GEERT
BAUDEWIJNS

ONDER HANDELEN IN HET DUISTER

Lannoo

INHOUD

01

DE ZAAK ANTWERPEN

‘De stad Antwerpen is gehackt.’

Op mijn visitekaartje staat iets anders, maar als mensen me vragen wat ik doe, zeg ik meestal: 'Onderhandelen met cybercriminelen.' Dat is het meest tastbare aspect van mijn werk in cybersecurity: communiceren met hackers die via ransomware het netwerk van een bedrijf lamleggen. Die hackers vinden steeds nieuwe manieren om netwerken te infiltreren, schadelijke software te installeren, alle data onleesbaar te maken en die te kopieren. Vervolgens vragen ze losgeld om de data weer toegankelijk te maken en niet te publiceren. Pure chantage dus.

De getroffen bedrijven staan met hun rug tegen de muur. Niks werkt nog, waardoor ze hun mensen huiswaarts moeten sturen, de productie en hun dienstverlening stilliggen en hun IT-personeel overuren klopt. Vaak volgt al snel de conclusie dat losgeld betalen de snelste, goedkoopste of zelfs enige oplossing is. Op dat moment roepen ze mijn hulp in. Als onderhandelaar is het niet mijn taak om cybercriminelen op te sporen, maar om met hen te praten, soms dagen- of wekenlang. Mijn doel is om hun prijs te verlagen en te achterhalen hoe ze zijn binnengekomen. Natuurlijk voelt het wrang om in te gaan op de eisen van gewetenloze hackers, maar ik doe er alles aan om het losgeld zo laag mogelijk te krijgen, zodat de meeste bedrijven een aanval heelhuids doorstaan.

De bekendste hacking in Vlaanderen is wellicht die van de stad Antwerpen eind 2022. Wanneer ik toevallig met iemand aan de praat raak en over mijn werk begin, volgt bijna steevast de vraag: 'Hoe zat dat eigenlijk in Antwerpen?' De cyberaanval op de stad, nota bene op sinterklaasnacht, blijft mensen fascineren en is in het collectieve geheugen gegrift. Het verhaal heeft dan ook flink wat ingrediënten die de verbeelding prikkelen: een iconische datum, een belangrijke stad en een vreemde ontknoping waarover geruchten de ronde blijven doen.

Voor mij heeft deze vraag een dubbele lading, want eerlijk gezegd doet 'de zaak Antwerpen' me nog steeds iets. Op het moment van de hacking waren we als leverancier nauw betrokken bij Digipolis, de IT-partner van de stad die verantwoordelijk is voor een breed scala aan diensten, van het onderhouden van het stadsnetwerk tot de digitale ontwikkeling van de stadsdiensten. Ook cybersecurity valt onder hun bevoegdheid, iets wat Antwerpen sinds de hacking van Luik bijzonder serieus nam.

Luik werd in juni 2021 getroffen door een ransomware-aanval door de groep Ryuk. Voor het eerst lag een Belgische grootstad helemaal plat. De stad betaalde volgens mediaberichten 30 miljoen aan losgeld, wat in Antwerpen een alarmbel deed afgaan. Cybersecurity stond er plots hoog op de agenda en het stadsbestuur maakte extra middelen vrij om een scenario als in Luik te vermijden. Met die gedachte in het achterhoofd gaven ze Digipolis, hun technologiepartner, de taak om een grondig cybersecurityplan te ontwikkelen. Het doel was duidelijk: de digitale verdediging van de stad versterken en haar systemen ondoordringbaar maken voor cyberdreigingen. Digipolis schreef een aantal opdrachten uit, waarvan onze firma er een paar binnenhaalde. Heel concreet was het onze taak om te zoeken naar mogelijke kwetsbaarheden in het netwerk en die te signaleren. Het operationele lag niet bij ons, wij moesten enkel aangeven langs waar aanvallers zouden kunnen binnenraken.

Op het moment van de hacking waren we als leverancier nauw betrokken bij Digipolis, de IT-partner van de stad.

