S'unir pour la cybersécurité des infrastructures industrielles

par

Laurent Hausermann
Directeur général de Sentryo, entreprise membre de Hexatrust

En bref

En juin 2014, Laurent Hausermann et Thierry Rouquet créent Sentryo, pionnier du domaine de la cybersécurité de l'Internet industriel. Les risques que représentent la cybercriminalité sont encore trop peu connus. Ils engendrent pourtant des pertes financières déjà considérables et ceux qui visent des systèmes industriels pourraient avoir des conséquences dramatiques sur l'économie, la santé publique ou encore l'environnement. À l'heure de l'Industrie du Futur et du déploiement d'applications d'analyse de données, Sentryo permet aux entreprises de l'énergie, du transport, de l'industrie manufacturière ou aux infrastructures publiques de maintenir l'intégrité de leurs réseaux de contrôle, de détecter les comportements malicieux et d'assurer la continuité de leurs opérations. Pour faire face à une concurrence internationale très vive, Sentryo a adopté une stratégie d'emblée européenne et compte déjà plusieurs entreprises allemandes parmi ses clients. Elle cherche maintenant de nouveaux investisseurs pour poursuivre son internationalisation.

Compte rendu rédigé par Élisabeth Bourguinat

Le séminaire Management de l'innovation est organisé avec le soutien de la Direction générale des entreprises (ministère de l'Économie et des Finances) et grâce aux parrains de l'École de Paris (liste au 1er septembre 2018) :

Algoé [1] • Caisse des dépôts et consignations • Carewan [1] • Conseil régional d'Île-de-France • Danone • EDF • Else & Bang • ENGIE • FABERNOVEL • Fondation Roger Godino • Groupe BPCE • Groupe OCP • GRTgaz • HRA Pharma [2] • IdVectoR [2] • IPAG Business School • La Fabrique de l'industrie • Mairie de Paris • MINES ParisTech • Ministère de l'Économie et des Finances – DGE • Renault-Nissan Consulting • RATP • SNCF • Thales • UIMM • Ylios [1]

1. pour le séminaire Vie des affaires
2. pour le séminaire Ressources technologiques et innovation

Après avoir débuté ma carrière chez EADS, j'ai travaillé entre 2003 et 2013 chez Arkoon Network Security, un des leaders européens de solutions de sécurité des systèmes d'information, dont les clients sont de grands groupes comme Total ou Michelin, ou encore le ministère de la Défense. J'étais le directeur technique de cette société et Thierry Rouquet, mon associé actuel, en était le président. Nous l'avons cédée en 2013 à la branche Défense du groupe Airbus et nous sommes restés dans l'entreprise pendant un an, pour assurer la transmission aux nouvelles équipes.

La création de Sentryo

En 2014, nous avons quitté Airbus pour créer notre propre entreprise, Sentryo. Nous n'avions aucune animosité vis-à-vis d'Airbus, qui est l'un de nos clients aujourd'hui, mais notre profil est plutôt celui d'entrepreneurs que de cadres dans un grand groupe. De plus, nous avons changé d'objet : Arkoon proposait des systèmes de sécurité pour les réseaux informatiques classiques, tandis que Sentryo se concentre sur la sécurité des réseaux dans l'industrie. Notre projet est d'aider les organisations industrielles à améliorer la continuité de leurs opérations, la résilience de leurs activités industrielles et la sûreté du fonctionnement de leurs systèmes, à un moment où elles sont en train de se digitaliser et de s'exposer, de ce fait, à un plus grand nombre d'attaques.

Thierry Rouquet est président de Sentryo et j'en suis le directeur général. Rapidement, Romain Françoise a rejoint notre équipe pour prendre la direction de la technologie. Nous sommes basés à Lyon et employons vingt-cinq personnes. Parmi nos clients figurent des entreprises des secteurs de l'énergie, de la défense, des *process* industriels, du *manufacturing* et des transports, notamment ferroviaire. Nous nous sommes dotés de bureaux en Allemagne et en Amérique du Nord, et nous avons signé des partenariats de distribution avec des groupes comme Vinci Energies, Siemens ou Schneider Electric pour apporter des services à leurs clients autour de nos produits, notamment aux États-Unis, en Amérique latine, en Asie du Sud ou au Moyen-Orient.

