat principe alles met het internet verbonden is en alles met elkaar kan praten, levert toch wel een unieke set aan kwetsbaarheden en dreigingen op. En daar doen wij onderzoek naar.

LIESBETH

Oké. Om alles wat volgt wat beter te kunnen begrijpen: hier een klein geschiedenislesje. Op 4 oktober 1957, om precies te zijn om half acht 's avonds, sturen de Russen de allereerste satelliet de ruimte in, Spoetnik genaamd. Het is een klein zilver bolletje en dat kleine bolletje is een gigantische doorbraak in de technologie race. De Amerikanen kunnen dan niet achterblijven en bedenken een manier waarop hun onderzoeksuniversiteiten en het ministerie van Defensie, nog sneller met elkaar kunnen samenwerken. Mocht je hier echt alles van willen weten, zou ik zeggen: doe even een rondje Wikipedia. Maar voor nu is het voldoende om te weten dat ze lokale netwerken met elkaar gaan verbinden, waardoor opeens iemand die in Chicago zit een berekening kan uitvoeren op een computer die eigenlijk in Seattle staat. Helemaal aan de andere kant van het land. Het Amerikaanse netwerk en Europese netwerken worden met elkaar verbonden, en uiteindelijk resulteert dit in wat wij nu het internet zijn gaan noemen.

TOM

Het feit dat alles met elkaar verbonden is, betekent dus ook dat alle bedrijven met elkaar verbonden zijn. Alle overheden zijn met elkaar verbonden. Ja, en dat biedt gewoon ontzettend veel mogelijkheden voor een lekker potje spionage. Ehm... Want de meeste dingen die interessant zijn om te weten tegenwoordig, en om te stelen, staan gewoon op iemands computer, uiteindelijk.

LIESBETH

Ja.

TOM

En dat is allemaal bereikbaar via het internet. Als je toegang kunt krijgen tot de systemen. Iemand kan het in principe doen in z'n eentje, achter z'n eigen toetsenbord thuis, en dat maakt het allemaal heel aantrekkelijk voor spionage en gerelateerde zaken.

LIESBETH

En dat maakt het ook aantrekkelijk voor Tom. Wat dat betreft voldoet hij aan het cliché beeld dat ik heb van mensen die overweg kunnen met computers. Zo'n liefde zit er gewoon van jongs af aan al in.

TOM

Ik weet nog dat ik altijd een fascinatie had met Efteling.nl. Dat is echt heel bizar. Als kind ging ik altijd naar die website, en ook om uit te printen ook. En als je dan terugdenkt, denk je: waarom ga je er in hemelsnaam een website uitprinten? Maar dat was voor mij echt alles. Dat, en dat gecombineerd met mijn basisschool... Daar hadden we een leraar en ik geloof dat hij Jo heette. En hij nam altijd ouwe computers, ouwe printers, ouwe dingen nam 'ie gewoon altijd mee naar school. En dan donderdagmiddag kon je, op een soort crea-middag... Eén van de dingen die je kon doen, was met Jo al die dingen uit mekaar gaan halen...

LIESBETH

Wat geweldig.

TOM

...en gewoon te kijken wat er inzit. En ja, nee... Als 9, 10 jarig jongetje begreep ik echt niet wat het allemaal was. Dat je dingen als de cpu en de harde schijf en het geheugen, dat kun je er wel een beetje uithalen. Eh, maar wat er precies allemaal deed en dat wist ik ook niet. Maar goed, dat heeft op een moment die interesse aangewakkerd. En dan ga je gewoon dingen lezen en opzoeken. Van ja, hoe werkt het nou precies? Ik heb iets gestudeerd wat helemaal niks te maken heeft met het vakgebied. Maar omdat ik vanaf kinds af aan al die interesse had voor alles cyber, en alles computers, en alles internet... Uhm, heb ik eigenlijk na mijn studie soort van de vraag 'wat wil je nou gaan doen' beantwoord met 'ik wil iets in de cyber wereld doen'.

LIESBETH

Wat heb ik gestudeerd dan? Je zegt dat het helemaal anders is.