Er waren toen heel wat kwetsbaarheden, dat is niet abnormaal en zien we bij heel veel bedrijven. Je moet er rekening mee houden dat het netwerk van Antwerpen, net als bij veel andere

grote steden, steunt op een infrastructuur die wel 20 tot 30 jaar oud is. Bij veel van onze klanten zien we hetzelfde probleem. Ze beginnen met een klein netwerk dat heel snel moet groeien zonder dat de werking van bestaande applicaties of diensten mag worden onderbroken. Door de digitale omslag van stadsdiensten bijvoorbeeld, groeide het Antwerpse netwerk in de laatste 15 jaar zienderogen. De focus lag op bouwen, bouwen, bouwen, en de snelheid waarmee dat moest gebeuren, liet eigenlijk niet toe om stil te staan bij de vraag: zijn onze fundamenten eigenlijk wel goed en correct beveiligd? Zijn die wel sterk genoeg om daarop te blijven uitbreiden? Zijn die toekomstbestendig genoeg als het bijvoorbeeld gaat over netwerkbeveiliging?

Het moderniseren van zo'n oud systeem is verre van eenvoudig en wordt door IT-mensen vaak gezien als de moeilijkste opdracht omdat je een weg moet zoeken om oude en nieuwe technologieën aan elkaar te koppelen. Dat vereist niet alleen significante tijds- en financiële investeringen, maar ook uitgebreide technische expertise. Een van de meest effectieve methoden om de beveiliging te versterken, is het toepassen van 'Chinese walls', wat ook weleens 'subnetting' wordt genoemd.

Subnetting is het proces waarbij je een groter netwerk opdeelt in kleinere, beheersbare segmenten of subnetten. Elk van deze subnetten kan dan functioneren als een onafhankelijk netwerk, met zijn eigen unieke beveiligingsprotocollen en toegangsbeheer. Door het netwerk van de stad op deze manier te segmenteren, wordt elke sectie afgeschermd van de andere, waardoor de reikwijdte van mogelijke cyberaanvallen wordt beperkt en gevoelige informatie beschermd blijft.

Het invoeren van Chinese walls in een bestaand netwerk is een gigantisch en heel complex werk. Je moet nieuwe protocollen implementeren, medewerkers opleiden om met de nieuwe structuur te werken en verouderde systemen vervangen. Je kunt daarvoor

niet even alle stadsdiensten platleggen, alle aanpassingen moeten gebeuren zonder de dagelijkse werking van de stad te verstoren. Naast technische vaardigheden komt er dus ook ontzettend veel coördinatie bij kijken. Bovendien, en daar moeten we niet flauw over doen, kost een dergelijke aanpassing geld. Véél geld.

Een bijkomend probleem bij oude netwerken is dat je bepaalde software niet zomaar kunt upgraden omdat de onderliggende technologie te oud is. Als je zo een oud systeem optimaal wilt beveiligen, heb je immers de steun van de leverancier nodig. Vaak stopt die echter vijf jaar na het ontwikkelen van de software met het ondersteunen van de oude technologieën. Daardoor kun je vanaf dat ogenblik geen veiligheidsupdates meer installeren. De klok blijft vanaf dan stilstaan voor die oude applicaties, maar de klok van hackers begint dan te lopen. Hackers zoeken naar kwetsbaarheden die ze kunnen uitbuiten, wetend dat de leveranciers zelf niets meer gaan doen om deze te verhelpen. Het is met andere woorden een kwestie van tijd voordat er iets gebeurt. Als stad sta je met de rug tegen de muur omdat je oude applicaties moeten blijven werken, ondersteund door de leveranciers of niet.

Op een bepaald moment vroeg ik daarom een gesprek aan met de CEO van Digipolis. Ik wilde hem persoonlijk op de hoogte brengen van de ernst van de problemen en hem overtuigen om actie te ondernemen. Het gesprek verliep best gemoedelijk. Ik legde hem stuk voor stuk uit waar de zwakheden zaten en de CEO knikte vaker dan ik had verwacht. Hij beaamde dat er iets moest gebeuren, maar tegelijkertijd voelde ik maar al te goed dat ze bij Digipolis de urgentie van de situatie niet helemaal inzagen.