La cybersécurité dans les systèmes industriels

Pour parler de cybersécurité dans les systèmes industriels, on utilise deux acronymes, l'OT et l'IIoT. La notion d'OT (*Operational Technology*) a été définie par opposition à l'IT (*Information technology*). Cette dernière désigne l'informatique classique telle qu'elle s'est développée depuis quatre-vingts ans, alors que l'OT renvoie à tous les systèmes assurant des interactions entre l'informatique et le monde physique (usines, production d'énergie, etc.). L'IIoT (*Industrial Internet of Things*) recouvre tous les objets industriels connectés, par exemple les tramways autonomes, les réseaux électriques intelligents ou encore le *smart manufacturing*, qui permet de connecter les usines et de fabriquer des petites séries.

Dans le monde de l'IT, la cybersécurité consiste à protéger les entreprises contre le vol de données personnelles, qui peut entraîner des pertes financières. Dans le monde de l'OT et de l'IIoT, l'impact est très différent, car les hackers s'en prennent à la disponibilité ou à l'intégrité d'ordinateurs ou d'équipements qui pilotent des équipements physiques et que l'on appelle des ICS (*Industrial Control System*, ou systèmes numériques de contrôle-commande). Or, les ICS sont présents dans de nombreux secteurs (énergie, extraction pétrolière, transports, infrastructures urbaines, industrie…) et servent souvent à piloter des systèmes critiques. Si quelqu'un modifie le taux de chlore dans un château d'eau, par exemple, c'est la santé des citoyens qui peut être atteinte. S'il perturbe les mouvements d'un robot dans une usine, des salariés peuvent être blessés. S'il ouvre certaines vannes dans une raffinerie, la rivière voisine pourra être polluée.

Il y a quelque temps, une entreprise qui venait d'achever la construction d'un stade a expliqué dans la presse qu'un grand nombre des fonctions de cet équipement (éclairage, détection incendie, portiques de sécurité,

climatisation, chauffage…) étaient pilotées de façon entièrement numérique, à partir de tablettes connectées par wifi. Pour valoriser ses savoir-faire, elle fournissait même quelques schémas du dispositif… On imagine ce qui arriverait si, lors d'un match réunissant 50 000 spectateurs, une personne malveillante éteignait toutes les lumières, fermait les portes et déclenchait l'alarme incendie. J'ai cité cet exemple à l'occasion d'une conférence et un gendarme qui était présent dans l'assistance m'a demandé : « *Pouvez-vous m'envoyer le plus vite possible une note à ce sujet ?* » J'espère que, depuis, ces informations ont disparu d'Internet.

Non seulement les attaques contre les OT et les IIoT peuvent être beaucoup plus graves que celles visant les IT, mais elles peuvent engager la responsabilité pénale des dirigeants et pas seulement le portefeuille de l'entreprise.

Plusieurs sortes d'attaques

Les attaques contre les activités industrielles peuvent prendre plusieurs formes.

Détruire les capacités de production

L'attaquant peut chercher à saboter un procédé de façon invisible afin de détruire les capacités de production, ou même l'ensemble du système. En Iran, en 2009, les services secrets américains et israéliens ont fait en sorte de dérégler les centrifugeuses qui servent à enrichir le combustible nucléaire en faisant passer son taux d'uranium de 4 à 97 %. L'intervention consistait à faire accélérer ou ralentir ces appareils de façon imperceptible, ce qui provoquait leur vieillissement prématuré. D'après l'Agence internationale de l'énergie atomique, cette attaque a conduit à remplacer un millier de centrifugeuses, ce qui a retardé de deux ans le programme nucléaire iranien. Cela se passait avant les négociations internationales.

Interrompre la production

L'attaquant peut aussi se contenter d'interrompre la production, ce qui peut représenter des pertes financières importantes. L'un de nos clients exploite des FPSO (*Floating production storage and offloading*), c'est-à-dire des plateformes mobiles permettant de produire, stocker et décharger le pétrole. Chacun de ses bâtiments transporte chaque jour l'équivalent de 20 millions de dollars…

Autre exemple, le virus WannaCry, qui chiffrait les données contenues dans les ordinateurs et exigeait une rançon pour les déverrouiller, a obligé Renault à interrompre sa production pendant quinze jours sur des usines de Douai et en Angleterre. Touché par la même attaque, Saint-Gobain a évalué ses pertes à 250 millions d'euros, le transporteur maritime danois Maersk, à 200 millions de dollars et l'on estime les pertes de Merck, le laboratoire pharmaceutique américain, à plus de 400 millions de dollars.

