Operatie POSITRON aflevering 3 - Nerden tot een uurtje of vier

ELLEN

Als je echt wil dat jouw geheimen over dertig jaar nog steeds helemaal veilig zijn, dan moet je ze uitprinten en in een kluis leggen. En alle andere geheimen... Ja, daar kan je digitaal gewoon mee aan de slag.

LIESBETH

Sinds ik aan deze zaak ben begonnen, zie ik overal om me heen cyber nieuws. Er was een grote storing in de beveiligingssystemen van de Amsterdamse metro. Er zijn Indiase afpersers die je foto's stelen en gebruiken voor pornografische deep fakes en een ROC in Den Haag kan al een maand hun computersysteem niet meer in door een ransomware aanval, waarbij 4 miljoen euro wordt geëist. De ouderwetse schoolborden staan daar met krijtjes en al weer in de lokalen.

LIESBETH

Maar in mijn omgeving hebben we het hier eigenlijk nooit over. Als ik mijn vrienden bijvoorbeeld vraag hoe zij op persoonlijk vlak hun digitale veiligheid hebben geregeld, word ik glazig aangestaard en worden de schouders ongeïnteresseerd opgehaald, terwijl een cyberaanval vele malen realistischer is om mee te maken dan een terrorisme aanval.

ELLEN

Wij zeggen altijd tegen onze klanten: ga er van uit dat je gehackt wordt op een tijd, op een moment en tijd, en neemt dan de juiste maatregelen zodat je de juiste detectie ook hebt.

LIESBETH

Mijn naam is Liesbeth Rasker. Dit is aflevering 3 van Operatie Positron, de podcast van de AIVD. Welkom bij De Dienst.

LIESBETH

Tom, er zitten hele kleine oogjes tegenover mij.

TOM

Ja, het was een beetje laat gisteren. We hebben toch een uurtje of vier zitten door nerden. We hadden eindelijk de data van Elektron gekregen, inclusief kopie van de implant, van de malware. Van tevoren hebben we ons de vraag gesteld: ja, wat zijn nou hun intenties dit keer? Doen ze nog hetzelfde als een jaar geleden of zijn ze volledig geswitcht? Nou, rond een uurtje of twee waren we er wel uit. En dingen zijn wel vrij serieus geworden op een gegeven moment.

LIESBETH

Want, oké, wat hebben jullie gevonden?

TOM

Nou, we kwamen erachter dat er een extra module in de malware zat, die specifiek op zoek was naar de industriële controlesystemen bij Elektron. En dat betekent eigenlijk maar één ding: dat is gewoon dat ze echt op zoek zijn naar de systemen die alle generatoren, alle switches, alles besturen. En dat doe je niet als je bedrijfsgeheimen wil stelen. Dat doe je als je een positie wil verwerven om misschien ooit dingen te saboteren.

TOM

RUSTIGE MUZIEK

LIESBETH

Als ik denk aan de hackers mindset waar hij me eerder over vertelde, zie ik voor me hoe hij en zijn collega's tot diep in de nacht met honderd bakken koffie en in een donker kantoor met fel verlichte computerschermen zitten. Om tot een zorgwekkende conclusie te komen. De aanvaller zit niet zomaar stiekem in de systemen. Hij wil ze ooit kunnen uitschakelen.

TOM

Ja, dat begint er wel heel erg op te lijken nu, ja.

LIESBETH

En wat... Wat... Wat doen jullie dan, als je er achter komt zo na zo'n nacht?

TOM

Nou, in eerste instantie gaan we gewoon door, maar eigenlijk net een stukje harder. Want we weten dat de stakes gewoon echt significant hoger geworden zijn. Maar dat we vooral nu, overdag, moeten we echt gaan nadenken. Wat moeten we gaan doen en waar zitten onze leads? En ja, hoe gaan we dit ontrafelen, wat er nou echt aan de hand is?

LIESBETH

Ja, want het is nog steeds niet duidelijk wie er dan achter zit.

TOM

Nee, volledig. Volledig niet. En nou hebben we natuurlijk een mooie lead. Want we hebben de malware, die zien we communiceren met een ander systeem van de actor. Dat is pannenkoekenpalazzo.nl.

LIESBETH

Pannenkoekenpalazzo.nl.

LIESBETH

Op het eerste gezicht is die site gewoon een site van een pannenkoekenrestaurant in Nederland. Niets aan de hand, maar nader onderzoek wees toch iets anders uit. Dat restaurant bleek namelijk helemaal niet te bestaan. En die site was niet zomaar een site.

TOM

Dus ze hebben een nep website opgezet. Volledig in het Nederlands ook. En toen we dat doorhadden, dan schrik je daar toch wel een beetje van. Want dat geeft je wel een hele sterke indruk van hoe voorbereid, en hoeveel man en daadkracht zo'n actor heeft, tot zijn beschikking. Als ze al zo ver willen gaan om te zorgen dat de decoy-website in volledig Nederlands is... Ja, dan hebben we wel met goeie, goeie mensen te maken.

LIESBETH

Die site is als het ware een vermomming, een manier waarop de aanvaller ongezien contact kan onderhouden met zijn malware. Tom, gaat je dit zo verder uitleggen. Het is in ieder geval een hele grote ontdekking en een goede stap dichter bij de actor. Maar we zijn er nog lang niet.