Ik zal er geen doekjes om winden, dat frustreerde me. Terwijl ik in het buitenland erkenning krijg als expert, word ik in eigen land vaak gezien als de zoveelste adviseur. Alleen zit ik dagelijks midden in de actie, ken ik als geen ander de informatie en de tools die op

het dark net te vinden zijn en kan ik met mijn team zwart op wit aantonen waar de gaten in een beveiligingssysteem zitten. Vaak slagen wij erin om een aanval te ontdekken voordat hij al effectief heeft plaatsgevonden omdat de eerste tekenen steeds te vinden zijn op het dark net. Dat maakt ons anders dan andere beveiligingsfirma's. Ik kan veel dingen niet, maar dit kan ik wel: aanvoelen wanneer het fout gaat lopen en tonen waar het fout kan lopen, enkel en alleen met informatie die we terugvinden op het dark net.

Op een bepaald moment zag ik zoveel alarmbellen afgaan dat ik het heft in eigen handen nam. Begin november stuurde ik Bart De Wever, burgemeester van de stad Antwerpen en partijvoorzitter van de N-VA, een bericht. Die stap was niet zo groot, al had ik hem tot dan nog nooit persoonlijk ontmoet. Ons bedrijf heeft een nauwe samenwerking met N-VA nationaal en in mijn eigen gemeente kwam ik destijds op voor dezelfde partij. Ik stuurde hem heel eenvoudig het volgende bericht: 'Ik zou graag eens met u willen samenzitten.' Zijn antwoord kwam vrij snel: 'Goed, plan maar iets in via mijn secretaresse.' We prikten een datum, 28 november, en hij en zijn kabinetschef maakten een uur voor me vrij.

Die dag wandelde ik door de imposante deuren van het Antwerpse stadhuis, een plek die ik tot dan toe alleen van buitenaf kende. Na registratie en aanmelding aan het onthaal liep ik de statige trappen op, langs prachtige schilderijen, tot aan de kantoren van de burgemeester. Zijn kabinetschef en hijzelf ontvingen me hartelijk, al verspilden we weinig tijd aan beleefde smalltalk; ik was daar met een missie. Wat oorspronkelijk een uur zou duren, liep uit tot een intens gesprek van twee uur. Ik deelde mijn bezorgdheid over hoe hackers te werk gaan, wees op de zwakke plekken, en drukte mijn frustratie uit over bepaalde zaken die maar niet veranderden.

Amper een week later, terwijl ik in Japan was voor een economische missie, kreeg ik een bericht van het hoofd van ons technisch departement: 'De stad Antwerpen is gehackt.' Het was 6 december, ik zal het nooit vergeten.

Ik klapte meteen mijn computer open, het dark net op. En inderdaad, Play, een van de grote hackerscollectieven, claimde de aanval op de stad. Op haar 'wall of shame' – wat je kunt zien als een digitaal annonceblad met alle 'lopende zaken' – stond *the city of Antwerp* helemaal bovenaan, inclusief een aftelklok naar de deadline die de hackers hadden bepaald. Alle grote ransomware-collectieven hebben zo'n wall of shame. Zodra het losgeld is betaald, halen ze het slachtoffer van hun muur. Dat was hier nog niet aan de orde: onder de naam Antwerpen tikte de klok genadeloos verder.

Ik geef toe dat ik behoorlijk verrast was door de snelheid waarmee mijn woorden werkelijkheid waren geworden. Nog geen week ervoor had ik zitten zeggen dat er een aanval kon komen en nu was het al zover. Zonder aarzeling stuurde ik een bericht naar Bart De Wever: 'De stad Antwerpen is gehackt. Bent u al op de hoogte?' Dat lijkt misschien een vreemd bericht om te versturen, maar het is niet ongewoon dat de hoogste leidinggevenden vrij laat op de hoogte worden gebracht van een cyberaanval. Vaak zie je bijvoorbeeld dat IT-diensten de storing eerst intern willen oplossen, of terugkoppelen naar hun directe leidinggevende voordat de CEO of in dit geval de burgemeester ingelicht wordt. Bart zond meteen een bericht dat hij zeer zeker wist wat er gaande was. Hij vroeg mij om voorlopig niets te ondernemen en schreef al grappend: 'Je bent nu wel verdachte nummer één, door me een week op voorhand precies te voorspellen wat er vandaag is gebeurd.' Ik kon het niet helpen en antwoordde lachend: 'Elk verhaal heeft een verdachte nodig en ik speel die rol met plezier.'

