NÉGOCIER DANS L'OMBRE

GEERT
BAUDEWIJNS

NÉGOCIER DANS L'OMBRE

Racine

SOMMAIRE

01

L'AFFAIRE D'ANVERS

« La Ville d'Anvers
a été piratée. »

Ce n'est pas ce qui est indiqué sur ma carte de visite, mais lorsqu'on me demande ce que je fais, je réponds généralement: «Négocier avec des cybercriminels.» C'est en effet l'aspect le plus concret de mon travail dans la cybersécurité: communiquer avec les pirates informatiques qui paralysent les réseaux des entreprises à coup de *ransomwares*, des rançongiciels. Les pirates trouvent sans cesse de nouvelles méthodes pour infiltrer les réseaux, installer des logiciels malveillants, rendre toutes les données illisibles et les copier. Ils exigent ensuite une rançon pour rétablir l'accès aux données et ne pas les divulguer. Autrement dit, ils pratiquent le chantage pur et simple.

Les entreprises concernées se retrouvent au pied du mur. Plus rien ne fonctionne et elles sont donc obligées de renvoyer la plupart de leurs employés chez eux, d'interrompre la production et les services et de demander au personnel informatique de faire des heures supplémentaires. Elles en arrivent souvent à la conclusion que payer une rançon est la solution la plus rapide, la moins coûteuse, voire la seule possible. C'est alors qu'elles font appel à moi. En tant que négociateur, mon travail ne consiste pas à traquer les cybercriminels, mais à discuter avec eux, parfois pendant des jours ou des semaines. Mon objectif est de faire baisser leurs exigences financières et de comprendre comment ils sont entrés dans le système. Bien sûr, devoir céder aux exigences de pirates informatiques sans scrupules me laisse un goût amer, mais je fais tout mon possible pour réduire au minimum le montant de la rançon, de sorte que la plupart des entreprises s'en sortent indemnes.

L'affaire de piratage la plus célèbre en Flandre est sans doute celle qui a frappé la Ville d'Anvers à la fin 2022. Chaque fois que je discute avec quelqu'un et qu'on en vient à parler de mon travail, on me pose cette question: «Mais que s'est-il réellement passé à Anvers?» La cyberattaque dont la Ville a été victime – cerise sur

le gâteau, c'était la nuit de la Saint-Nicolas – continue de fasciner et reste gravée dans la mémoire collective. L'histoire a effectivement de quoi attiser l'imagination: une date symbolique, une ville renommée et un dénouement curieux, sur lequel des rumeurs persistent. Pour moi, cette question a une double connotation, car pour être franc, «l'affaire d'Anvers» suscite toujours en moi une certaine émotion. À l'époque du piratage, nous étions, en tant que fournisseurs, étroitement liés à Digipolis, le partenaire informatique de la Ville, responsable d'un large éventail de services allant de la maintenance du réseau au développement numérique des services municipaux. La cybersécurité relève également de ses attributions, un aspect qu'Anvers prend particulièrement au sérieux depuis le piratage de Liège.

À l'époque du piratage, nous étions, en tant que fournisseurs, étroitement liés à Digipolis, le partenaire informatique de la Ville.

En juin 2021, la Ville de Liège avait été victime d'une attaque de *ransomware* menée par le groupe Ryuk. C'était la première fois qu'une métropole belge se retrouvait totalement paralysée. Selon les médias, la Ville aurait payé une rançon de 30 millions d'euros, ce qui, à Anvers, a fait retentir toutes les sonnettes d'alarme. En conséquence, la Ville a fait de la cybersécurité une priorité, et le conseil municipal a débloqué des fonds supplémentaires pour éviter un scénario similaire à celui de Liège. C'est dans ce contexte qu'Anvers a confié à Digipolis, son partenaire technologique, la tâche d'élaborer un plan de cybersécurité approfondi. L'objectif était clair: renforcer les défenses numériques de la Ville et rendre ses systèmes imperméables aux cybermenaces. Digipolis a alors lancé plusieurs appels d'offres, dont certains ont été remportés par notre société. Notre mission

consistait à rechercher et à signaler les vulnérabilités potentielles du réseau. Nous n'étions pas responsables des tâches opérationnelles; notre rôle consistait à repérer les points d'accès utilisables par des attaquants potentiels.