LIESBETH

En je kunt dan niet zomaar vinden van wie pannenkoekenpalazzo.nl is, of...? Want die site is dus van dezelfde...

TOM

Nee. Dit is natuurlijk een van de vragen die we ons meteen gesteld hebben. En we hebben bevoegdheden om dat na te vragen bij de plaats waar die website gehost is. Maar ja, in negenennegentig punt negenennegentig procent van de gevallen krijg je dan een fictieve naam terug, in een fictieve locatie, op een adres dat niet bestaat. En daar is ook nog vaak betaald met Bitcoin, dus...

LIESBETH

Dat is niet een route waarbij je waarbij je bij het einde komt.

TOM

Absoluut niet. Nee, het aanschaffen van deze infrastructuur op een anonieme manier is eigenlijk best wel simpel.

TOM

In dit geval staat het waarschijnlijk in Nederland, zowel omdat ze willen dat de communicatie naar die website minder opvalt bij Elektron. Ja, want het is niet zo raar als een medewerker van Elektron naar een pannenkoekenrestaurant website gaat om een tafeltje te reserveren voor die avond, bijvoorbeeld. Dat valt niet zo erg op, als je een beetje wil blenden in het normale netwerkverkeer bij Elektron BV.

LIESBETH

Ja, want dat wordt natuurlijk in de gaten gehouden. En ja, oké.

TOM

Zeker. Daar zit ook gewoon een security team achter. Met die mensen hebben we nu ook goed contact hierover.

LIESBETH

Hoe komt die malware nou hier? Nemen jullie dat mee op een USB stick, op een cd rom? Gaat dat via een e-mail? Hoe verplaatst zich dat, of hoe werkt dat?

TOM

Dat dat gaat gewoon per USB stick.

LIESBETH

Een USB stick?

TOM

Ja, en dat wordt op een nette manier op onze systemen geladen, en dan van vernietigen we de USB stick.

LIESBETH

Vernietigen jullie USB sticks, zo. Oké, dan staat het daar. Hoe kom je er dan achter dat dat die M.O. van van die malware veranderd is? Wat, wat doe je dan, als je die code denk ik hebt.

TOM

Ja, dus dan pakken we gewoon de code zoals we 'm op dat moment hebben. Die is geconfisqueerd. Daar gaan geen enkele leesbare strings meer in. Dus die gaat zo snel mogelijk Aida in. En daarnaast gaat ie ook nog een virtuele omgeving in waar we 'm gewoon dynamisch kunnen analyseren. We laten 'm gewoon draaien...

LIESBETH

Oké. In grote lijnen komt het hierop neer: op de USB stick staat de malware zoals die is gevonden bij Elektron. Die malware wordt in systemen geladen waar de AIVD idee mee werkt, zoals AIDA, een programma waarmee ze in detail kunnen zien waar het uit is opgebouwd. Vergelijk het met een microscoop. Vervolgens hebben ze de code van de malware stukje voor stukje ontrafeld, en op die manier vonden ze dat de malware op zoek was naar de SCADA systemen. Dat zijn meet- en regel systemen die voor de aansturing van industriële processen worden gebruikt. Simpel gezegd: als je daar controle over hebt, zit je direct aan de knoppen in de controlekamer van Elektron.

TOM

En aan de hand daarvan kunnen we terug redeneren wat voor functionaliteiten die allemaal heeft. En toen zagen we dat die met... O, X, F, E, geloof ik... Dat was een of andere code die die gebruikte, dat dat de functie was om te te gaan scannen op apparaten die spraken met het modbus protocol. En dat is een van de protocollen die onderliggend zijn aan een uitgebreid SCADA systeem.

LIESBETH

Dit kan allemaal alleen maar als je dus inderdaad die malware krijgt, dus degene waar dat gevonden is moet dat dus wel afstaan aan jullie?

TOM

Zeker.

LIESBETH

Ja. Is het detecteren en het en het vinden van die malware ook nog ingewikkeld, of...?

TOM

Ja, want je weet natuurlijk in principe niet waar op welk systeem dat ding op het moment aan het draaien is. Wat we natuurlijk alleen gezien hebben is, we hebben één van die beacons gedetecteerd.

LIESBETH

En die is aan het communiceren met de actor heen en weer.

TOM

Correct. Ja, zeker. En wat we uiteindelijk gedaan hebben, we zijn gewoon naar Elektron gegaan en daar hebben we een tapje aangesloten op hun interne netwerk. Gewoon gekeken: waar zien we nou die beacons nog meer voorbijkomen? En dan ga je een stapje verder, en dan: zien we het hier nog? Ja? Nee? Nou, oké, en dan: zien we het hier nog? En op een gegeven moment kom je uit bij één computer, en dan zeg je: ja, daar moet het op staan. En dan ga je dus niet de moeite doen om die computer opstarten helemaal te gaan uitpluizen waar die precies zit. Je maakt gewoon een kopie van dat hele systeem, en neemt die hele kopie mee. En op je gemak, ga je die kopie, die ga je analyseren op artefacten.

LIESBETH

Ja, om te kijken wat u doet, waar 'ie heen gaat.

