JANVIER 2021

DE LA MÉTHODOLOGIE AUX RETOURS D'EXPÉRIENCES

Comment instaurer une cyberculture au sein de votre organisation ?

Infoprotection, un média Expoprotection.
www.infoprotection.fr

Sommaire

Introduction

Cybermenaces : on n'a encore rien vu p. 3

01 Cybersécurité :
une culture à insuffler à tous les étages p. 6

02 Security by Design :
les règles à suivre pour les équipements connectés p. 10

03 Cyberattaques :
retours d'expériences p. 13

Intro

Cybermenaces : on n'a encore rien vu

Places de marché électroniques dédiées aux outils de cyberattaque, prestataires d'attaque, botnets massifs et intelligence artificielle… À mesure que les entreprises se digitalisent, leurs vulnérabilités augmentent.

Dans un rapport du Centre d'études stratégiques et internationales (CSIS) daté de début décembre 2020 pour le compte de l'éditeur de logiciels de cybersécurité McAfee, les pertes mondiales dues à la cybercriminalité s'élèvent à plus de 1 000 milliards de dollars pour l'année 2019. Soit 1 % du PIB mondial. Qui plus est, elles sont en augmentation de plus de 50 % par rapport à 2018. Deux tiers des entreprises interrogées par le CSIS ont signalé un type de cyberattaque au cours de l'année 2019. Parmi les attaques les plus répandues, le rançongiciel (Ransomware) vient en tête. Dans son étude de mai 2020, l'éditeur de logiciels de cybersécurité Sophos indique que 51 % des 5 000 entreprises interrogées dans 26 pays en avaient été victimes durant l'année écoulée. Pour sa part, LexisNexis Solutions remarque que le taux d'attaque mobile a augmenté de 56 % alors que le taux d'attaque sur PC a chuté de 23 %, confirmant ainsi la croissance vers la fraude mobile.

Des outils pour les pirates

Dans le monde, combien sont les cyberpirates ? Des dizaines, des centaines de milliers, des millions ? Difficile à dire. Mais leur nombre augmente à mesure que se démocratisent les outils de piratage sur près d'une vingtaine de places de marché électroniques dans le Dark Web. Outre les logiciels malveillants, il est de plus en plus facile d'acheter ou vendre non seulement des numéros de cartes bancaires, des données personnelles complètes, des accès frauduleux à des systèmes d'information, des failles Zero Day mais aussi des prestations de « Pirate as a Service ». *« Nous installons des Honey Pots, des machines faites pour attirer les pirates. En une semaine, on enregistre jusqu'à 125 000 attaques »,* confie le hacker éthique Gaël Musquet.

Des attaquants de bas étage mieux armés

Déjà, les cyberattaquants de bas étage exploitent les nombreuses failles inhérentes à tout logiciel pour lancer très facilement des campagnes virales massives sur des applications largement utilisées. Comme Prestashop (boutique électronique) ainsi que WordPress ou Joomla (publication de contenus). D'où l'intérêt d'installer les mises à jour régulières de ces logiciels. A côté de cela, il suffit de saisir certaines requêtes sur Google pour entrer sans difficulté dans des groupes Whatsapp et aspirer des données personnelles sensibles. Du simple bricolage. *« On peut ainsi traquer des personnalités politiques ou des chefs d'entreprise dans des groupes X ou gay et les faire chanter »*, explique le hacker éthique Clément Domingo, alias SaxX.