Déstabiliser un pays

L'interruption de la production peut aussi avoir des objectifs tout autres que financiers. En 2015, juste avant Noël, 225 000 foyers de l'est de l'Ukraine ont été privés de courant pendant sept heures. Il est difficile d'identifier avec certitude l'auteur d'une attaque, mais en l'occurrence, il s'agissait probablement d'une opération de déstabilisation menée par le gouvernement russe. L'essentiel de l'attaque a consisté à s'assurer que les opérateurs ukrainiens ne puissent pas remettre le courant.

Les attaques contre les véhicules

Parmi les différents sujets sur lesquels nous travaillons, nous nous sommes particulièrement intéressés aux attaques concernant les véhicules. Le programme Windows 7 comprend 40 millions de lignes de code ; Ubuntu Linux, 60 millions ; Max OSX Tiger, 80 millions ; le programme d'une voiture, 120 millions. Au cours de la seule année 2015, les propriétaires des trois premiers logiciels ont identifié respectivement 147, 172 et 417 failles dans leurs programmes. Renault, PSA, BMW ou General Motors n'ont jamais fait d'annonce de ce genre, mais on imagine que leurs programmes comportent bon nombre de failles également. La prise de conscience doit être plus forte. La menace se précise : des hackers ont publié une vidéo où ils montrent comment prendre

le contrôle d'une voiture à partir de son système de parking automatisé. À la suite d'une démonstration de ce type, Chrysler a dû rappeler 1,4 million de véhicules…

Des armes réutilisables à l'infini

Il existe une grande différence entre un missile et un *malware* (logiciel malveillant). Une fois qu'un missile a été utilisé, il est par principe entièrement détruit. En revanche, un *malware* peut être recopié à l'infini.

Dans le cadre de l'ISA (Association internationale de l'automatisme), nous avons participé à l'étude sur l'affaire ukrainienne et nous avons été frappés de constater que le programme en question avait été configuré de façon à pouvoir être réutilisé contre n'importe quelle sorte de réseau électrique, même ancien, partout dans le monde.

De même, l'enquête sur WannaCry a montré qu'un élément du programme avait été volé deux mois plus tôt à la NSA (*National Security Agency*). En quelques semaines, un outil élaboré par les services de renseignements américains avait été mis au service d'une activité criminelle.

Sentryo ICS CyberVision

Il existe deux grandes façons de se protéger des cyberattaques : soit ériger des murs et des portes pour empêcher les intrusions ; soit se doter d'outils permettant de détecter les attaques et de donner l'alerte. Sentryo s'est positionnée plutôt sur cette deuxième approche.

Notre plateforme ICS CyberVision comprend un réseau de capteurs et un logiciel central de visualisation et d'analyse des données, qui peut être positionné à l'intérieur du site industriel ou ailleurs, par exemple lorsqu'il s'agit de surveiller un réseau électrique, un pipeline ou un parc d'éoliennes.

Quand nous installons notre solution, nous faisons toujours des découvertes intéressantes : des systèmes censés être débranchés qui ne le sont pas, un sous-traitant avec lequel l'entreprise n'a plus de contrat mais qui est encore connecté à l'usine… Notre intervention commence par une simple opération d'hygiène consistant à fermer toutes les portes qui ont été laissées ouvertes par inadvertance.

Ensuite, démarre la surveillance proprement dite, afin de détecter des anomalies. Une machine est en principe programmée pour effectuer chaque jour la même opération (lire telle variable, consulter telle liste, etc.). Chaque écart par rapport au programme doit attirer l'attention, ainsi que chaque message cherchant à le modifier.

Cette surveillance s'exerce de façon complètement non intrusive, un peu à la façon d'une caméra placée dans une pièce pour détecter les mouvements. L'enjeu est de pouvoir déployer notre technologie sans avoir besoin d'apporter de modification au système, ce qui représente notre principal atout par rapport à nos concurrents.

Notre deuxième atout est le fait que notre outil est accessible même à des non spécialistes. Nos efforts ont porté tout particulièrement sur la visualisation des résultats : moyennant une petite formation, tout opérateur industriel ou automaticien peut comprendre qu'une anomalie a été détectée et savoir ce qu'il doit faire.