TOM

En waar de malware zit.

LIESBETH

En waar de malware zit. Hoe... Hoe groot is dit? Waar, waar hebben we 't over?

TOM

Ja, dit... Voor mij is dit volledig uniek. Spionage, dat euh... Daar word ik echt niet warm, niet koud van. Dat gebeurt zoveel. Maar echt intentie tot sabotage laten zien, dat heb ik persoonlijk nog nooit eerder meegemaakt.

LIESBETH

En wat... Wat... euh... Wat gebeurt er dan op een afdeling?

TOM

Na mensen worden vooral, en dat is altijd een beetje cru, vooral heel enthousiast. Want als we iets nieuws hebben en iets nieuws gevonden hebben, dat betekent dat we aan de bak mogen. En ja, daar worden wij gewoon heel blij van. Maar daarnaast ook gewoon heel serieuze toon aanhouden. En zeker bij onze analisten. Omdat het nieuw is, En omdat het toch best wel een hoge potentie is tot gewoon gevaarlijke situaties... Ik bedoel stroomuitval in Nederland. De consequenties zijn gigantisch. En daar moet ook heel goed nagedacht worden over: Wie gaan we hierover informeren en hoe gaan we dat doen? Maar ook zo volledig mogelijk.

LIESBETH

Ja.

TOM

En dat is onze taak. Om... Als bewerkers moeten wij zorgen dat we al die informatie gaan zien te vinden.

LIESBETH

Ja, en zit je dan ook al meteen na te denken over: oké, dan gaat het dus nu echt over sabotage? Welke partij hebben daar belang bij? Wie moeten we dan...

TOM

Ow ja, nee, absoluut in je achterhoofd gaat het meteen draaien. Hebben we dit eerder ergens gezien in een andere context? Kennen we partijen die dit soort strategieën toepassen? Waarom doe je het nu? Zover ik weet zijn we niet in een oorlogssituatie verwikkeld. Dus zijn mensen positie aan t opbouwen voor toekomstige scenario's? Wellicht allemaal dat soort dingen. Die hele molen gaat echt nu draaien. Ja. Kijk, gelukkig, het... Een kleine lichtpuntje in deze donderwolk: het is niet zo dat deze systemen van deze energiemaatschappijen dusdanig fragiel zijn dat één hackertje dat hele ding kan omgooien. Er zijn echt heel slimme mensen die over de design van die systemen nagedacht hebben. Er zijn meer lagen beveiligingen ingebouwd. Maar dan nog. Er zal maar een foutje zijn. En zal iemand maar een kabeltje getrokken hebben waar het niet hoort. Ja. En de hackers hebben tijd. Die gaan gewoon rustig hun werk doen.

LIESBETH

Oké, dus we hebben die malware, die zit er in die is gevonden. Daar is gebleken dat die niet alleen op spionage zit, maar ook waarschijnlijk op sabotage.

TOM

Absoluut.

LIESBETH

Omdat 'ie zich richt op bepaalde systemen bij Elektron, die zich bezighouden met uhm... Nou ja... basically dat de machine aan blijft staan.

TOM

Dat is exact wat het is, ja.

LIESBETH

Wat doe je dan nu? Je hebt die hele nacht gehad. Je komt erachter dat de zaak toch toch wel... Nou, wel... Wel serieuzer is dan dat je denkt. Maar ja, die server die leidt sowieso tot een dood spoor, want daar zitten allemaal fake aliasses achter.

TOM

Zeker.

LIESBETH

Wat... Wat... Wat nu?

TOM

Nou ja, we moeten op zoek gaan naar dat ene kleine, leadje wat we hebben. En dat is toch echt pannenkoekenpalazzo.nl. Want hoewel we uit registratie gegevens waarschijnlijk niks interessants gaan vinden... Die website draait wel nog gewoon. En dat geeft ons wel mogelijkheden.

LIESBETH

De vraag is dan natuurlijk welke mogelijkheden? Dat ga ik vragen aan Joey. Hij is jurist bij de Dienst.

JOEY

Ja, we noemen dat de Juridisch Adviseur Operatie en Inlichtingen. Dus eigenlijk ben ik operationeel jurist, dus ik ben... Ik adviseer verschillende teams, waaronder ook het cyberteam.

LIESBETH

Joey is een jonge gast die strak in het pak tegenover me zit, en ik vraag hem hoe hij hier terecht is gekomen.

JOEY

Ik werk hier nu bijna twee jaar. Heb natuurlijk rechten gestudeerd. En nu is het niet standaard dat bijvoorbeeld in een rechtenstudie de WIV, de Wet op de Inlichtingen en Veiligheidsdiensten centraal staat. Dat zie je niet vaak terug. Nu heb ik daar toevallig zelf wel voor gekozen. Richting mensenrechten, nationale veiligheid... En ik dacht tijdens m'n master van: goh, hoe werkt dat eigenlijk in Nederland? Hoe voeren zij hun bevoegdheden uit om Nederland veilig te houden?

LIESBETH

Net als zijn collega's bazuint Joey niet overal rond waar hij werkt. Maar, zo ontdekte hij, het kan ook best handig zijn als er mensen zijn die wel weten dat hij hier elke dag naartoe gaat.

