La cyberdéfense dans l'environnement critique belge : de la protection à l'entraînement proactif

Clément Le Gouellec

Veiligheidsstrategie - Stratégie de sécurité

De digitale wereld moet een betrouwbare omgeving blijven, daarom is cyberveiligheid een niet meer weg te denken begrip voor mensen, ondernemingen en staten. De hieraan verbonden uitdagingen zijn talrijk: bescherming van de persoonlijke levenssfeer, geringere beschikbaarheid van de essentiële diensten, financiële risico's en imagoschade voor de ondernemingen, of zelfs schending van de soevereiniteit in het geval van naties. Vooral de Belgische omgeving is het slachtoffer van cyberaanvallen, aangezien belangrijke internationale organisaties hun zetel in België hebben. Cyberaanvallen vinden veelvuldig plaats, zijn min of meer ernstig en kunnen het werk zijn van actoren die over zeer heterogene vaardigheden bezitten. Het is dan ook onontbeerlijk dat de ingezette menselijke middelen een degelijke voorbereiding genieten en de beschikbare systemen al in een vroeg stadium van de ontwerpfase rekening houden met het aspect "cyberveiligheid".

Om die reden heeft Thales beslist tot de oprichting van een nieuwe trainings- en testomgeving op het vlak van cyberveiligheid: het CyberLab. Dit centrum simuleert alle cyberaanvallen, zelfs de recentste en meest complexe, en helpt trainen op de verdediging van de meest complexe systeemarchitecturen. De opleiding voorziet in een vorming over cyberveiligheid voor operationele teams bij aanvalsscenario's en in de beheersing van cybertechnologieën. Goed opgeleid personeel en veilige IT-voorzieningen bieden bescherming, zelfs bij de gevaarlijkste cyberaanvallen.

Het CyberLab van Thales kan ook systemen simuleren, van de eenvoudigste tot de meest complexe, om hun veerkracht bij een aanval te analyseren. Ingenieurs gespecialiseerd in cyberveiligheid testen de systemen om eventuele tekortkomingen op te sporen. Als men de tekortkomingen van een systeem kent, kan Thales dit systeem beveiligen tegen eventuele cyberaanvallen en veerkrachtiger maken.

In België begeleidt Thales al 70 jaar de regering en de grote Belgische strategische ondernemingen bij de ontwikkeling en het beheer van hun kritieke systemen, onder meer op het gebied van cryptografie en cyberveiligheid. Soevereiniteit inzake cyberveiligheid is absoluut noodzakelijk wil men succes oogsten bij de strategische uitdagingen die de digitale wereld inhoudt. Wij zijn ervan overtuigd dat deze zelfstandigheid technische vaardigheden op regeringsniveau vereist, waarbij men op redelijke wijze afhankelijk is van betrouwbare nationale industriëlen.

Ces dernières années ont vu apparaître une évolution majeure : l'intégration des technologies numériques dans tous les systèmes, qu'ils soient industriels, militaires ou dans les services aux citoyens. Le tout numérique, c'est une opportunité majeure pour l'évolution de notre société au sens large du terme, et pour la Défense en particulier. Par exemple, l'opportunité de prendre des décisions plus rapidement ou encore l'opportunité d'optimiser les coûts des fonctions de supports.

Les *cybermenaces* sont le revers de la médaille de la digitalisation. Il est primordial de les prendre en compte, afin que l'univers numérique reste un environnement de confiance. La cybersécurité est donc un enjeu majeur de ce 21e siècle. Les sujets sont multiples : protection de la vie privée, risque financier pour les entreprises, espionnage industriel et atteinte à la souveraineté pour les nations.

L'environnement belge fait souvent l'objet de cyberattaques, avec ses organisations internationales, fédérales et régionales, ainsi qu'avec ses entreprises industrielles de premier plan. La description de la menace par les médias peut sembler superficielle et ne fait pas nécessairement état de la gravité des différents types d'attaque. Nous nous proposons ici d'en faire un rapide tour d'horizon.