De plus en plus de botnets pour les cyberattaques avec la 5G

Depuis quelques années, les botnets se développent. Ces réseaux de milliers, voire de millions de machines ou objets connectés pilotés à distance sont utilisés par les pirates pour lancer des cyberattaques. Leur usage va devenir exponentiel. Il n'y a qu'à consulter le site Shodan.io pour découvrir quels sont les modèles d'objets connectés (frigos, caméras, usines électriques…) non sécurisés. Et avec la 5G, ce phénomène ne fera que s'amplifier. Avantage de la 5G, pour les cyberpirates, plus besoin de se connecter avec un câble pour pénétrer les réseaux. D'autant qu'avec une capacité d'absorption d'un million d'équipements par km², la 5G promet une prolifération incontrôlée des objets connectés. En outre, rien ne garantit pour l'heure que ces objets seront développés en Security By Design. Pour mémoire, ce sont des caméras chinoises de vidéosurveillance qui sont à l'origine du terrible botnet Mirai. L'autre menace de la 5G porte sur la souveraineté des infrastructures de télécommunication. Pointé du doigt, l'équipementier chinois Huawei a fait, en France, l'objet d'une loi dite « Loi Huawei » qui impose à chaque réseau 5G d'obtenir une certification validée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Botnets multi-fonctions

Démantelé en août 2019, le Botnet Retadup a ainsi fédéré plus de 850 000 machines dans le monde. Après les attaques en déni de service distribué (DdoS), de telles puissances de calcul servent aujourd'hui à plusieurs tâches : casser des mots de passe en Brute Force, miner des cryptomonnaies comme le Monero ou injecter des virus comme les cryptolockers. *« Le Botnet qui se contente de paralyser un site, c'est fini. Sa capacité à cartographier les failles est redoutable,* remarque Gaël Musquet. *Souvent les cibles sont observées pendant des semaines ou des mois. Et comme le botnet est international, il offre une furtivité incomparable pour localiser et suivre des cibles. »*

IA offensive

Après la puissance de calcul gratuite des Botnets, l'espionnage industriel prend une nouvelle dimension. *« À l'instar des entreprises, les malfaiteurs accèdent aux publications scientifiques en matière d'Intelligence artificielle (IA). Ils infiltrent une entreprise, récupèrent des océans de données, les recoupent avec de l'IA offensive pour essayer de faire parler la data et trouver le meilleur retour sur investissement : vendre la donnée à un concurrent, faire chanter l'entreprise, vendre l'accès à son système d'information compromis, reprend SaxX. Il ne leur en faut pas plus pour avoir une bonne longueur d'avance. La menace est de grande ampleur et on n'a encore rien vu. »*

Une chose est sûre : chaque entreprise est, plus que jamais, susceptible de subir toute une variété de cyberattaques. Pour s'en prémunir, il faut développer une culture de la cyberprévention à tous les étages (y compris celui de la direction générale), mettre en place les outils de la cybersécurité et instaurer une démarche de sécurité dès la conception des nouvelles applications. Sans oublier, bien sûr, d'organiser des plans de sauvegarde, base de la reprise et de continuité d'activité.

01

Cybersécurité : une culture à insuffler à tous les étages

En matière de sécurité informatique, le processus d'acculturation est multiple et complexe. Il ne suffit pas d'investir dans les technologies de cybersécurité pour être à l'abri. Il apparaît nécessaire de miser sur les organisations, les processus et les managers de proximité. Quitte à organiser des exercices de cybercrise, et à utiliser les mêmes outils que les pirates.

Faux sites de vente de masques chirurgicaux, attaque au faux président, rançongiciels… Les pirates du monde entier ont profité de la brèche du coronavirus pour intensifier la propagation de leurs infections. En effet, le confinement a contraint de nombreuses entreprises à mettre précipitamment leurs salariés au télétravail. *« La cybermalveillance est le revers de la digitalisation. Les modes de piratage sont proportionnels à ce que les entreprises ont exposé sur Internet pour dépasser leurs concurrents »*, soulève Alain Bouillé, président du Club des experts de la sécurité de l'information et du numérique (Cesin). Au-delà des indispensables outils de protection, la cybersécurité repose avant tout sur l'humain. Facile à dire, car sensibiliser ses équipes aux cyber-risques ne se limite pas à l'application de quelques règles élémentaires. L'enjeu consiste surtout à instiller une véritable culture de la cybersécurité au sein de l'organisation.