JOEY

De gouden tip die ik heb gekregen is er ook wel van: goh, zorg er wel voor dat ook mensen je kunnen helpen. En dus, dus mijn ouders weten het natuurlijk. Maar er zijn ook een klein... Een klein groepje vrienden weet het ook. Op het moment dat ik een vraag krijg van: 'goh, waarom neem jij doordeweeks je telefoon niet op? Of wat doe jij voor werk, of eh... Of ben jij... Zit je bij Binnenlandse Zaken? Oh wat leuk. Ik werk bij Justitie en Veiligheid ernaast, kunnen we misschien lunchen dan?' Dan zijn zij ook degene die me bijvoorbeeld er uit kunnen redden of van onderwerp kunnen veranderen. Als me zelf dat niet lukt.

JOEY

Wat er in de buitenwereld gebeurt bepaalt eigenlijk ook hoe mijn dag eruit ziet. Dus heel vaak heb ik een hele mooie planning gemaakt, maar die kan als ik binnenkom al het raam uit, omdat er iets aan de hand is of je moet ergens adviezen geven. Je moet het wel zo zien: mijn rol is eigenlijk dat ik... Ik zit zeg maar in de lijn. Dus een team besluit een aanvraag te schrijven, om een bevoegdheid aan te vragen. Ja en dan gaat 'ie natuurlijk naar een teamhoofd, naar een unit hoofd. Uiteindelijk komt 'ie dan bij de afdeling juridische zaken, nou dan komt 'ie bij mij terecht. Dan toets je natuurlijk of een aanvraag, of de inzet van die bevoegdheid noodzakelijk is in een democratische samenleving. En dan heb je natuurlijk ook nog de eisen van proportionaliteit subsidiariteit. Dus... Dus is dit... Is wat we nu gaan inzetten, de inbreuken die we gaan maken, staat dat in verhouding tot de dreiging die er is?

LIESBETH

Zoals bij alle middelen die de dienst in kan zetten, gaat daar dus eerst een uitgebreide juridische afweging aan vooraf. Wie denkt dat je als techneut hier lekker de hele dag iedereen kan zitten hacken, dat valt dus tegen. Of mee. Het is maar hoe je het bekijkt.

JOEY

Wat je in praktijk ziet is dat wij al vaak aan de voorkant er al bij zitten. We zien wat, we schrijven een aanvraag. Maar om dat... We moeten de dynamische wereld wel zo goed mogelijk proberen te vangen op papier, en dat is natuurlijk lastig. En dan zie je ook vaak dat het wel een samenspel is tussen een bewerker en een jurist. Misschien af en toe ook wel een hacker die daarbij betrokken is. En en dan kan het af en toe wel zo zijn dat zegt van... ja. Op deze manier kan je niet deze aanvraag schrijven. Op deze manier kan je niet de bevoegdheid inzetten zoals je nu voor ogen hebt.

LIESBETH

Vlak voordat je hier binnen kwam begreep ik dat er even een spoedje was. Wat voor spoedjes zijn er, dienen zich aan voor een jurist?

JOEY

Nou, op het moment dat er een een digitale aanval bezig is, of dat wij die zien, of dat er inderdaad iets voorkomt waar nu op geacteerd moet worden... Dan gaan we niet een week wachten. Maar dat betekent wel dat... Eigenlijk gaat het bij iedereen die toestemming moet geven, die in de lijn zit als het ware, dat gaat dan versneld. En dat gaat dan telefonisch. En dat kan in het weekend zijn. En het spoedje wat we vanochtend hadden was niet zozeer dat het spoed was, dat er ook iets aan de hand was. Maar het betekent wel dat er inderdaad uh... We zijn ergens met een operatie bezig, en dan wil het wel eens zo zijn dat er dan juridische vragen op komen. Dat de praktijk toch iets anders is dan we misschien voor ogen hadden. Je schrijft een aanvraag op het moment dat inderdaad de eerste informatie tot je komt. Maar als je eenmaal bezig bent, dan kan dat ook zomaar zijn dat er nieuwe vragen op komen. En hoe verhoudt zich dit tot, ja inderdaad tot de juridische eisen? Wat we... Ja, je komt soms inderdaad op andere andere feiten terecht.

LIESBETH

Ja, je zit natuurlijk op een cyber zaak. Ik kan me voorstellen dat daar best vaak een spanning op zit. Dat er... Dat er dingen mogelijk, technisch mogelijk zijn, die misschien juridisch nog niet helemaal doordacht zijn? Als in... Is dat zo?

JOEY

Nee, ja, dat is zeker zo. Je ziet inderdaad dat de wet de technologie volgt. Op het moment dat er iets nieuws is, is er natuurlijk niet een wet die daar... Het kan niet zo zijn dat er al een wet is en dan pas de technologische ontwikkeling komt. De wet volgt altijd de technologische ontwikkelingen.

LIESBETH

Maar hoe ga je daar mee om? Want dat betekent dus ook dat dat er mannen en vrouwen hier rondlopen die denken: oh, dit is een geweldig idee om het zo en zo op te lossen, maar dat er dan nog niet een wet voor ligt waar jij meteen mee uit de voeten kan.