JACOB

Wat ik precies gestudeerd heb, dat wil niet vertellen. Maar ik kan wel zeggen dat ik de hele academische ladder doorgelopen ben tot aan mijn uiteindelijke PHD toe. Niet echt noodzakelijk denk ik, maar ik vond het gewoon ontzettend leuk om die hele wereld gewoon mee te maken.

LIESBETH

Toen dacht je ik wil in de cyber...

TOM

Ik wil in de cyber, en letter exact op dat moment zag ik gewoon letterlijk een vacature online voorbij komen voor bewerker met een cyber achtergrond bij de AIVD. En ik heb mijn kans gegrepen.

LIESBETH

En en wat doet een bewerker bij de AIVD, op de Cyber afdeling?

TOM

Uhm... Uiteindelijk best wel hetzelfde als een bewerker bij een contraterrorisme afdeling zou doen. Alleen onze targets zijn iets anders, dus we zijn nog steeds op zoek naar 'waar is de dreiging en hoe kunnen we die dreiging onderkennen'? En van wie gaat de dreiging uit? Want realiseer je wel,uiteindelijk: het zijn allemaal computers en het klinkt allemaal heel abstract. Maar uiteindelijk zit er ergens iemand achter z'n toetsenbord commando's in te voeren om onze geheimen te jatten.

LIESBETH

Ja.

TOM

Dus dat is allemaal hetzelfde.

LIESBETH

En dat is een goed punt. Want zodra het over surfers, netwerken en internet protocollen gaat, is het makkelijk te vergeten dat die dingen niet uit zichzelf handelen. Er zit iemand achter, iemand geeft een opdracht en die iemand is wel degelijk een echt persoon. Tom en zijn team doen onderzoek naar die figuren, die dus voor een statelijke actor kunnen opereren. Als ik een voorstelling moet maken van het bureau waar Tom die onderzoek aan uitvoert, dan doemt er een beeld op van een plek vol bliepende computers en knipperende beeldschermen.

TOM

Vijf.

LIESBETH

Vijf?

TOM

Vijf. Ja, vijf computers en vijf beeldschermen. En dit heeft natuurlijk alles te maken met wat ik eerder zei, dat al die computers allemaal met elkaar verbonden zijn.

LIESBETH

Ja.

TOM

Ja, dat willen we natuurlijk niet, want bij de eigen idee hebben we flink wat geheimen die ook geheim moeten blijven. En ja... De meest praktische en de toch wel, uiteindelijk, denk ik, de beste manier om dat te doen is om gewoon die netwerken fysiek van elkaar te scheiden. Dus we hebben gewoon binnen losse netwerken met verschillende doelen. Ja die gewoon niet met elkaar mogenpraten. En vandaar dat ik dus vijf computers, vief schermen, vijf toetsenborden en vijf muizen heb. Dat is dus één

groot spaghetti op mijn bureau, en dat het nog zonder alle prullaria en koffiekopjes en al dat gedoe. Ja, nee, absoluut.

LIESBETH

Uhm, ik ben een hele normale computer gebruiker, in de zin: ik heb een laptop thuis en dat is het.

TOM

Ja.

LIESBETH

En ik weet er eigenlijk gewoon heel weinig van. Dus ik heb een hoop te leren, ook een hoop te begrijpen. En ik denk dat heel veel dingen die voor jou heel normaal zijn, ze voor mij al heel ingewikkeld zijn. Als we het al hebben over hackersgroep, hacker, dan denk ik al: ja oké, een hacker... Dan heb ik toch eigenlijk ook een soort cliché beeld voor me van een gast in een donkere hoodie op een zolderkamer. Maar volgens mij ligt het ook al wel weer iets genuanceerder.