Les entreprises pas si mal loties en période normale

Bonne nouvelle, les entreprises ne sont pas si mal équipées, selon le baromètre 2020 de la cybersécurité du Cesin. D'ailleurs, 39 % d'entre elles sont prêtes à affronter de fortes cyberattaques. Avec une douzaine de solutions installées, elles se protègent mieux. Pour 83 % des sociétés interrogées, ces solutions sont même jugées adaptées aux besoins. Par ailleurs, quatre entreprises sur dix choisissent de faire appel à des solutions innovantes ou proposées par des start-up. Les autres invoquent le manque de maturité de ces solutions. Qui plus est, 91 % des entreprises instaurent un programme de cyber-résilience ou envisagent de le faire, contre 79 % l'année dernière. De même, elles sont plus nombreuses à avoir souscrit une cyberassurance (60 % en 2020 contre 50 % en 2019).

Des salariés sensibilisés aux cyber-risques mais pas forcément impliqués

Revers de la médaille, il ne suffit pas d'investir dans des solutions technologiques de cybersécurité pour que l'entreprise soit protégée. D'ailleurs, dans l'étude du Cesin, 98 % des usages numériques réalisés par les salariés présentent des risques. C'est ce qu'on appelle le Shadow IT, à savoir les applications, notamment les applications Cloud (Software as a Service) mises en œuvre au sein de l'entreprise sans la connaissance ou l'approbation de la direction des systèmes d'information (DSI). D'après les Responsables de la sécurité des systèmes d'information (RSSI), 74 % des salariés sont pourtant sensibilisés aux cyber-risques. Cependant, visiblement, ils manquent d'implication. Pour preuve, ils sont seulement la moitié à respecter les

recommandations de cybersécurité. Pour enrayer ce phénomène, 77 % des entreprises instaurent des procédures pour tester l'application des recommandations par les salariés, comme l'envoi de faux mail de pirates.

L'humain, maillon faible

« En matière de cybersécurité, l'humain est le principal point de vulnérabilité, estime dans son blog Franck Nielacny, directeur des systèmes d'information chez Stormshield, spécialiste de sécurité des infrastructures digitales (filiale d'Airbus CyberSecurity), que ce soit par accident (erreur, non-respect ou oubli des consignes…), que ce soit par compromission (à son insu, le salarié est vecteur d'une intrusion malveillante), ou que ce soit par préméditation (pour diverses raisons, le collaborateur veut intentionnellement nuire à l'entreprise). » Entre ces cas de figure, la typologie des maillons faibles est très large. *« À un niveau individuel, on trouve vos enfants, votre conjoint (ou conjointe) et toute la série des « ex ». Et au niveau de l'entreprise, il faut penser aux ex-salariés mécontents ou encore aux collaborateurs maladroits, voire peu précautionneux »*, précise Gaël Musquet, hacker éthique, hébergé par l'Armée américaine sur la base aérienne 105 à Évreux.

Donner les bons outils aux salariés

En raison du confinement dû au coronavirus, certaines entreprises ont généralisé le télétravail du jour au lendemain, sans y être préparées. Il leur a été difficile d'équiper 100 % de leur personnel avec les outils de sécurité nécessaires : *« Un réseau privé virtuel (VPN) suffisamment dimensionné pour accueillir tout le monde. Puis un système d'authentification forte. Sans oublier les Virtual Desktop Infrastructures (VDI) pour travailler de façon sécurisée sur les données de l'entreprise, au lieu de les rapatrier sur le PC de la maison,* décrit Gérôme Billois, expert en cybersécurité et gestion des risques numériques au cabinet Wavestone.

Ces faiblesses peuvent ouvrir la porte aux pirates, notamment si le salarié a le même mot de passe pour la vie professionnelle et la vie personnelle. » Fournir les bons outils aux salariés constitue donc le socle technologique nécessaire pour asseoir la culture de la cybersécurité.