Les attaques courantes les plus visibles sont les défigurations de sites Internet d'entreprises ou d'administrations.

L'objectif peut être ludique, ou plus répréhensible avec la diffusion de messages faisant l'apologie du terrorisme. Ces attaques sont aisées et accessibles à un large public.

Début 2015, à la suite des attentats contre *Charlie Hebdo*, il y a eu, par exemple, une vague de défigurations de sites Internet pour afficher des messages favorables aux attentats. Ces « graffitis du web », peu complexes, ont un impact médiatique très fort.

Les attaques par déni de service distribué (désignées par l'acronyme « DDoS », *distributed denial-of-service*) visent, quant à elles, à bloquer les services en saturant les serveurs. Ces attaques peuvent être très complexes tout en n'ayant pour seul impact immédiat l'indisponibilité de ces services.

À l'automne 2016, une attaque DDoS sur les services de redirection d'URL, se manifestant par la prise de contrôle de milliers de caméras connectées, a rendu indisponible une grande partie des géants de l'Internet pendant plusieurs heures. En Belgique, des attaques de ce type ont eu pour cible des administrations publiques.

Par ailleurs, un véritable cyberbanditisme se développe. Les virus ont maintenant trouvé un modèle économique de criminalité classique. Appelés *ransomware* ou rançongiciel (mot-valise de « rançon » et « logiciel »), ces logiciels chiffrent les données pour les rendre inutilisables, exigeant le paiement d'une rançon en échange du déchiffrement.

Les rançons augmentent et les logiciels se complexifient. Ces techniques sont aujourd'hui mises en œuvre par des organisations de plus en plus structurées. L'origine géographique est difficile à détecter, même si de forts soupçons pèsent sur la Chine ou encore sur la Russie.

Depuis le mois de mai, les *ransomwares* Wannacry et NotPetya ont frappé des centaines d'organisations à l'échelle mondiale. Dans les hôpitaux, ces attaques ont des conséquences immédiates sur la chaîne logistique, pouvant aller jusqu'à entraver le fonctionnement opérationnel des services.

D'autres attaques, très silencieuses et discrètes, visent à pénétrer les réseaux d'acteurs industriels ou étatiques afin de voler des informations techniques, stratégiques ou encore commerciales. Ces intrusions nécessitent une connaissance technique pointue, les assaillants étant sous la protection de certains États, ou directement sous les ordres d'un gouvernement.

Les exemples sont multiples bien que souvent confidentiels. Aux États-Unis, un vol de données sur les dossiers des habilitations de sécurité a eu lieu. En France, plusieurs cas par semaine sont signalés par les industriels. Il est difficile de détecter ces intrusions car les assaillants souhaitent rester discrets. Si aucune recherche proactive n'est engagée, il est peu probable que les assaillants soient identifiés.

L'étape suivante consiste à prendre le contrôle de systèmes pour agir directement sur ceux-ci. Ainsi, le vol d'informations n'est pas dangereux en soi, mais la modification de paramètres de contrôle l'est. Par exemple, l'altitude d'un avion n'est pas une donnée confidentielle, mais si cette donnée est modifiée, l'accident est assuré.

Nombreux sont les exemples non létaux : la destruction de centrifugeuses du programme nucléaire iranien par des assaillants gouvernementaux ou encore l'interception de drones de combat.

À l'heure actuelle, il existe peu d'exemples de ce type d'attaques complexes ayant entraîné de graves conséquences qui sont connus du grand public. Ce n'est pas une question de faisabilité. L'existence d'organisations capables de mener des actions offensives de mercenariat pour le compte d'acteurs terroristes est un risque très inquiétant.

Les cyberattaques sont nombreuses, de gravité variable et peuvent être menées par des acteurs aux compétences très hétérogènes. Il faut avoir conscience de ces menaces pour être capable de les combattre. Aujourd'hui, la menace s'accroît vers les systèmes d'armes ou aéronautiques : le champ et la pertinence des contremesures doivent s'adapter, les compétences du personnel et l'expertise également.