Les innovations de Sentryo

Nous avons commencé par investir assez lourdement, pendant deux ans, dans des technologies dites de surveillance protocolaire (*Deep Packet Inspection*) pour permettre à notre logiciel de comprendre l'intégralité des messages circulant sur un réseau donné, un peu comme s'il devait apprendre toutes les langues du monde. Par exemple, si dans le champ 125 d'un message figure le chiffre 2 ou le chiffre 3, le logiciel doit savoir que 2 signifie « *démarre* » et 3, « *arrête-toi* ». Nous avons également travaillé sur de premières visualisations des données collectées.

Au bout de deux ans, nous nous sommes associés à deux programmes de R&D soutenus par l'État. Le premier, TIAKI, est financé par la DGA (Direction générale de l'armement) dans le cadre du dispositif RAPID (régime d'appui pour l'innovation duale), destiné à soutenir les innovations susceptibles de trouver des applications

à la fois sur les marchés militaires et civils. Le programme TIAKI, sur lequel nous travaillons en collaboration avec la division Énergie nucléaire du CEA (Commissariat à l'énergie atomique et aux énergies alternatives), nous a permis de créer des algorithmes de détection et de suivi de nouveaux types d'attaques à partir de techniques d'intelligence artificielle. Cet investissement en R&D représente 1 million d'euros.

Le deuxième programme, baptisé PUNGA, est financé par Bpifrance dans le cadre du Concours mondial de l'innovation, destiné à soutenir des programmes de R&D très amont. Il nous a permis de travailler sur la surveillance du bus de données CAN (*Control Area Network*), utilisé dans les automobiles pour transmettre des messages d'une dizaine d'octets destinés à déclencher des actions sur les organes de la voiture (lire la vitesse, demander au coffre de s'ouvrir, etc.). Nous sommes actuellement en phase d'industrialisation d'un système de surveillance qui viendra s'insérer à l'intérieur du véhicule, avec une contrainte de taille : l'ensemble du dispositif, y compris la puce qui fait tourner l'algorithme, ne doit pas coûter plus de 5 euros…

Nos différentes innovations nous ont valu plusieurs prix, que ce soit au sein de la communauté de la cybersécurité (le Prix de l'Innovation des Assises de la sécurité et des systèmes d'information de Monaco, en octobre 2015) ou dans le cadre de concours organisés par de grandes entreprises comme Cisco (*Acceleration Prize*, en juin 2016) ou BMW (Tech Date, en juin 2016).

La concurrence

Nous sommes confrontés à une concurrence très vive, essentiellement aux États-Unis et en Israël. Depuis les années quatre-vingts, des entrepreneurs israéliens développent des start-up qu'ils revendent souvent pour des montants de plusieurs dizaines ou centaines de millions d'euros. La plupart d'entre eux réinvestissent ces sommes dans de nouvelles start-up, d'autant plus que le système fiscal les y incite. C'est également le cas en Californie, où un entrepreneur qui réinvestit son argent sur des sociétés successives ne paiera de taxes que sur la dernière de ses sociétés, lorsqu'il la vendra pour prendre sa retraite. Dans ce contexte, les start-up bénéficient de financements colossaux.

La société israélienne Claroty, notre principale concurrente, a été créée aux États-Unis la même année que Sentryo. Elle compte 60 salariés et a déjà levé 100 millions de dollars. Cet argent est utilisé, entre autres, pour la R&D, mais ce n'est pas là que se fait la différence, car nos technologies sont de niveaux comparables. Les fonds dont dispose Claroty lui servent surtout à embaucher des dizaines de commerciaux pour aller "prendre des parts de cerveaux" partout dans le monde. Ces sociétés développent une stratégie marketing agressive et sont très présentes dans les cercles professionnels (événements, salons, conférences).

Ces sommes peuvent aussi représenter un handicap : lorsque des investisseurs misent 15 millions de dollars sur une start-up, cela signifie qu'ils estiment sa valeur à 60 millions de dollars et escomptent qu'ils pourront la vendre 150 ou 200 millions de dollars dans un délai de cinq ans. Une telle valorisation correspond à un chiffre d'affaires d'environ 50 millions de dollars, dans un secteur où les cycles de vente sont particulièrement longs. La pression sur les entreprises est donc forte.

Il n'en reste pas moins que de telles opérations ont lieu : Continental vient, par exemple, de racheter pour 400 millions de dollars une société israélienne, Argus, qui emploie une soixantaine de personnes et développe le même genre de logiciel que nous sur le bus CAN.