Automatiser les processus de connexion

À cet égard, les entreprises peuvent également s'adresser à un gestionnaire de parc informatique. Celui-ci va adapter, à la demande, leurs infrastructures au télétravail, comme les téléformations à la sécurité et extension du VPN, ou la distribution au domicile des salariés de laptops configurés et sécurisés selon la stratégie de l'entreprise.
« Nous savons qui se connecte au système d'information de l'entreprise, selon quels droits et pour quelles applications, fait valoir Jean-Benoît Nonque, responsable Europe du sud chez Ivanti, un gestionnaire de parcs informatiques. *Si, avec l'accord de l'entreprise, le salarié se connecte avec un ordinateur personnel, nous installons automatiquement les logiciels de l'entreprise, notamment le VPN et les logiciels de sécurité. Il travaillera comme s'il avait un PC professionnel. »*

Faire de la cybersécurité de l'entreprise l'affaire de tous

Reste à convaincre chacun que la cybersécurité est l'affaire de tous. Cette acculturation s'appuie d'abord sur un manuel des règles élémentaires de cybersécurité. Celui-ci comprendra aussi les coordonnées des personnes à contacter en cas de problème ou de doute. La démarche va également s'appuyer sur cinq acteurs clés : *« La direction générale, des représentants des collaborateurs (CSE), les RH, le RSSI et enfin la DSI »*, reprend Franck Nielacny. Cependant, l'adhésion des collaborateurs passera surtout par l'engagement des managers de proximité. Quitte à rendre la cybersécurité ludique : *« Lorsqu'un collaborateur quitte son poste en laissant son PC ouvert, il se fera « hacker » sa messagerie électronique. Il devra alors payer sa tournée de croissants à l'équipe ! »*, poursuit Franck Nielacny.

Organiser des exercices de cybersécurité

Reste que la mise en situation réelle vaut mieux qu'une tournée de croissants. Ou presque. C'est en tout cas ce que propose le partenariat entre Harmonie Technologie et la start-up Crisotech. Objectif : s'entraîner à gérer une cybercrise dans les conditions du réel. Avec le buzz sur les réseaux sociaux, les interviews, les plateaux TV, la cyberdéfense… Pour ce faire, le tandem reproduit un environnement hyper réaliste afin d'immerger les membres de la cellule de crise. Dans ce contexte, le scénario ne doit pas brider l'expérience. Il va même laisser les membres de la cellule agir et réagir comme dans la vraie vie. Enfin la sécurisation de l'environnement de l'exercice devra aussi éviter de générer une « vraie fausse » crise.

Utiliser les mêmes armes que les pirates

Autre forme d'acculturation, les entreprises peuvent s'adresser à des plateformes de Bug Bounty, comme Bugcrowd, HackerOne, YesWeHack ou Yogosha qui monétisent auprès d'entreprises clientes les Pen Test (tests de pénétration des systèmes d'information). La démarche est claire : utiliser les mêmes technologies pour pénétrer un système d'information que les cyberpirates. Mais dans un but éthique. Surtout, les attaques des hackers éthiques sont menées en continu. À la différence des audits de sécurité qui, même s'ils durent d'une à trois semaines, restent ponctuels. Chez les équipes de développement, le recours au Bug Bounty participe à une culture d'amélioration continue de la cybersécurité.

Alors que la cybermalveillance se développe en parallèle de la digitalisation des organisations, la culture de la cybersécurité doit se développer à tous les étages de l'entreprise. Même si les RSSI installent les bons outils de protection, cela ne suffira pas. Les applications que développent les entreprises réclament elles-aussi leur dose de sécurité. Généralement, celle-ci vient après le développement. Ce qui rend les opérations de sécurisation plus complexes, plus longues et plus onéreuses. D'où l'intérêt de développer une culture de Security by Design. Non seulement pour les applications métier mais aussi pour les systèmes de sécurité électroniques eux-mêmes.

02

Security by Design : les règles à suivre pour les équipements de sécurité connectés

Dans le cadre d'une stratégie d'acculturation en matière de cyberprévention, la sécurité des nouvelles applications dès la conception est à la fois un objectif et une philosophie. Surtout lorsqu'il s'agit d'équipement de sécurité et de sûreté. Au programme : analyse du code, corrections, mise en production, architectures orientées micro-composants, API standardisées et orchestrateur de déploiement et d'exploitation.