TOM

Er is eigenlijk niet zoiets als 'een hacker'. Er is wel 'een hacker mindset'. Het idee dat je dingen op een dusdanig gedetailleerde manier en niveau wil grijpen, dat je ze eigenlijk kunt manipuleren en soort van kunt laten doen wat jij wil, zonder dat ze daarvoor ooit ontworpen zijn. Daar komt het een beetje vandaan, die mindset om echt tot in de details door te dringen van hoe een systeem werkt. En dat vervolgens naar je eigen hand te zetten. Dat is uiteindelijk 'hacken'. Alleen, dat kun je natuurlijk doen omdat je het leuk vindt, als een soort van hobby achtige situatie. Maar je kunt het ook doen om andermans systemen binnen te dringen en dan dingen te stelen. Dus dat is eigenlijk het hacken waar het over gaat. Uhm, en daar zijn natuurlijk meerdere vormen in. En wat we bij de AIVD volgen, en ook echt alléén volgen, zijn hackers die werken voor andere overheden, en die dus in die capaciteit Nederland en onze belangen aanvallen. Dat is waar onze focus ligt.

LIESBETH

Ja, dus dat zijn andere landen waarmee de AIVD...

TOM

Dat zijn andere landen. Wij kijken naar Rusland, China, Iran en Turkije.

LIESBETH

Oké

TOM

En Noord-Korea.

LIESBETH

Oké, ja.

TOM

Als bronnen van grote hack-aanvallen over de hele wereld.

LIESBETH

Ja, die zijn het beste in dit spel. Die kunnen... Die hebben ook de beste hackers dus in huis.

TOM

Nou, die vormen in ieder geval de grootste dreiging voor Nederland op dit moment. Ja, zeker.

LIESBETH

Het hele idee dat je überhaupt in een computer in kan breken vind ik al heel moeilijk te snappen.

TOM

Zeker.

LIESBETH

Wat... Hoe kun je mij uitleggen wat hacken is? Hoe dat werkt? Hoe... Hoe moet ik me dit visualiseren?

TOM

Nou, hacken is eigenlijk best wel goed te vergelijken met gewoon een fysieke inbraak. Stel, je hebt een inbreker, je hebt een hele mooie villa gezien en je denkt: daar kan ik een PlayStation 5 halen. Nou, eerste wat je gaat doen natuurlijk is kijken. Hoe ziet die villa eruit? Waar ligt die villa? Hebben deze mensen misschien beveiligingscamera's? Is het een drukke straat? Hoe laat gaan ze naar hun werk toe? Hoe laat komen ze terug? Zijn er kinderen, zijn er honden, al dat soort vragen. Basically:verkennen. En dat ga je in een digitale hack ook doen. Alleen dan op een server of op een computer. Welke software draait er? In welke netwerken hangt deze server? Hoe is deze server te bereiken? Het zijn, analogie, alle logische vragen aan elkaar, maar dan voor computers. Nou, en als je dat eenmaal gedaan hebt, ga je natuurlijk zoek naar: okay, zit er ergen een kwetsbaarheid? En in het geval van een inbraak is dat vrij simpel. Hoe kom ik binnen? Letterlijk en fysiek? Nou, misschien laten ze altijd dat raam open staan of hebben ze een oud katten klepje wat niet naar één kant, maar per ongeluk naar twee kanten open gaat omdat zo versleten is. Allemaal... je gaat op zoek naar dit soort kwetsbaarheden. In het geval van een server gaat het over kwetsbaarheden in software die op zo'n systeem draait. Nou als je dat gevonden hebt, dan kun je toeslaan.

TOM

Een heel triviaal voorbeeld is: neem... Je hebt een hele simpele 'Mijn Eerste Programma' geschreven. En dat programma vraagt de gebruiker om een naam. En jij typt dan mooi als gebruiker je naam in. En dan zegt hij 'hallo', en dan je naam. Hartstikke leuk, maar deze programmeur die het gemaakt heeft... Stel... Dacht niet zo lang na en heeft in zijn programma letterlijk gezegd: deze naam zal nooit langer zijn dan 50 karakters. Want wie heeft er nou een naam langer dan 50 karakters? Maar ja, een hacker is dan wel zo: oké, jij zegt 50 karakters. Ja, dan ga ik er natuurlijk eenenvijftig proberen. Gewoon eens kijken wat dat oplevert. Nou in zo'n scenario dan ga je dus veel te veel input geven dan dat het programma verwacht, en dan krijg je hele... Dan kun je hele gekke momenten krijgen omdat dat niet is wat de programmeur voor ogen had.