JOEY

Ja. Nou ja, wat de wetgever hier wel voor ogen heeft gehad met de WIV, is dat die technologie onafhankelijk geschreven is. Dus dat betekent dat de wet, in hoever het kan, dat hij niet is vastgeknoopt aan een bepaalde naam van de technologie op dat moment.

LIESBETH

Dit is ook de reden dat veel van de termen zo omslachtig zijn. Hacken bijvoorbeeld noemen ze 'binnendringen in geautomatiseerde werken'. Maar goed. Terug naar de case, want ik wil weten of onze zaak inmiddels ook een spoed telefoontje zou kunnen opleveren.

JOEY

Dat zou wel kunnen.

LIESBETH

Ja ja. Het is dus duidelijk geworden dat die malware zich niet alleen op spionage richt, maar waarschijnlijk ook zich richt op sabotage. Dan, dan wordt het... Dan is het een serieus verhaal.

JOEY

Ja ja, in beide gevallen natuurlijk. En het is natuurlijk nogal een stapje erger. Statelijke actoren, of inderdaad waar digitale aanvallen vandaan komen... Dat gebeurt steeds vaker. En dat betekent ook dat als wij inderdaad een belletje krijgen, kan op verschillende manieren. Kan zijn dat de informatie tot ons komt van een andere partij die zegt: goh, er gebeurt iets op dat ip-adres. Kan zijn dat inderdaad er vitale investituur Nederland wordt aangevallen en dat wij met hun in contact staan. Kan zijn dat wij zelf iets zien op dat moment. Er gaat dan wel meestal een spoedprocedure in. Want we gaan natuurlijk niet een week wachten. We gaan niet cyber dreigingen en cyberaanvallen een week laten voortduren voordat wij toestemming hebben. Nee, dan hebben wij een concrete dreiging waarin het echt noodzakelijk is in onze democratische samenleving om daarop te acteren. En dat is hier dus ook het geval. En dan zou... Als dit op zaterdag gebeurt, dan zou het inderdaad zo maar kunnen zijn tot dat ik dan ook gebeld word omdat ik ook een van de personen ben die de toets uitvoert. Die de juridische toets uitvoert voordat iets naar de minister gaat of onze Directeur Generaal of na een tip, inderdaad.

LIESBETH

Wat zijn mijn opties in deze cyber zaak?

JOEY

We hebben artikel 45. Dat is onze hack bevoegdheid, 'Binnendringen in Geautomatiseerde Werken'. Je hebt artikel 54. Dat is het het opvragen van een kopie van een server. Dat als iemand bijvoorbeeld een server huurt bij een hosting partij en vanuit die server een aanval initieert, of in in een keten van verschillende servers zit die ofwel ons aanvallen of onze bondgenoten, dan zouden we daar een kopie van kunnen ophalen. Je hebt natuurlijk artikel 47 waarin je in een CT casus een microfoon kan plaatsen of z'n telefoon kan afluisteren. Al heeft dat hier niet zoveel zin. Maar wat we wel kunnen doen is en een gerichte tap aansluiten op een server om te kijken wat voor stroom aan data er heen en weer gaat.

LIESBETH

Een hoop verschillende wetsartikelen en een hoop opties die we moeten gaan afwegen. Ik vraag gooi wat hij van de zaak vindt.

JOEY

Dit is wel zorgelijk. Dit is ook wat je ook wel steeds vaker ook vanuit de AIVD naar voren zitten komen, is dat dreigingen uit deze sectoren echt wel wezenlijk is. Wij zouden volgens de artikel 73 zouden wij een maatregel mogen treffen om bijvoorbeeld de server waar de aanval vandaan komt te verstoren of uit te schakelen. Da's wel heel wat.

LIESBETH

Ja?

JOEY

Ja. Alleen dat is natuurlijk best wel makkelijk gezegd. In praktijk... Het is niet zo dat wij hier een knop hebben waar je een IP-adres kan invoeren en op verstoring kan drukken. Nee, dat zou heel makkelijk zijn natuurlijk. Maar dat, dat is het niet. Dus je hebt een en heel moeilijk situatie waarin je altijd voor jezelf moet afvragen van goh... Op het moment dat wij deze server kunnen uitschakelen is het natuurlijk maar de vraag of het ook echt gaat lukken. Maar is het ook wenselijk? Want als vanuit meerdere servers een aanval plaats kan vinden op onze vitale infrastructuur, en we schakelen er één uit omdat wij denken dat dat degene is wat vandaan komt... Dan ben je misschien en je zicht kwijt, en de aanval gaat door. En ze weten in ieder geval dat wij ervan weten. Het advies zou dan wel zijn om in deze wel, euh... Want wij zijn natuurlijk begonnen met informatie van Elektron zelf. Nou, op dat moment moet je heel duidelijk voor je hebben: wat is jouw doel van je onderzoek nu?

LIESBETH

Nou ja, in ieder geval zorgen dat die systemen niet uitvallen. Lijkt me. Dus die malware die is dus nu geanalyseerd, dat die dus op sabotage gericht is. Dat moet je voorkomen... En toch zo snel mogelijk weten waar dit vandaan komt.