Al viel er in dit verhaal weinig te lachen. Heel veel diensten konden hun werk niet meer doen en lagen stil: geen paspoorten, geen bouwvergunningen, containerparken gesloten – alles wat gedigitaliseerd was, moest manueel verder.

Bovendien hadden de hackers 557 gigabyte data buitgemaakt, die ze dreigden te publiceren. Over wélke data het precies ging, was niet geweten. De vrees was dat persoonlijke gegevens van burgers waren gekopieerd, iets wat de burgemeester een paar weken na de hacking zou ontkennen.

In een mum van tijd roken journalisten onraad en publiceerden ze artikel na artikel over de grootschalige aanval op het Antwerpse net. Te midden daarvan een burgemeester die bij zijn standpunt bleef: 'We onderhandelen niet, we betalen niet. Desnoods bouwen we het hele netwerk van nul weer op.'

Hij bracht een duidelijk en consistent verhaal. Alleen gebeurde er iets vreemds: de stad verdween van Play's wall of shame. Zonder te betalen? Dat kan eigenlijk niet, hackers zijn geen lieverdjes, en Play is een geoliede machine die een stad als Antwerpen niet zomaar zal laten gaan. Diezelfde avond nog stuurde Bart De Wever me een bericht. 'Antwerpen is van de wall of shame gehaald, zonder dat we iets deden. Is dit jou ooit eerder overkomen?' Mijn antwoord was kort maar duidelijk: 'Nee. Dit bewijst dat er onderhandeld wordt, of dat er betaald is.' De burgemeester herhaalde stellig dat dat niet het geval was. Dat kan, maar het is vrij onwaarschijnlijk. Ik ben ervan overtuigd dat De Wever echt gelooft dat er nooit met de hackers contact is opgenomen, al hoorde ik vanuit mijn netwerk dat Digipolis wel degelijk op zoek was naar een onderhandelaar, zolang die maar niet verbonden was met ons bedrijf. Door mijn rechtstreekse demarche richting Bart De Wever was de relatie met Digipolis wat verzuurd.

Om eerlijk te zijn weet ik niet exact hoe die case is afgehandeld. Waren er daadwerkelijk perfect bruikbare back-ups, zoals later werd beweerd? En zelfs als dat het geval was, startte niemand niet eens een onderhandeling op? Mijn vermoeden dat de stad betaalde, blijft groot. Al kan ik dat niet bewijzen. Uiteindelijk doet het er weinig toe. Het voornaamste is dat de stad de aanval aangreep om extra in te zetten op cybersecurity. Ze besloot de aanval aan te grijpen om door de zure appel heen te bijten en het verouderde netwerk grondig te verbeteren met Chinese walls. Nu zijn de fundamenten van het netwerk aanzienlijk sterker. Digipolis heeft de vernieuwing waar we zo vaak om vroegen uiteindelijk toch doorgevoerd. Al kwam onze samenwerking niet meer goed, het vertrouwen was zoek. Na het voorval is ons contract met hen voor zeventig procent teruggeschroefd. Enkel voor datgene waarin we in België uniek zijn, kloppen ze nog bij ons aan.

Het is wel grappig hoe er geruchten de ronde doen over een derde partij die het losgeld voor Antwerpen zou hebben betaald.