TOM

Het zijn foutjes in logica die gewoon door mensen gemaakt zijn, uiteindelijk. Dat is niet erg, dat is bijna onvoorkombaar. Maar daar kun je wel misbruik van maken door, soms, als een foutje op een dusdanig gevoelige plaats zit, een programma over te nemen en dat programma dingen te laten doen die jij wil. In plaats van waar het zelf voor gemaakt is.

LIESBETH

Heel simpel gezegd: hacken is speuren naar gaten in andermans werk en via die weg binnen zien te komen. Dat een buitenlandse overheid uit spionage overwegingen bij, ik noem maar wat, ons ministerie van Defensie zou willen rondneuzen, dat ligt voor de hand. Maar ook op de computers van gewone burgers zoals jij en ik valt genoeg te halen.

TOM

We hebben inderdaad overheden die hacken. Wat veel persoonlijker is, en waar mensen denk ik in het dagelijks leven veel meer in aanraking komen, zijn criminele hackers. Mensen die uit zijn op financieel gewin. Bekende voorbeelden zijn natuurlijk 'ransom ware', waarbij mensen inbreken in je systeem software droppen die al je bestanden versleutelt, en dan zeggen: ja, als je ons in bitcoins betaalt, krijg je al je bestanden terug. En er staat misschien voor jou niks staatsgeheims in. Maar het feit dat je opeens al je bestanden kwijt bent en niet meer kan werken. Je bent je foto's kwijt. Dat is toch schadelijk voor je. En ook iets wat wat de afgelopen paar jaar heel erg bekend is, en waar denkik de meeste mensen wel van gehoord hebben, is de zogenaamde de WhatsApp fraude, waarbij je vaak een sms-je krijgt van 'hé pap, mijn nummer is veranderd. Bij deze m'n nieuwe nummer. Ik ben een beetje blut kun je even 200 euro overmaken naar dit nieuwe rekeningnummer van mij, kusjes, bla bla. Nou, dat is ook weer zo'n stukje criminele cybercrime, waar echt wel veel, veel mensen in Nederland mee te maken krijgen.

LIESBETH

Met WhatsApp heb fraude werd in het eerste halfjaar van 2020 al 2,7 miljoen euro buitgemaakt. Maar toch is dit niet het werkveld van de AIVD, maar dat van de politie. De AIVD richt zich op de bescherming van de democratische rechtsorde. Om dat even in te kleuren, weer een klein beetje achtergrond. In december 2015 was er een storing bij een Oekraïens elektriciteitsnet, waardoor zo'n 80 duizend Oekraïense huishoudens dik zes uur zonder stroom zaten. Later bleek dat dit niet zomaar een storing was, maar een aanval van een Russische hackersgroep die de naam 'Sandworm' kreeg. 6 uur zonder stroom betekent zes uur zonder verwarming, midden in de winter. Maar betekent ook een gigantische ontregeling voor het openbaar vervoer, voor de financiële infrastructuur van een land, voor de veiligheid, kortom, voor de stabiliteit. En dat is dus precies waar de AIVD voor waakt.

TOM

Ja, dit soort... Dit zijn wel echt horror scenario's waar we bij de AIVD zeker onderzoek naar doen. En dat willen we echt koste wat kost voorkomen. Als we terugkijken op 2021: er zijn twee momenten geweest waarbij de NS helaas problemen had met hun communicatiesystemen. Zover wij weten niet gerelateerd aan statelijke actoren. Maar alsnog, wat je zag, was dat gewoon voor uren het hele trein netwerk in Nederland eruit lag. En de chaos op perrons, en mensen die niet thuis konden komen, en de gemiste werkuren... Dat is echt gewoon immens. Dus dat is echt een hele grote dreiging.