JOEY

Ja, ja. Ja, dus daarom zou je altijd een beginnen met het aanvragen van een artikel 54 om te weten wat er op de server gebeurt, als je tenminste hebt gezien het vandaan komt. Nou ja, we hebben informatie gekregen van Elektron dus we weten waar dit allemaal vandaan komt. En dan kan je een kopie van die server, kan je ophalen. Het aanzetten van een tap is ook altijd wel aangeraden, ook. Om te weten: wat komt er nou vandaan? En zien we bijvoorbeeld een andere infrastructuur die met deze server communiceert?

LIESBETH

De volgende zet om dichter bij de aanvallers te komen is dus bijvoorbeeld een kopie te maken van de server om te zien wat daarop gebeurt. Maar we zouden ook die server kunnen gaan tappen.

JOEY

Dit lijkt me ook wel handig om met het NBV nog even contact contact te zoeken. Want zij zijn hier wel degene die de contacten onderhouden met onder andere de vitale infrastructuur in Nederland. Dus de contacten daar, die is daar ruimschoots aanwezig.

LIESBETH

Vitale infrastructuur zoals bedrijven zoals Elektron.

JOEY

Ja zeker. Ja ja.

JOEY

RUSTIGE MUZIEK

LIESBETH

Ik ga dus praten met iemand van het NBV. Dat staat voor Nationaal Bureau voor Verbindingsbeveiliging. Dit is een onderdeel van de AIVD waar advies wordt gegeven over de bescherming van gegevens bij de overheid. Daarnaast beoordelen ze ook de producten die worden gebruikt voor de uitwisseling van staatsgeheimen die, zoals je kunt begrijpen aan de hoogstestandaarden moeten voldoen. Zij hebben bijvoorbeeld de Tiger telefoon ontwikkeld, een telefoon waarmee bewindspersonen veilig staatsgeheimen kunnen bespreken. Rutte heeft er ook eentje in de lade. Het NBV is trouwens ook bekend, of ik moet zeggen berucht, vanwege de openbare en enorm populaire AIVD kerst puzzel die ze ieder jaar publiceren. Ik weet niet of je die wel eens heb geprobeerd te maken, maar zelf struikelt ik al bij de eerste opgaven. Maar goed, op naar 't NBV.

LIESBETH

Ehm, welke naam gebruik ik voor jou?

ELLEN

Ellen.

LIESBETH

Ellen. Ellen dus. Ze legt uit wat haar baan inhoudt.

ELLEN

Ik ben adviseur, dus ik adviseer overheid maar ook vitale sectoren en topsectoren over hoe ze om kunnen gaan met statelijke dreiging. En nou ja, dus bijvoorbeeld dit soort aanvallen. Sectoren waar Nederland niet zonder kan. Vroeger waren het... Was het vooral het beveiligen van onze internetverbindingen door middel van cryptografie. Dus dat is het versleutelen van je netwerkverkeer zodat niet iedereen mee kan lezen. Inmiddels zijn we eigenlijk één van de onderdelen van de Dienst die zich bezighoudt met de C-taak, zoals wij dat noemen. Dus eigenlijk de weerbaarheidsverhoging. En wij bij het NBV doen dat voornamelijk op het gebied van cyber. Maar je ziet dat we dat toch wel steeds vaker met onze collega's die wat veel meer op de fysieke beveiliging zitten, samenwerken, omdat cyber en fysiek ook steeds minder gescheiden is.

LIESBETH

Op welke manier?

ELLEN

Nou bijvoorbeeld de casus. Uhm. Elektron is een energieleverancier, een bedrijf in de energiesector. Als die door een cyberaanval platgelegd wordt, dan heeft dat implicaties voor misschien wel de stoplichten. En als stoplichten uitgaan dan krijg je ongelukken en dan krijg je files. Mensen kunnen niet meer naar huis komen. Mensen kunnen niet meer naar de supermarkt, hun kinderen niet meer ophalen. Dus dat heeft... Zeg maar cyber en fysiek is al lang niet meer zo gescheiden als dat van oudsher was. Over het algemeen ben ik bezig met mijn klanten, dus wij krijgen vragen vanuit deverschillende sectoren of vanuit het rijk over hele specifieke technische vragen. Bijvoorbeeld over hoe je veilig kan telefoneren of videobellen. Dus ik ben bezig met ofwel het voorbereiden van dat soort sessies, ofwel bezig met juist het schrijven van een advies voor mijn klanten.

LIESBETH

En Elektron bijvoorbeeld, zo'n klant. Benaderen jullie dan hun of zij jullie? Of hoe komt zoiets tot stand?

ELLEN

Beiden. Wij hebben... Wij, maar de Dienst an sich heeft een groot aantal account managers die eigenlijk zoveel mogelijk hun tentakels uitspreiden door de hele samenleving. Dan heb je het over het bedrijfsleven lokaal. Je hebt het over het Rijk, je hebt over grote bedrijven, vitale sectoren. En dus daar hebben over het algemeen al goede contacten mee. En op het moment dat wij een dreiging zien, en dat zit natuurlijk vooral aan de inlichtingen kant, dan gaan we daarheen. Bijvoorbeeld een incident zoals deze casus. Dan nemen wij natuurlijk zelf contact op. En dan helpt het dat je al een contact heb gehad of we eens een keer een adviesopdracht hebben gedaan. Maar het kan ook zeker zijn dat bedrijven ons benaderen, van 'hé, de dreiging neemt toe, dat voelen wij. Hoe gaan we daarmee om?' Want een ransomeware aanval crimineel is echt heel anders dan spionage of sabotage.