Le monde est plus digital et plus dangereux, mais aussi plus réglementé qu'auparavant. Certains acteurs, privés ou publics, fournissent des services essentiels à la nation. On peut notamment citer les réseaux de distribution d'eau, les hôpitaux, les fournisseurs d'énergie, les entreprises de transport, les réseaux de télécommunications, les établissements financiers ou encore les administrations critiques. Une interruption de ces services n'est pas acceptable pour la société.

En 2018, deux réglementations majeures entreront en vigueur : la directive SRI et le RGPD.

La directive SRI (directive concernant la sécurité des réseaux et de l'information) oblige les acteurs économiques et gouvernementaux à prendre des mesures fortes pour garantir la sécurité de leurs systèmes

d'information. Les opérateurs concernés devront définir et appliquer une politique de sécurité adaptée au niveau de menace. Par ailleurs, ils devront notifier à l'autorité compétente tout incident lié à la sécurité informatique. Pour ce faire, des moyens de détection devront être mis en place.

Le RGPD (règlement général sur la protection des données) comporte des exigences de sécurité concernant les données personnelles. Les sanctions pour un manquement en matière de sécurité sont dissuasives (4 % du chiffre d'affaires annuel ou 20 millions d'euros pour les organismes publics). Les organisations qui traitent des données personnelles devront mettre en place les mesures techniques nécessaires à la confidentialité des données et en démontrer l'efficacité.

En Belgique, le Centre pour la cybersécurité Belgique (CCB) aura pour charge de transposer la directive SRI en droit national et d'en vérifier l'application. Le respect du RGPD sera, lui, vérifié par la Commission de la protection de la vie privée.

Par ailleurs, la Belgique a défini des intérêts essentiels de sécurité, qui délimitent les domaines stratégiques pour la défense et la sécurité nationales. Le domaine cyber est central dans ces intérêts de sécurité.

CYBERLAB

La cybersécurité est donc un marché en forte croissance (+10 % par an en moyenne), qui alimente un besoin permanent en nouveaux spécialistes. On estime d'ailleurs qu'il manquera quelque deux mille experts en cybersécurité en Belgique d'ici à 2020.

Dans un contexte de croissance de la menace et de la technicité des attaques, certains acteurs souhaitent entraîner leurs équipes (techniques et managériales) et s'assurer de la robustesse de leurs systèmes. Ces entraînements et ces tests de résistance sont difficiles à réaliser en environnement réel, car les conséquences sont peu maîtrisables et susceptibles mettre en danger les capacités opérationnelles des systèmes d'information. La possibilité de simuler est donc cruciale pour réduire les coûts et les risques.

La cybersécurité avait besoin de son simulateur de vol.

Le CyberLab permet de répliquer de façon réaliste les systèmes informatiques d'entreprises et d'acteurs publics, afin de les préparer aux cyberattaques. Il permet de renforcer l'entraînement des spécialistes et de contribuer aux activités de recherche et de développement en cybersécurité. Ce CyberLab est le centre européen de services d'entraînement et de simulation cyber du groupe Thales.

Il ne s'agit pas de se substituer aux organismes de formation en matière de cybersécurité bien établis, mais d'offrir des services sur mesure dans un environnement de confiance, en prenant en compte les spécificités métiers des utilisateurs, en particulier pour les applications de la Défense. Positionné au cœur de l'écosystème des institutions situées en Belgique, le CyberLab s'insère dans l'offre globale de services de sécurité.

La capacité CyberLab est aussi un puissant outil de vulgarisation : il permet de rendre le cyber visuel en montrant l'impact des attaques et l'efficacité des mesures de sécurité mises en place.

Pour proposer des services de type CyberLab de haut niveau, il convient de combiner deux atouts essentiels. D'une part, la maîtrise de l'ensemble de la chaîne de la cybersécurité : c'est-à-dire du conseil en gouvernance à la réponse aux incidents, en passant par la détection d'attaques et par le chiffrement des données. D'autre part, la connaissance des métiers permet de s'adapter au mieux aux enjeux spécifiques des utilisateurs.