À l'époque, les failles de sécurité étaient nombreuses; ce n'est pas inhabituel et c'est le cas dans de nombreuses entreprises. Il faut tenir compte du fait que le réseau d'Anvers, comme celui de nombreuses autres grandes villes, repose sur une infrastructure datant de 20 ou 30 ans. Nous observons le même problème chez bon nombre de nos clients. Ils commencent par mettre en place un petit réseau, qui doit ensuite faire l'objet d'une extension ultrarapide sans qu'il soit possible d'interrompre le fonctionnement des applications ou des services existants. Au cours de ces 15 dernières années, par exemple, avec la numérisation des services municipaux, le réseau d'Anvers s'est considérablement développé. Partout, les réseaux doivent sans cesse évoluer, et à un rythme qui ne laisse pas vraiment le temps de se demander si les fondations du système sont sécurisées de manière adéquate et correcte, si elles sont suffisamment robustes pour supporter de nouvelles extensions, ou suffisamment à l'épreuve du temps en termes de sécurité, par exemple.

La modernisation de systèmes obsolètes est loin d'être simple et les informaticiens la considèrent comme la tâche la plus complexe, car ils doivent trouver un moyen de combiner les nouvelles technologies aux anciennes. Ce processus demande non seulement des investissements considérables en temps et en argent, mais aussi une expertise technique approfondie. L'une des méthodes les plus efficaces pour renforcer la sécurité consiste à mettre en place des *Chinese walls*, une technique également connue sous le nom de *subnetting*.

Le *subnetting* est le processus qui consiste à diviser un réseau en segments ou sous-réseaux, plus petits et plus faciles à gérer.

Chacun de ces sous-réseaux peut alors fonctionner de manière autonome, avec ses propres protocoles de sécurité et son propre contrôle d'accès. En segmentant ainsi le réseau d'une ville, on isole des autres chacune des sections, ce qui limite l'impact potentiel des cyberattaques et protège les informations sensibles.

La mise en place de sous-réseaux dans un réseau existant représente une tâche considérable et extrêmement complexe. Il faut en effet mettre en place de nouveaux protocoles, former les employés à l'utilisation de la nouvelle structure et remplacer les systèmes obsolètes. Comme il est impossible d'interrompre, même brièvement, l'ensemble des services municipaux, toutes les modifications doivent être apportées sans perturber les activités quotidiennes de la ville. En plus des compétences techniques nécessaires, un important travail de coordination est donc requis. De plus, inutile de le nier, ces changements coûtent cher. Très cher.

Un problème supplémentaire lié aux réseaux vieillissants est l'impossibilité de mettre à jour certains logiciels en raison de l'obsolescence de la technologie sous-jacente. En effet, pour sécuriser de manière optimale un système relativement ancien, l'assistance du fournisseur est indispensable. Cependant, les fournisseurs arrêtent souvent de soutenir les technologies obsolètes environ cinq ans après le développement d'un logiciel. Dès lors, il devient impossible d'installer des mises à jour de sécurité. Pour ces applications dépassées, la pendule s'arrête à ce moment-là, tandis que celle des pirates informatiques se met à tourner. Ces derniers recherchent les failles exploitables, sachant que les fournisseurs ne prendront plus de mesures pour y remédier. En d'autres termes, il ne s'agit que d'une question de temps avant qu'un incident survienne. Une ville peut alors se trouver dos au mur, car que les fournisseurs les soutiennent ou non, ses applications obsolètes doivent continuer à fonctionner.

C'est pour cette raison qu'à un moment donné, j'ai demandé à rencontrer le PDG de Digipolis. Je souhaitais lui faire part personnellement de la gravité des problèmes et le persuader d'intervenir. Notre échange a été plutôt cordial. Je lui ai expliqué point par point où se situaient les vulnérabilités et il a acquiescé plus souvent qu'à son tour. Toutefois, même s'il convenait qu'une action était nécessaire, j'ai bien senti que chez Digipolis, personne n'était pleinement conscient de l'urgence de la situation.