Une stratégie d'emblée européenne

Compte tenu de ce contexte, nous avons compris qu'il était indispensable de construire d'emblée une entreprise européenne afin de disposer d'un marché de taille suffisante pour soutenir les investissements nécessaires.

Nous avons commencé par l'Allemagne, sachant que son industrie est quatre à cinq fois plus puissante que l'industrie française, avec un marché très structuré (associations professionnelles, salons…) et de grands acteurs qui ont une vision de long terme grâce au programme Industrie 4.0. Nous travaillons aujourd'hui avec Siemens, ou encore BMW.

Un cycle de vente long

Notre marché se caractérise par un cycle de vente très long et, même si nous avons quelques clients prestigieux, ils commencent toujours par de petites commandes. J'adorerais que les grands groupes industriels français nous signent un contrat de 3 millions d'euros pour équiper tous leurs sites, mais ce n'est pas ainsi que les choses se passent. Nous commençons toujours par un premier essai à quelques dizaines de milliers d'euros, puis nous équipons un premier site et, si tout se passe bien, il nous faudra six ou sept ans pour déployer notre produit dans l'ensemble des sites partout dans le monde. Or, les fonds d'investissement ont une durée de vie de dix ans au maximum, dont quatre à six ans d'investissement et quatre à six ans de désinvestissement. Autant cela fonctionne bien pour les entreprises du Web, qui peuvent décoller ou échouer en quelques années, autant c'est compliqué pour une entreprise avec un cycle de vente aussi long que le nôtre, lié à l'industrie.

Le défi est d'autant plus rude que les grandes entreprises ne jouent pas forcément toujours leur rôle. Souvent, notre interlocuteur raisonne à une trop grande échelle : « *Pour pouvoir défendre ce dossier, je vais devoir présenter un scénario à ma hiérarchie où nous installerions cet outil partout en trois ans.* » Or, les start-up comme la nôtre ont plutôt besoin d'expérimenter leur technologie sur un périmètre restreint et pour une durée courte, mais le plus vite possible…

Si chacun des grands comptes avec lesquels nous travaillons misait 100 000 euros pour créer des sites pilotes, nous avancerions beaucoup plus vite et nous pourrions nous présenter devant les investisseurs pour trouver les sommes dont nous avons besoin pour nous internationaliser. Pour le moment, les contrats sont plutôt de l'ordre de 20 000 euros que de 100 000, ce qui n'est pas suffisant pour nous rendre crédibles.

Hexatrust

Hexatrust est un club d'entreprises qui a été créé en 2013 par un groupe de PME et d'ETI françaises des domaines de la sécurité des systèmes d'information, de la cybersécurité et de la confiance numérique, avec pour objectif de pouvoir proposer aux industriels un ensemble complet de services. Par exemple, Sentryo est spécialisée dans la surveillance, alors que Seclab, société basée à Montpellier, propose des systèmes de protection permettant d'isoler un réseau industriel du reste de l'entreprise, grâce à une technologie de filtrage très avancée. Désormais, quand nous rendons visite à un prospect, nous y allons à plusieurs, pour lui montrer que sa problématique peut être abordée sous différents angles et que nous pouvons y apporter une réponse complète.

Hexatrust comprend une cinquantaine d'entreprises qui emploient au total 2 500 salariés, pour un chiffre d'affaires de 400 millions d'euros. Elles réalisent en moyenne 30 % de leurs ventes à l'export, ce qui est encore beaucoup trop faible, et réinvestissent 30 % de leur chiffre d'affaires dans la R&D, ce qui est considérable.

Nous organisons tous les ans une université d'été, mais également des événements sur le *cloud*, du *networking*, des conférences, etc. Notre association nous permet aussi de disposer d'une plus grande visibilité sur les salons. En principe, une PME de trente personnes doit se contenter d'un petit stand tout au fond du salon, près des toilettes, où personne n'ira la voir. Cette année, sur le FIC (Forum international de la cybersécurité) de Lille, le "village Hexatrust" était le premier exposant du point de vue de la taille : notre stand rivalisait avec ceux d'Orange, de Thales ou d'Airbus, ce qui nous a valu la visite des ministres et des délégations étrangères.