Entreprises, administrations, collectivités… Toutes les organisations ont besoin de développer une stratégie d'acculturation en matière de cybersécurité. Cependant, elles ne sont pas les seules. Et les campagnes massives de rançongiciels cryptolockers (Wannacry, Petya, NotPetya, Industroyer…) nous le rappellent. Terriblement destructrices, leurs points d'entrée, pour certaines, furent des équipements de sécurité électronique. Un comble ! Mots de passe ouverts à tous vents, absence de mise à jour du système d'exploitation, adresses IP librement accessibles aux moteurs de recherche… Il devient urgent que les fabricants et intégrateurs de systèmes et équipements de sécurité renforcent non seulement leur culture de la sécurité mais aussi la cybersécurité des équipements qu'ils vendent ou installent. Pour opérer cette révolution, ils doivent adopter une démarche de Security by Design. On en est loin : 85 % des logiciels dans le monde contiennent au moins une vulnérabilité, selon SOSS V9.

Comment mettre en place une stratégie de « Security by Design » dans les systèmes de sécurité électronique ?

Sécuriser l'équipement, le protocole et la cible d'enregistrement

« Il est nécessaire de s'appuyer sur des produits ou des processus de confiance », insiste Jacques Roujansky, délégué permanent du Comité stratégique de filière Industries de sécurité (CSF-IS) et délégué général du Conseil des industries de la confiance et de la sécurité (CICS). Message reçu 5/5 par le fabricant allemand de caméras de vidéoprotection Mobotix. Lequel estime qu'il faut sécuriser à la fois l'objet connecté, le protocole de communication avec lequel l'équipement échange sur le réseau, mais aussi la cible d'enregistrement des images. *« Aucun de ces trois maillons ne doit être faible »*, indique Patrice Ferrant, responsable commercial France et Afrique chez Mobotix. Baptisée « Cactus », cette approche holistique de la sécurité a été certifiée par l'Agence nationale pour la sécurité des systèmes d'information (ANSSI) et le Centre national de prévention et de protection (CNPP).

« Le CNPP nous a conduit à évoluer dans le processus d'installation. Désormais, nous obligeons l'installateur à changer le mot de passe de la caméra. S'il ne le fait pas, il ne peut poursuivre son installation », précise Patrice Ferrant. Ensuite, la caméra IA MX7, codéveloppée avec Konica-Minolta (actionnaire majoritaire de Mobotix depuis 2016) bénéficie de deux environnements propres. La caméra gère en local ses enregistrements, ses traitements d'image et sa protection contre les attaques en déni de service. Ensuite, elle possède une machine virtuelle qui embarque les algorithmes d'intelligence artificielle de partenaires. *« Nous désolidarisons donc le fonctionnement de « l'œil intelligent » des algorithmes tiers, ce qui renforce la sécurité »*, fait valoir Patrice Ferrant.

Scanner les vulnérabilités du code source

Stéphane de Saint Albin, vice-président d'Hexatrust

« La Security by Design est à la fois un objectif et une philosophie. Elle n'est pas inatteignable. Mais elle n'est pas non plus définitive. Il y a donc des méthodes pour s'approcher d'un optimum, expose Stéphane de Saint Albin, vice-président d'Hexatrust, l'association qui fédère des entreprises françaises spécialisées en cybersécurité. *On peut commencer par scanner les vulnérabilités du code source. »* Parmi les acteurs capables de réaliser ces analyses, citons Veracode. Ce fournisseur étasunien, qui figure au Magic Quadrant 2020 du Gartner, affirme que 70 % de ses clients comblent les failles du code qu'ils développent. Mentionnons aussi CheckMarx, ImmuniWeb ou Synopsys. *« C'est la base du DevSecOps, à savoir l'intégration de la sécurité au sein du processus de développement agile du code avant la mise en production (DevOps) »*, reprend Stéphane de Saint Albin.