Honnêtement, je me suis senti frustré. Alors qu'à l'étranger, mon expertise est reconnue, dans mon propre pays, on me considère souvent comme un consultant parmi tant d'autres. Sauf que je suis quotidiennement au cœur de l'action, que je connais mieux que quiconque les informations et les outils que l'on peut trouver sur le darknet et que je suis capable de démontrer précisément avec mon équipe où se trouvent les failles d'un système de sécurité. Nous parvenons souvent à détecter une attaque avant même qu'elle se produise, car les premiers signaux peuvent toujours être identifiés sur le darknet. C'est ce qui nous distingue des autres sociétés de sécurité. Il y a beaucoup de choses que je ne suis pas en mesure de faire, mais il y en a une que je maîtrise parfaitement: sentir quand les choses vont mal tourner et désigner le point faible concerné. Et tout cela, uniquement grâce aux informations que nous trouvons sur le darknet.

À un moment donné, face à la multiplication des signaux d'alarme, j'ai décidé de prendre les choses en main. Début novembre 2022, j'ai contacté Bart De Wever, bourgmestre de la Ville d'Anvers et président de la N-VA, la Nouvelle Alliance flamande. Ce pas n'a pas été difficile à franchir, même si je ne l'avais jamais rencontré en personne auparavant. Notre entreprise travaillait en étroite collaboration avec la N-VA au niveau national et, à cette époque, j'étais candi-

dat pour ce parti dans ma commune. Je lui ai simplement envoyé un message: «J'aimerais vous rencontrer un de ces jours.» Sa réponse ne s'est pas fait attendre: «Très bien, fixez un rendez-vous avec ma secrétaire.» Nous avons convenu d'une date, le 28 novembre. Son chef de cabinet et lui-même m'accordaient une heure.

Le jour venu, j'ai franchi les portes imposantes de l'hôtel de ville d'Anvers, un endroit que je ne connaissais jusque-là que de l'extérieur. Après m'être enregistré et présenté à la réception, j'ai monté les marches majestueuses de l'escalier, bordé de splendides tableaux, qui menait au bureau du bourgmestre. Son chef de cabinet et lui m'ont accueilli chaleureusement, même si nous n'avons pas perdu de temps en politesses; j'étais venu avec une mission bien précise. L'entretien devait durer une heure, mais nous avons finalement discuté à bâtons rompus pendant deux heures. J'ai partagé mes inquiétudes à propos des méthodes des hackers, souligné les failles du système et exprimé ma frustration face au manque de réactivité.

À peine une semaine plus tard, alors que je participais à une mission économique au Japon, j'ai reçu un message du chef de notre service technique: «La Ville d'Anvers a été piratée.» C'était le 6 décembre, je ne l'oublierai jamais.

J'ai immédiatement allumé mon ordinateur pour consulter le darknet. Effectivement, le groupe Play, l'un des grands collectifs de pirates informatiques, revendiquait l'attaque de la Ville. Sur son *Wall of shame* – le «mur de la honte», un genre de tableau d'affichage numérique où sont listées toutes les «affaires en cours» –, le nom d'Anvers figurait en tête de liste, accompagné d'un compte à rebours jusqu'à l'échéance fixée par les hackers.

Tous les grands collectifs de *ransomware* possèdent ce genre de mur de la honte, dont le nom de la victime est effacé une fois la rançon payée. Mais ce n'était pas encore le cas: sous le nom d'Anvers, les secondes s'égrenaient inexorablement.