Techniquement, une capacité de type CyberLab se base sur trois composants principaux :

- une plateforme de virtualisation de réseaux ;
- un générateur de trafic ;
- des composants réels ou virtuels.

Une capacité CyberLab est pertinente quand elle est destinée à des utilisateurs ayant déjà une certaine maturité en matière de cyberdéfense. Il s'agit donc principalement :

- d'organisations internationales (OTAN, UE) ;
- de l'ensemble des services gouvernementaux ;
- d'entreprises critiques, notamment dans l'énergie, les transports, le spatial, l'industrie, les télécommunications ou encore le monde bancaire.

APPLICATIONS

La plateforme propose trois applications.

La première application porte sur l'entraînement des acteurs de la cybersécurité dans un environnement représentatif des systèmes réels.

Le facteur humain est essentiel pour l'amélioration de la sécurité des systèmes. La cybersécurité n'est pas un enjeu auquel seuls les informaticiens doivent être formés, il doit s'agir d'une démarche collective et coordonnée de toute structure qui souhaite se protéger. Le CyberLab contribue à la sensibilisation aux menaces et aux comportements d' « hygiène de sécurité » à adopter. Par ailleurs, il se profile un enjeu au niveau de l'entraînement des spécialistes.

Le CyberLab permet d'organiser des exercices de gestion de cybercrise, avec des scénarios d'attaque et de défense d'un système d'information. Ces exercices permettent notamment l'entraînement des équipes d'intervention rapide et de la chaîne de défense opérationnelle.

La qualité des scénarios est un élément essentiel pour proposer aux utilisateurs des situations réalistes d'entraînement. On peut distinguer deux types de scénarios : les scénarios généralistes, qui s'opposent aux scénarios « métiers » qui prennent en compte les spécificités du secteur de l'utilisateur.

La deuxième application concerne la validation de la stratégie de protection et du niveau de sécurité des architectures des systèmes d'information.

Cela permet aux États, aux administrations et aux entreprises de tester et de valider leurs systèmes d'information, en toute sécurité et en toute discrétion. Il s'agit de mener des *pen tests* (tests d'intrusion) simulés, sur le réseau d'une organisation reproduit dans le CyberLab.

Il est question ici d'évaluer la capacité de résistance et de résilience d'un État ou toute autre organisation face au cyberespionnage et aux cyberattaques.

Une troisième application est l'accompagnement pendant le développement de produits intégrant la cybersécurité dès leur conception, en les soumettant à une série de tests très exigeants. Demain, les produits non sécurisés perdront toute valeur sur le marché. Il s'agit donc d'accompagner les entreprises dans une approche de *security by design* (autrement dit, une sécurisation dès le stade de la conception) de leurs produits et solutions.

Par ailleurs, il est difficile pour les organisations de distinguer les produits de qualité dans l'ensemble de l'offre proposée sur le marché. Ainsi, les tests menés garantissent un certain niveau de qualité pour ces solutions et permettent d'accompagner les entreprises et les administrations pour réaliser les bons investissements.

Ce centre de recherche et d'entraînement est appelé à se développer. Au-delà de l'adaptation permanente à la menace, nous renforçons nos compétences et capacités, notamment en matière de simulation de systèmes industriels et de plateformes militaires.

Enfin, nous avons renforcé notre soutien au master en cybersécurité en lui ouvrant notre CyberLab. Ce cursus, premier du genre créé en Belgique, s'appuiera sur la plateforme pour mettre les étudiants dans des conditions d'attaque réalistes.

CHALLENGES

Nous sommes convaincus que les progrès en cours en Belgique, qui se sont concrétisés notamment avec la création du CCB et l'élaboration du cyberplan d'urgence, doivent encore s'amplifier pour atteindre un niveau satisfaisant en matière de cybersécurité.