Enfin, Hexatrust travaille avec l'ANSSI (Agence gouvernementale de la sécurité des systèmes d'information), qui est rattachée au Premier ministre, mais aussi avec le label France Cybersecurity, une sorte d'AOC de promotion du savoir-faire français en cybersécurité, avec la French Tech et Enfin Cyber, réseau informel des pôles de compétitivité relevant de ce domaine.

La politique de l'autruche

Un intervenant : *Les risques colossaux que représente la cybercriminalité sont identifiés depuis longtemps, mais tout le monde fait l'autruche. Sachant que Microsoft déconseille formellement l'usage de son système d'exploitation Windows XP depuis dix ans, la police londonienne vient enfin d'y renoncer… pour adopter Windows Vista !*

Autre exemple, il existe encore des gens pour promouvoir le vote électronique, alors qu'il est parfaitement impossible de le sécuriser.

Quant aux constructeurs automobiles, ils s'opposent depuis des années à toute forme de certification en matière de sûreté et de sécurité, car un code certifié peut coûter jusqu'à cent fois plus cher qu'un code non certifié.

Laurent Hausermann : Tant que l'on n'a pas été victime d'un cambriolage, on croit que cela n'arrive qu'aux autres. La prise de conscience est plus forte en Asie ou aux États-Unis que chez nous. Quand je fais une conférence sur la cybersécurité, je perçois toujours des petits sourires entendus (« *Naturellement, il force le trait…* »). Il faudrait que le mouvement vienne d'en haut. Aux États-Unis, le président Obama faisait chaque année un discours d'une heure sur cette question.

La culture du secret

Int. : *Les entreprises qui ont été victimes de cyberattaques ne pourraient-elles participer à l'effort de pédagogie ?*

L. H. : Autant les attaquants se partagent les informations sur des forums, autant les victimes font preuve de pudeur… Même les assureurs ont du mal à recueillir des données pour leurs statistiques. Quant à l'État, il ne voit cette question que sous l'angle de la défense nationale et ne publie pas de statistiques.

Les Anglo-Saxons ont une approche très différente. Aux États-Unis, par exemple, la loi prévoit que lorsque des industriels d'un même secteur se partagent des informations sur les cyberattaques dont ils font l'objet, ce n'est pas considéré comme relevant d'une pratique anticoncurrentielle.

Int. : *Cette culture du secret est d'autant plus déplorable que, pour un hacker, le secret, c'est le bonheur, tout simplement parce que ce qui est secret est généralement mal protégé. Au cours d'une expertise sur le logiciel d'arrêt des centrales nucléaires, j'ai demandé à vérifier les fonctions de sécurité du logiciel, et on m'a répondu :* « Certainement pas ! Vous n'avez pas le droit de regarder ça. »

L. H. : Auguste Kerckhoffs a pourtant démontré dès la fin du XIX^{e} siècle que la sécurité par le secret ne fonctionne pas. Un algorithme de chiffrement doit être rendu public afin que la communauté scientifique puisse vérifier s'il est fiable. Seule la clé doit rester confidentielle.

Prévenir ou guérir ?

Int. : *Votre approche consiste à surveiller les flux de données, sans vous préoccuper des faiblesses de l'architecture sous-jacente. Cependant, si le système présente une faille et que vous décelez une attaque, ne sera-t-il pas déjà trop tard ?*

L. H. : Même après avoir posé une porte blindée à l'entrée de sa maison, il peut être utile de savoir que quelqu'un est en train de gratter et d'essayer de l'ouvrir !

Int. : *Mais si vous détectez un problème, votre client a-t-il la possibilité d'y répondre dans un délai suffisamment bref ?*

L. H. : La quasi-totalité des attaques se déroulent sur plusieurs mois. Par exemple, un hacker commencera par envoyer un CV piégé à une assistante du service des ressources humaines. Comme le travail de cette dernière

consiste à réceptionner les CV, elle l'ouvre sans méfiance. L'attaquant prend alors le contrôle de son ordinateur et procède à ce qu'on appelle des "déplacements latéraux" au sein du réseau, d'ordinateur en ordinateur, jusqu'à parvenir à ce qui l'intéresse, par exemple un ICS à l'intérieur de l'usine. C'est alors seulement qu'il va commencer à déployer ses actions malveillantes. Les attaques qui ont été documentées ont mis, en moyenne, entre trois et six mois pour aboutir.