Het is wel grappig hoe er geruchten de ronde doen over een derde partij die het losgeld voor Antwerpen zou hebben betaald. Over het drugsmilieu bijvoorbeeld, dat niet zou willen dat bepaalde gegevens naar buiten zouden komen, of criminele organisaties die koste wat het kost wilden vermijden dan hun interne keuken bekend zou raken. Dat zijn mooie verhalen, maar de kans is bijzonder klein. Je kunt niet zomaar even onderhandelen met hackers. Dat kan enkel in een beveiligde omgeving die door de hackers zelf is gecreëerd en die je alleen kunt bereiken via een link in de ransom note. Dat is het bericht dat de hackers naar je computer sturen om uit te leggen wat er is gebeurd en welke stappen

je nu moet volgen. Ik schat dat ongeveer vijftig medewerkers van de stad die note hebben gezien, maar dat iemand zomaar even op de link heeft geklikt en een paar miljoen aan bitcoins heeft betaald zonder dat iemand dat wist? Die kans is toch nihil?

Het is ook niet alsof iedereen zomaar een mail kan sturen naar de hacker met 'Zeg, ik wil dit betalen voor Antwerpen, kunnen we een deal maken?' Zo werkt het niet. Heel veel journalisten hebben geprobeerd met hackersplatform Play in contact te komen omdat het een grote zaak was. Maar die reageren daar niet op.

Wat in Antwerpen precies gebeurd is, weet ik dus niet. Ik weet ook niet voor helemaal zeker langs welke van de vele zwakheden van het netwerk de hackers zijn binnengeraakt. Ik weet alleen dat het netwerk er een pak veiliger is geworden dankzij een aanzienlijke investering en het feit dat deze aanval een downtime heeft gegeven die IT-diensten nodig hadden om alles te verbeteren. Journalisten en politici schatten het kostenplaatje als gevolg van de cyberaanval op 100 miljoen. Hoe duur de les voor de stad echt was, zullen we wellicht nooit weten.

02

HOE HET BEGON

‘Geert, begin alsjeblieft
nooit iets in de
elektronica, want
je zou onze school een
slechte naam geven.’

Het is vreemd hoe sommige momenten later kantelmomenten blijken te zijn, voorbodes voor wat komt. Als kind had ik echt niet kunnen denken dat ik ooit aan het hoofd zou staan van mijn eigen cybersecuritybedrijf, laat staan dat ik hele dagen met cybercriminelen zou onderhandelen. Maar er waren wel degelijk omstandigheden en mensen in mijn jeugd die me hebben gevormd, die me dingen hebben geleerd, die me hebben gebracht waar ik nu sta.

Met stip op één: de school. Niet om de reden die je misschien zou denken, ik kan nog steeds geen vijf zinnen zonder fouten schrijven en wat wiskunde betreft hoef je me ook niet veel te vragen. Voor een deel komt dat doordat ik tijdens mijn lagereschoolperiode zo vaak in het ziekenhuis lag door zware astma-aanvallen. Toen die rond mijn dertiende stopten, kreeg ik die achterstand niet weggewerkt. Ik kon me maar moeilijk concentreren, in die tijd spraken ze nog lang niet over zaken als ADHD, en ik worstelde me door de middelbare school. Soms slaagde ik, soms moest ik een jaar overdoen, die schoolperiode duurde tergend lang. Ik haatte iedere dag die ik op de schoolbanken moest slijten, niet alleen omdat ik de leerstof nauwelijks aankon, maar vooral vanwege de voortdurende stress om gepest te worden. En gepest werd ik, die hele ellendige schooltijd lang, om zoiets onbenulligs als mijn gewicht. Begrijp me niet verkeerd: over pesten valt er werkelijk niks positiefs te vertellen, maar het leerde me wel een vaardigheid die ik nog steeds goed kan gebruiken: ik leerde verdwijnen. Ik kan vrij makkelijk opgaan in de massa, me zo gedragen dat mensen me niet zien. Wie niet opvalt, kan kijken, mensen observeren, inschatten wat een ander denkt of zal doen. Ik trainde me in het doorgronden van de motieven van mensen, om te weten wat hun volgende zet zou zijn, om me uit een netelige positie te wringen en me niet te laten intimideren door een of andere bullebak. Ik hoef niet uit te leggen dat die gave me goed van pas komt wanneer een cybercrimineel me de zwaarste beledigingen naar het hoofd slingert.