J'avoue avoir été très surpris par la rapidité avec laquelle mes prédictions se sont réalisées. J'avais annoncé moins d'une semaine plus tôt qu'une attaque risquait de se produire, et voilà que c'était le cas. J'ai immédiatement envoyé un message à Bart De Wever: «La Ville d'Anvers a été piratée. En avez-vous déjà été informé?» Ce message peut sembler étrange, mais il est fréquent que les dirigeants soient avertis tardivement d'une cyberattaque. Souvent, les services informatiques tentent de résoudre le problème en interne ou préfèrent exposer la situation à leur supérieur direct avant d'informer le PDG ou, dans notre cas, le bourgmestre. De Wever m'a tout de suite répondu qu'il était parfaitement au courant de la situation. Il me demandait de ne rien faire pour l'instant, ajoutant en plaisantant: «La semaine dernière, vous m'avez décrit exactement ce qui allait se passer aujourd'hui. Vous êtes donc maintenant le suspect numéro un.» Je n'ai pas pu m'empêcher de lui répondre en gloussant: «Toute affaire a besoin d'un suspect, et je suis ravi de jouer ce rôle.»

Cependant, il n'y avait pas vraiment de quoi rire. De nombreux services étaient paralysés et incapables de fonctionner: pas de passeports, pas de permis de construire, déchetteries fermées – tous les processus informatisés devaient passer en mode manuel.

En outre, les pirates avaient mis la main sur 557 gigaoctets de données qu'ils menaçaient de divulguer. On ignorait précisément quelles données avaient été compromises, mais on craignait qu'il s'agisse de données personnelles d'administrés, ce que le bourgmestre démentirait d'ailleurs quelques semaines plus tard.

En peu de temps, les journalistes ont eu vent de l'histoire et ont publié article sur article au sujet de la cyberattaque massive contre le réseau informatique d'Anvers. Au milieu de ce tumulte, le bourgmestre est resté ferme: «Nous ne négocierons pas, nous ne paierons pas. Si nécessaire, nous reconstruirons tout le réseau

à partir de zéro.» Son discours était clair et cohérent. Pourtant, une chose étrange s'est produite: le nom de la ville a disparu du mur de la honte du groupe Play. Sans paiement? Difficile à imaginer. Les hackers ne sont pas tendres, et Play est une organisation bien rodée qui ne laisserait pas une ville comme Anvers s'en sortir aussi facilement. Le soir même, Bart De Wever m'envoyait un message: «Anvers a été retirée du mur de la honte sans que nous ayons fait quoi que ce soit. Vous avez déjà vu ça?» Ma réponse a été brève, mais sans équivoque: «Non. Cela prouve qu'il y a eu soit négociations, soit paiement.» Le bourgmestre m'a alors fermement répété que ce n'était pas le cas. Possible, mais peu probable. Je suis convaincu que De Wever croyait réellement que les hackers n'avaient pas été contactés, bien que mon réseau m'ait informé que Digipolis cherchait effectivement un négociateur, qui devait n'avoir aucun lien avec notre entreprise. Ma démarche directe auprès de Bart De Wever avait quelque peu tendu les relations avec Digipolis.

Ce qui est amusant, c'est que des rumeurs circulent au sujet d'une tierce partie qui aurait payé la rançon pour Anvers.

Pour être franc, je ne sais pas exactement comment cette affaire a été résolue. Y avait-il réellement des sauvegardes parfaitement exploitables, comme on l'a prétendu par la suite? Et même si c'était le cas, est-il vrai que personne n'a engagé de négociations? Je soupçonne toujours fortement la Ville d'avoir payé, même si je ne peux pas le prouver. Au final, cela importe peu. L'essentiel, c'est que la Ville a profité de l'occasion pour redoubler d'efforts en matière de cybersécurité. Elle a décidé de tirer parti de l'attaque, d'avaler la pilule et de moderniser complètement son réseau informatique obsolète en le dotant de sous-réseaux. Aujourd'hui,

ce réseau repose sur des bases beaucoup plus solides. Digipolis a enfin procédé au renouvellement que nous avions si souvent réclamé. Mais cela n'a pas été bénéfique à notre collaboration, car la confiance avait disparu. Après cette affaire, notre contrat a été réduit de 70 %. Digipolis ne fait plus appel à nous que pour les services que nous sommes les seuls à offrir en Belgique.