La sécurisation du monde digital se nourrit de plusieurs facteurs : compétence technique autonome, formation de spécialistes, souveraineté des solutions mises en place, protection rigoureuse des acteurs critiques et coopération internationale. C'est l'ensemble de ces sujets qu'il convient de traiter. Au niveau gouvernemental, un des enjeux est d'assurer la protection du secret de défense et du secret industriel. Pour y répondre, il convient d'adopter une stratégie ambitieuse dans des domaines larges.

La souveraineté en matière de cybersécurité est absolument essentielle tant le monde numérique est le théâtre d'affrontements qui ne traduisent pas le jeu des alliances du monde physique. Ainsi, la capacité d'autonomie de décision nécessite des compétences techniques au niveau gouvernemental, en s'appuyant de façon raisonnable sur des industriels nationaux de confiance. Les similarités avec le renseignement sont réelles et les modes de fonctionnement de cette compétence peuvent s'inspirer des mêmes méthodes. Il s'agit de déployer une gestion continue des menaces en passant par une veille active sur l'état de l'art et une gestion proactive des configurations déployées par les services essentiels de l'État.

Par ailleurs, il est important que les autorités gouvernementales renforcent leur capacité à réagir face à une situation de crise intense. Cette « force d'intervention rapide » gouvernementale vise à aider les acteurs critiques à retrouver leurs capacités opérationnelles et permet à l'État de répondre si l'attaque provient d'un groupe criminel ou gouvernemental étranger. La cyberdéfense constitue la réponse « interactive » à des cyberattaques : la fulgurance et la professionnalisation des techniques d'attaques imposent une capacité de confinement de celles-ci, via une posture permanente de défense des ressources critiques.

La capacité de résistance d'un État face au cyberespionnage et aux cyberattaques étatiques dépend de la souveraineté, c'est-à-dire de la maîtrise technique de bout en bout, des solutions mises en place. C'est la seule façon de lutter contre les attaques, très silencieuses et souvent très discrètes, qui visent à pénétrer les réseaux d'acteurs industriels ou gouvernementaux afin de voler de l'information. Il nous semble naïf de se reposer sur des acteurs non européens pour fournir des solutions et produits de sécurité, dans le contexte actuel de recrudescence d'espionnage industriel.

Pour protéger ces systèmes sensibles, il faut prendre une avance technologique décisive dans le domaine du chiffrement et de la protection des données. Il s'agit d'initier une dynamique vertueuse pour le développement d'un tissu économique et technologique à haute valeur ajoutée dans ce domaine.

Pour les opérateurs économiques critiques, il convient de prendre des mesures exigeantes pour garantir qu'une cyberattaque n'aura pas de conséquences sur les services rendus. Une capacité de détection des attaques, une adaptation de la gouvernance de ces organisations face à ce risque, ainsi qu'une capacité à répondre rapidement aux incidents semblent être le minimum pour assurer une bonne continuité des services. Les coûts associés à ces mesures ne sont pas négligeables, pouvant représenter jusqu'à 20 % des dépenses en systèmes d'information pour ces acteurs. C'est néanmoins la condition pour assurer la continuité de ces fonctions essentielles à la population.

Si la confiance entre les gouvernements est difficile à atteindre en matière de cybersécurité et de cyberespionnage, cela ne doit pas occulter la collaboration entre États, par exemple au niveau européen, sur des sujets bien spécifiques. Il est, par exemple, tout à fait souhaitable d'échanger entre gouvernements des informations sur la menace et sur les vulnérabilités des systèmes.

Aujourd'hui, le cyberespace n'a pas de frontière, les effets de bord ne sont pas à sous-estimer et une protection harmonisée est donc souhaitable. Tel le nuage de Tchernobyl, il ne faut pas croire que les attaques informatiques seront cantonnées à certains pays à travers l'Europe.

Le numérique est un enjeu stratégique pour la Belgique et pour l'Europe. L'ambition européenne est forte et exigeante. Nous devons être à la hauteur.

Mots-clés : cybersécurité, CyberLab, compétences humaines, entraînements, simulations ultraréalistes, tests de résistance, souveraineté, protection du secret, partenaires de confiance, maîtrise technique de bout en bout