LIESBETH

Ja en zo'n Elektron, hoe reageren die als je belt met dergelijk nieuws?

ELLEN

Verschillend. Euhm... Wij hebben mensen die reageren met 'oké, maar is dat een probleem?' Ja, dan moet je toch een hele andere manier het gesprek aan gaan dan wanneer ik bijvoorbeeld al een advies opdracht heb gedaan en een klant bel en zeg 'Hé euh, hoe is het met je, ga er even bij zitten, ik heb nieuws.' En wat helpt is dan natuurlijk als wij advies opdracht daar hebben gedaan... Maar het is natuurlijk niet alle credits naar ons... Uhm, als ze al wat volwassener zijn in de Cyber Security, want dan kunnen ze ook daadwerkelijk stappen ondernemen om te reageren op zo'n boodschap.

LIESBETH

Ja, en het feit dat wij dus nu op deze manier met Elektron kunnen samenwerken, dat komt door de afdeling waar jij op zit.

ELLEN

Onder andere. Kijk, ik ben adviseur op het gebied van statelijke actoren. Dat betekent natuurlijk niet dat ik opeens... Dat door mij zij hun security op orde hebben. Maar het helpt wel dat wij vanuit eenblik van de aanvaller en vanuit statelijke actoren met deze klant gesproken hebben. Een voorbeeld hiervan is misschien wel... Kijk, ze zijn gehackt. Dan kan je als reactie geven 'oh, wat slecht wie wordt er nu... Je moet gewoon niet gehackt worden'. Maar je hebt het over een statelijke actor. En we hebben het dan over iemand met oneindige middelen, wat ook een beetje abstract is. Maar dat betekent gewoon al moeten ze er drie of vier jaar over doen, als ze je willen hacken dan lukt dat. Dus wij zeggen altijd tegen onze klanten: ga ervan uit dat je gehackt wordt op een tijd, op een moment tijd en neemt dan de juiste maatregelen zodat je de juiste detectie ook hebt en de juiste logging hebt, zodat je kan onderzoeken welke systemen allemaal gehackt zijn.

LIESBETH

Het verhaal van Ellen doet me denken aan wat ik eerder met Tom besprak. Dat computers niet zomaar zelf dingen verzinnen, maar dat er iemand achter zit. Ook in Ellens werk gaat cyber voortdurend gepaard met ouderwets mensenwerk.

ELLEN

Het is begrijpen wat mensen willen. Begrijpen wat er beschermd moet worden. En uhm, dus je moet, ja... technische kennis hebben. Maar je hoeft geen techneut te zijn. Je moet het vooral heel leuk vinden om je te verdiepen in de techniek en in de mensen.

ELLEN

Kijk sabotage zoals deze casus. Mensen begrijpen dat. Dat is, dat is groot. Mensen begrijpen wat er gebeurt op het moment dat het licht uitgaat. Terwijl we in Nederland heel vaak te maken hebben juist met spionage. Dus dat er wordt meegekeken in de systemen van bedrijven of organisaties. En niet iedereen begrijpt dat dat een probleem is. Bijvoorbeeld kennisinstellingen. Die zijn van nature heel open. Dus waarom is het eigenlijk een probleem? Want we gaan het toch publiceren? Dus dat. En die mensen vinden het vooral heel lastig om te beseffen dat ook zij mogelijk een target zijn. Dat wat zij doen voor andere landen dusdanig interessant is dat iemand over de schouder mee wil kijken. En dat is, uhm... En soms lukt dat om dat mensen te vertellen, en soms lukt dat niet. Maar goed, ik ben en blijf een adviseur. Dus op een gegeven moment moet ik ook accepteren als mensen het niet willen zien of het zich slecht kunnen voorstellen.

LIESBETH

Hoe langer ik hier zit en hoe langer ik nu op deze cyber afdeling loop. Soms denk ik: het was toch ook eigenlijk wel een overzichtelijke, makkelijke tijd toen het allemaal nog aan het papier stond.

ELLEN

Klopt. En als je echt wil dat jouw geheimen over dertig jaar nog steeds helemaal veilig zijn, dan moet je ze uitprinten en in een kluis leggen. En alle andere geheimen... Ja, daar kan je digitaal gewoon mee aan de slag.

LIESBETH

Ja. Ja, dat is toch wel... Dat is... Dat vind ik toch een rare realisatie dat het allemaal veiliger en veiliger wordt, maar tegelijkertijd ook dus... In principe zit altijd ergens een klein gaatje in.