LIESBETH

Er is dus terroristische dreiging, dreiging van links- en rechts extremisme, en cyberdreiging. En dat laatste neemt in een verontrustend tempo toe, dus daar moeten we ons beter tegen zien te wapenen. Hoe de AIVD dat doet en hoe die onderzoeken lopen. Dat ga ik ook deze stage weer ondervinden door mee te lopen met een zaak. Een fictieve case, maar wel eentje met elementen die echt gebeurd zouden kunnen zijn of die kunnen gaan gebeuren.

TOM

Als AIVD hebben we natuurlijk het belang van Nederland en de veiligheid van Nederland voorop. En in die ja, weet je wel, in die rol houden we ook echt heel goed contact met de... Wat wij de vitale sector noemen. En een van de grote bedrijven in Nederland, en van de grote energieleveranciers is Elektron BV. We hebben informatie ontvangen dat zij het doel zijn van een hack.

LIESBETH

Oké, wat... Wat impliceert dat? Wat, euh, waar denk je dan?

TOM

Ja, in mijn achterhoofd ga meteen radertjes lopen. Want dit betekent dus feitelijk gezien dat er een groep mensen toegang heeft tot één van de grootste energiemaatschappijen van heel Nederland. Dat is nogal wat. Daar zitten nogal wat consequenties aan.

LIESBETH

Dat ze daar... dat ze daar aan de knoppen kunnen zitten.

TOM

Exact. Ja, precies. En waarom ze dat hebben gedaan, en hoe ze daar binnen gekomen zijn, en wie ze zijn of waar ze vandaan komen... Dat zijn allemaal vragen die we gaan beantwoorden, die we gaan proberen te beantwoorden.

LIESBETH

Maar hoe kom je er überhaupt achter dat ze gehackt zijn?

TOM

Ja, goeie vraag. In dit geval gaat het om een hackersgroep die we al eerder in onderzoek hebben gehad. Uhm, intern heeft deze groep de naam 'Zuurkool' gekregen. Blijkt dat het een groep was waar we tot ongeveer 12 maanden geleden echt actief onderzoek naar deden. Toen waar ze ook echt actief, heel veel slachtoffers gemaakt ook. Euhm. Maar daarna is het stil komen te vallen. Euh, en ja... Als het stilvalt en de actor lijkt verdwenen, dan moeten wij ons onderzoek afschalen. Want er is gewoon zoveel actiefs, dingen om te onderzoeken.

TOM

We hebben geen idee welke staat er achter zit. We weten wel vrij zeker dat het statelijke actoren zijn, het is gelieerd aan een overheid ergens. En ze hebben al sinds 2018 verscheidende slachtoffers gemaakt in Nederland. Ook buiten Nederland, Europa, ook wereldwijd, eerlijk gezegd. En dan gaat het voornamelijk om overheidsinstellingen. En dan hebben ze dat voornamelijk gedaan om te spioneren, letterlijk om geheimen te stelen. Beetje klassieke spionage, maar dan op internet.

LIESBETH

Dus een partij die al langer op de radar stond van de AIVD en in die onderzoeken de codenaam Zuurkool kreeg, is weer opgedoken. Ditmaal bij Elektron BV.

TOM

En een van hun kenmerkende technieken is inzet van een bepaald stukje malware. En die hebben we 'Rookworst' genoemd, en daar hebben we... Die kunnen we heel goed herkennen in internetverkeer. En wat er dus gebeurd is, is dat we op de SIGINT stroom is er een alert afgegaan...

LIESBETH

Wat is SIGINT? Wie is SIGINT?

TOM

SIGINT staat voor Signals Intelligence. Het is een euh... best wel centrale activiteit van de AIVD als het gaat om het cyberwereldje. Want alles in cyber speelt zich af op het internet en via SIGINT kunnen wij het, nou ja... Het internet in de gaten houden met als doel om Nederland veilig te houden aan en om dus kwaadwillenden te detecteren. En dat is hier gebeurd.