Le délai pour réagir ne se compte donc pas en minutes, ni même en jours. Si, chaque semaine, l'opérateur applique une procédure d'hygiène consistant à examiner toutes les alertes lancées par un outil comme le nôtre, ce sera suffisant pour parer les attaques, ne serait-ce qu'en débranchant du réseau l'ordinateur infecté jusqu'à ce que le problème ait pu être traité.

Int. : *Pourquoi votre logiciel ne bloque-t-il pas lui-même le système dès qu'il détecte une anomalie ?*

L. H. : On est rarement complètement sûr d'avoir affaire à une attaque. Quand un mail est traité à tort comme un spam, c'est agaçant, mais ce n'est pas très grave. Si une centrale électrique est arrêtée par erreur, c'est beaucoup plus ennuyeux. C'est pourquoi nous nous contentons de fournir toutes les informations sur les anomalies tout en nous gardant bien de programmer des décisions de coupure automatique.

La protection du système de protection

Int. : *Votre dispositif de surveillance ne pourrait-il être hacké lui-même ?*

L. H. : La première chose que fait un cambrioleur, c'est effectivement de débrancher la caméra de surveillance… Nous travaillons sur ce sujet avec l'ANSSI et nous avons intégré à nos produits des fonctions de sécurité qui cantonnent les différentes parties de nos programmes. Par ailleurs, nous faisons appel à des évaluateurs indépendants pour tester nos propres produits du point de vue de la sécurité.

Le recrutement

Int. : *Les informaticiens que vous employez ne doivent pas avoir des profils très ordinaires. Comment les recrutez-vous ?*

L. H. : C'est un vrai problème. L'an dernier, pour un poste de responsable marketing, j'ai reçu 250 CV. Quand je cherche un ingénieur en R&D, j'en reçois entre 5 et 10. Les gens ont malheureusement une image assez négative de ce métier, qu'ils jugent compliqué, technique et pas passionnant… En général, nous cherchons des personnes ayant un fort potentiel et nous nous chargeons de les former.

Int. : *Cela vous arrive-t-il de recruter des hackers repentis ?*

L. H. : Cela nous arrive.

Le choix de la France

Int. : *Pourquoi avez-vous choisi de rester en France plutôt que d'émigrer à San Francisco comme tant de vos collègues ?*

L. H. : Tout simplement parce que j'ai de fortes convictions sur la France et sur l'Europe. J'avoue d'ailleurs avoir du mal à comprendre la tendance actuelle qui consiste à dépenser l'argent du contribuable pour des start-up françaises qui se développeront aux États-Unis plutôt que sur le marché européen. Une fois là-bas, elles se font racheter par un investisseur américain, elles installent leur siège social dans le Delaware et c'est fini.

Identifier les attaquants ?

Int. : *Votre outil permet-il d'identifier les attaquants ?*

L. H. : L'attribution des attaques est un sujet très compliqué. Certains essaient de traquer des signaux faibles à l'intérieur des logiciels malveillants. Par exemple, ils trouvent quelques mots en russe au milieu du code et en concluent que le logiciel vient de Russie. Mais des Chinois peuvent très bien avoir mis à dessein des mots en russe pour brouiller les pistes…

Les articles publiés par les experts montrent que le secteur du hacking est très organisé, avec des spécialistes pour chaque brique : les uns se chargent de prendre le contrôle des ordinateurs, les autres de passer d'un ordinateur à l'autre, d'autres encore de vendre ces briques sur Internet. Nous avons cherché à savoir combien coûte le lancement d'une attaque : pour 35 000 à 40 000 euros, vous pouvez trouver sur des forums russes tout ce dont vous avez besoin. L'attribution d'une attaque nécessite de cartographier tous ces acteurs et de comprendre quelles relations ils entretiennent. Cela relève des techniques du renseignement, ni plus ni moins.

Présentation de l'orateur

Laurent Hausermann : Cofondateur et directeur général de Sentryo. Il a exercé différentes responsabilités managériales et techniques dans des entreprises de *Deep Tech*. Il a été le CTO (*Chief Technical Officer*) d'Arkoon Network Security où il a dirigé une équipe de plusieurs dizaines d'ingénieurs dans des projets de R&D ambitieux. Il enseigne à l'École des mines et édite le blog En Route pour l'Innovation. Il est un inconditionnel de la philosophie *Lean Startup*.

Diffusion septembre 2018