Ce qui est amusant, c'est que des rumeurs circulent au sujet d'une tierce partie qui aurait payé la rançon pour Anvers. On parle de barons de la drogue, par exemple, qui n'auraient pas voulu que certaines informations soient divulguées, ou d'organisations criminelles qui auraient cherché à tout prix à éviter que leurs activités soient révélées au grand jour. Ce sont des histoires amusantes, mais il est très peu probable qu'elles soient vraies. Négocier avec des pirates informatiques n'est pas simple. Cela ne peut se faire que dans un environnement sécurisé créé par les hackers eux-mêmes et accessible uniquement via un lien figurant dans la note de rançon, un message que les pirates envoient à l'ordinateur de la victime pour expliquer ce qui s'est passé et indiquer la marche à suivre. J'estime probable qu'une cinquantaine d'employés de la Ville aient vu cette note, mais la possibilité que l'un d'entre eux ait cliqué sur le lien et payé quelques millions d'euros en bitcoins à l'insu de tous est inexistante.

On ne peut pas envoyer un e-mail à un pirate pour lui dire: «Dites-moi, je veux payer la rançon pour Anvers. On peut passer un accord?» Ça ne fonctionne pas comme ça. Comme il s'agissait d'une grosse affaire, de nombreux journalistes ont tenté d'entrer en contact avec la plateforme de hackers Play, mais ils n'ont reçu aucune réponse.

Je ne sais donc pas exactement ce qui s'est passé à Anvers. Je ne sais pas non plus avec certitude laquelle des multiples failles a été exploitée par les pirates pour pénétrer dans le réseau. Tout ce que

je sais, c'est que ce réseau est désormais beaucoup plus sûr grâce à un investissement considérable et au fait que la cyberattaque a provoqué l'interruption du système dont les services informatiques avaient besoin pour apporter toutes les améliorations nécessaires. Journalistes et politiciens ont estimé le coût de cette cyberattaque à 100 millions d'euros. Mais nous ne saurons sans doute jamais combien cette leçon a réellement coûté à la Ville.

02

COMMENT TOUT A COMMENCÉ

«Geert, s'il te plaît, ne travaille jamais dans l'électronique; la réputation de notre école en souffrirait.»

Avec le recul, il est étonnant de constater que certains moments ont été de véritables signes avant-coureurs, annonçant la tournure que prendrait notre vie. Enfant, je n'aurais jamais pu imaginer que je dirigerais un jour ma propre entreprise de cybersécurité, et encore moins que je passerais des journées entières à négocier avec des cybercriminels. Pourtant, durant ma jeunesse, certaines circonstances et certaines personnes ont forgé ma personnalité et m'ont appris des choses qui m'ont permis de devenir celui que je suis aujourd'hui.

L'école figure en tête de liste, mais pas pour les raisons auxquelles on pourrait s'attendre: je suis toujours incapable d'écrire trois phrases sans faire de faute, et je ne suis vraiment pas doué en maths. Ces lacunes sont en partie dues au fait que pendant l'école primaire, j'ai passé beaucoup de temps à l'hôpital en raison de graves crises d'asthme. Quand elles ont cessé, vers l'âge de 13 ans, je n'ai pas pu rattraper mon retard. J'avais du mal à me concentrer – à l'époque, on ne parlait pas encore de TDAH – et j'ai eu de grosses difficultés au collège. J'obtenais parfois de bons résultats; parfois, j'ai dû doubler; cette période de ma scolarité m'a semblé interminable. J'ai détesté chacune des journées passées sur les bancs de l'école, non seulement parce que j'avais toutes les peines du monde à comprendre les matières enseignées, mais surtout parce que la peur d'être harcelé me stressait continuellement. J'ai en effet été harcelé tout au long de ma maudite scolarité à cause de mon poids. Le harcèlement n'a évidemment absolument rien de positif, mais il m'a permis d'acquérir une compétence qui me sert encore aujourd'hui: j'ai appris à disparaître. Je peux facilement me fondre dans la masse et agir de manière à passer inaperçu. Ne pas se faire remarquer permet d'observer les autres, d'évaluer leurs pensées ou leurs intentions. Je me suis entraîné à sonder les motivations des gens, à anticiper leurs actions, à me tirer de situations délicates et à ne pas me laisser in-