LIESBETH

Signals Intelligence. SIGINT, nog zo'n term die jij vaker gaat horen de komende afleveringen. Dit zijn inlichtingen die verzameld worden door het onderscheppen van signalen, bijvoorbeeld van pakketjes internetverkeer. We komen later nog een keertje terug op hoe dit precies werkt. De wet staat in ieder geval toe dat de dienst onderzoeksopdracht gerichte interceptie mag doen. Dat betekent dat ze onder hele strenge voorwaarden op vooraf bepaalde plaatsen verkeer van de kabel mogen onderscheppen,

om daarna naar eveneens vooraf afgesproken stukjes data te zoeken. Aan al het overige dataverkeer dat wordt binnengehaald wordt vernietigd en bij alles komt een hele batterij juristen aan te pas. En door SIGINT zijn ze dus een stukje malware tegengekomen. Dat is software die gebruikt wordt om computersystemen te verstoren, en die malware kreeg de codenaam Rookworst.

TOM

Dus we hebben pakketjes zien langskomen waarvan onze systemen konden vaststellen: dit is die Rookworst malware.

LIESBETH

En wat deed 'ie toen?

TOM

Ehm, niets meer dan zichzelf verbergen op het systeem, rustig dingen in de gaten houden. Hij kon bestanden downloaden. Met een moeilijk woord noemen we dat 'exfill'. Dat betekent gewoon dat de actor bestanden waar ‘ie in geïnteresseerd is download. En hij gaf ook de aanvallers de mogelijkheid om gewoon elke code, elke computer code uit te voeren op dat systeem wat ze wilden. Eigenlijk de klassieke spionage backdoor.

LIESBETH

Want nu inderdaad, wat er verder omheen hangt, dat weten jullie, nog niet.

TOM

Nee, we hebben geen idee. We hebben dus vast kunt stellen dat er de malware gelokaliseerd is in een netwerk bij Elektron B.V. Maar meer dan dat weten we nog niet.

LIESBETH

Nee. En omdat het dus zo'n belangrijke sector is, zijn dit dingen die jullie überhaupt altijd in de gaten.

TOM

Dit zijn dingen die we continu in de gaten houden. Absoluut. Want je kunt je voorstellen als Elektron B.V. plat gaat... Ja, dan gaat de Nederlandse samenleving echt, echt even op halt.

LIESBETH

Ja, en Rookworst, Zuurkool? Jullie... Dat soort codenamen verzinnen jullie er dan nog voor.

TOM

Oh ja, nee, alles in de AIVD krijgt een codenaam. Inclusief de cases die we nu gaan bewandelen. En die hebben we operatie Positron genoemd.

LIESBETH

Positron?

TOM

Jazeker, het antideeltje van Elektron.

LIESBETH

Het antideeltje van elektron. Hier heb je zeker heel veel pret om gehad.

TOM

Geen commentaar!

LIESBETH

Ja, heel goed.

LIESBETH

En daarmee is mijn tweede stage en de zaak officieel begonnen. Sigint, malware, internetprotocollen. Er komt een hoop nieuws op me af. In de volgende aflevering praat ik met iemand van de afdeling CND. Wat staat voor Computer Network Defence. Hij gaat me uitleggen wat dat inhoudt, en vooral hoe hij de oude hackersgroep weer op het spoor kwam en wat we tot op heden van ze weten. Voor wie alle termen die er bij zijn gekomen al lang gesneden koek zijn, heeft de AIVD iets bijzonders. Je kunt dit seizoen namelijk niet alleen meeluisteren. Je kunt ook met ons mee doen in de speciaal hiervoor opgezette challenge. Dat betekent dat je toegang krijgt tot de data die wij vinden en de dossiers die we er over aanleggen. Tom vertelt je wat de eerste opdracht is.

TOM

Mochten iemand willen meedenken, of zelf aan de slag willen: dan hebben we de inlichtingen dossiers online gezet op OperatiePositron.nl. Dus kijk maar hoever je komt. Kijk maar hoe goed je bent, en probeer alle vlaggetjes te vinden.

LIESBETH

Dit was de eerste aflevering van het nieuwe seizoen van De Dienst, een podcast van de AIVD, gepresenteerd door mij, Liesbeth Rasker en geproduceerd door Het Podcast Kantoor in samenwerking met WerkMerk. 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 podcast app.