ELLEN

Klopt, en dat is natuurlijk ook waar we het net over hadden. Dat is dat principe binnen ons risicomanagement waarin we zeggen: ga er van uit dat je gehackt wordt. En neem daar je maatregelen op. Zorg dat je je beveiligingsmaatregelen zo ingericht zijn dat je daar mee om kan gaan. En een voorbeeld daarvan is bijvoorbeeld, als jij inlogt op je e-mail of je computer en je hebt vijf keer je wachtwoord verkeerd ingetikt, dan wordt je account geblokkeerd. Dus wat er op dat moment gelogd wordt is het aantal keer dat je foutieve inlog pogingen hebt gedaan. En dat is top vanuit het beveiligingsperspectief, maar vanuit het perspectief van een aanvaller... Die heeft misschien wel via een datalek jouw gegevens van het internet geplukt, dus die logt in één keer heel soepel in. Dus je moet niet alleen loggen wat je foutief inlogt, maar je moet ook zorgen dat je opslaat vanuit welke plekken daar goed is ingelogd. Want als iemand jouw gegevens heeft, dan kan 'ie gewoon inloggen en doorstappen. En dat is het. Ga er van uit dat je gehackt wordt en zorg dat je daar je maatregelen toe neemt. En dat is denk ik een van de allerleukste dingen van mijn baan, is dat ik dat perspectief mee mag nemen bij klanten. Dus het is niet alleen denk vanuit een verdedigingsperspectief, maar ga in de stoel zitten van een aanvaller. Wat eh, wat wil je eigenlijk bereiken? Wat wil je hebben? Op welke plek wil je zitten? Welke informatie wil je vinden en hoe wil je daar komen?

LIESBETH

Ik vraag Ellen wat belangrijk is om in mijn achterhoofd te houden als ik verder ga met deze zaak.

ELLEN

Verplaats je in een ander. Zorg dat je het belang van de mensen om je heen goed duidelijk hebt, maar ga vooral op de stoel van de aanvaller zitten. Wat wil de aanvaller? Waar is de aanvaller mee bezig en hoe gaan ze daar komen? Dat gaat je helpen om de juiste stappen, de juiste vraag te stellen.

LIESBETH

Ga er van uit dat je gehackt wordt en print al je grootste geheimen uit. Mijn vader heeft een opschrijfboekje waarin hij al zijn wachtwoorden in een zelfbedachte codetaal heeft opgeschreven, en deed ik daar altijd een beetje lacherig over. Eigenlijk heeft hij dus gewoon een hartstikke veilig systeem voor zichzelf. Nadat ik met Ellen heb gepraat, loop ik snel terug naar Tom om te bepalen welke stappen de zaak nodig heeft.

TOM

Heb je een doel in je hoofd waar je naartoe zou willen werken? Wat je nu graag zou willen weten?

LIESBETH

Euhm ja, ik... Ik wil gewoon heel graag weten wie het doet, maar ik geloof dat dat niet... Dat dat helemaal niet is... Het pad waar ik op zou moeten.

TOM

Euh ik... Die vraag is is nu nog gewoon niet te beantwoorden.

LIESBETH

Nee, precies.

TOM

Het is wel een pad waar we echt in een lange termijn echt wel heen willen en gaan werken. Maar ik denk dat handig is als we nu gewoon beginnen met het enige lijntje, het enige draadje wat we hebben en daar maar eens aan gaan trekken en kijken wat er uitkomt.

LIESBETH

Ja, ja, en je wil natuurlijk weten of dit euh, of dit het enige is wat ze aan doen zijn.

TOM

Absoluut.

LIESBETH

Binnen Elektron.

TOM

Zeker binnen Elektron, en ook op dat euh pannenkoekenpalazzo, die C2 server die we hebben gevonden. Dat is eigenlijk het feitelijke draadje dat we nu hebben. Ja, of daar nog meer mee communiceert? Want we zien alles vanuit het perspectief van Elektron BV nu. Maar we hebben nog niet eens kunnen vaststellen of Elektron BV het enige slachtoffer is, of dat er nog veel meer slachtoffers zijn, wellicht.

LIESBETH

Dat zou... Die optie licht er ook nog?

TOM

Zeker. Ja, die is absoluut niet uitgesloten.

LIESBETH

Ja. Dus je moet... Ja, wat moet je nou eigenlijk? Wat, wat... Wat is dan de stap? Hoe ga je er achter komen?

TOM

We gaan tappen. Ik zou willen voorstellen om de website pannekoekenpalazzo.nl Artikel 47 te schrijven, en daar al het verkeer van te gaan tappen om te kijken: wie communiceren er met die server? We weten dat de implant bij Elektron BV moet communiceren? Nou, logischerwijs moet de actor ook op een of andere manier met die server communiceren. En dat geeft ons wellicht weer een stapje verder om, zeg maar die keten waar je zo graag heen wil, 'wie doet het', om die te gaan bewandelen. En we kunnen kijken of we al andere slachtoffers zien.

LIESBETH

Dus dat is wat er gaat gebeuren. We gaan tappen. Niet een telefoon zoals vorig jaar, maar een server, zodat we te weten kunnen komen welke informatie waarheen gaat. In kaart kunnen brengen of er nog meer slachtoffers zijn en hopelijk weer een stapje dichter bij de dader komen.

TOM

En als je nou zelf de uitdaging aan wil gaan en dus laten zien hoe goed je bent in het kaf van het koren te scheiden, dan is alle data te vinden op OperatiePositron.nl. Veel succes.

LIESBETH

Dit was de derde aflevering 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.