Théorie mathématique des méthodes formelles

Parmi les stars de l'analyse itérative, la startup française TrustInSoft fait figure à part. C'est l'un des rares éditeurs au monde dont la technologie s'appuie sur la théorie mathématique des méthodes formelles. Autrement dit, son service apporte la preuve mathématique que le code source n'a plus de bug ! Pour y arriver, le code à analyser passe à la moulinette de la plateforme de TrustInSoft. *« Les erreurs de conception et les bugs apparaissent alors soulignés en rouge »*, explique Fabrice Derepas, cofondateur de TrustInSoft. Il ne reste alors aux DevSecOps plus qu'à les corriger. Par itérations successives, le code sera ainsi nettoyé de toutes ses vulnérabilités. Reste que certains codes sont trop importants pour être aisément analysés et corrigés. Notamment les applications de sécurité dans le Cloud qui fonctionnement avec des IoT.

Sécuriser les API

C'est pourquoi les nouvelles architectures logicielles reposent sur des composants qui échangent leurs données via des interfaces de programmation applicatives (API).

« Les API publiques qui font partie d'un service et concernent les utilisateurs finaux. Quant aux API privées, ces interfaces techniques se placent entre des briques du système d'information. Elles ne sont visibles que par un superviseur, décortique Édouard Viot, directeur produit chez Rohde & Schwarz. *En fonction de leur maturité, les entreprises sécurisent en priorité les API publiques car ce sont les plus exposées. Mais les plus matures sécurisent également les API privées. »* Une manière de sécuriser ces architectures dès la conception consiste à connecter les composants ou applications à des coupe-feux applicatifs en ligne [Web Application Firewall (WAF)]. *« Le DevSecOps écrit son API selon la spécification standard Open API 3.0, laquelle renseigne ce qu'elle expose et accepte. Autrement dit à qui et comment elle parle »*, renchérit Édouard Viot.

Édouard Viot, directeur produit chez Rohde & Schwarz.

Des architectures de micro-composants

L'autre dimension des nouvelles architectures, c'est la conteneurisation d'applications. Objectif : automatiser leur déploiement et leur maintenance. Les architectures les plus récentes conteneurisent non plus des applications entières dans une machine virtuelle mais aussi des micro-services dans un Docker. Intérêt : on ne clone que ce dont on a besoin. Ces micro-composants s'assemblent également via des API et constituent l'application globale que supervise un orchestrateur comme Kubernetes. Cette plateforme Open Source que Google a offerte à la Cloud Native Computing Foundation automatise le déploiement, la montée en charge et la mise en œuvre de conteneurs, notamment de Dockers. *« 20 % des entreprises, principalement les startups, savent déployer les conteneurs. Les autres recourent à des machines virtuelles »*, analyse Édouard Viot.

Sécuriser les API entre les micro-composants

Point fort de Kubernetes, il permet, selon ses configurations, aux DevSecOps de mener des investigations de bugs. *« Comme l'exploitation est automatisée, le DevSecOps corrige les bugs directement dans le code source, puis redéploie automatiquement l'application. Plus besoin d'attendre des mois pour une correction, c'est du Continuous Delivery,* souligne Édouard Viot. *Les entreprises les plus matures le font quatre fois par jour. Les autres, une fois par mois. »* En outre, les DevSecOps vont compter sur une arme supplémentaire pour intégrer la sécurité à la conception : Rohde & Schwarz compte lancer d'ici cet automne un micro-WAF. Autrement dit un firewall en micro-service, proche de l'application, qui pourra protéger deux Dockers de micro-composants. La sécurité logique va donc commencer dès l'échelle microscopique.

En clair, prendre en compte la sécurité dès la conception des applications ou des produits reste une démarche lourde qui réclame, la plupart du temps, un accompagnement. Mais, au fur et à mesure du temps, les méthodologies sont à la fois s'affiner et se systématiser. Dans quelques années, le Security by Design sera un réflexe naturel.

03

Cyberattaques : retours d'expériences

Que se passe-t-il lorsque les organisations ont omis ou remis à plus tard la culture de la cybersécurité et la sécurisation des équipements de sécurité ? Elles prêtent davantage le flan au risque cyber. Panorama de quelques retours d'expérience d'entreprises qui ont été piratées.

Les attaques par rançongiciels connaissent une augmentation sans précédent. *« Le 15 novembre 2019, un interne des urgences signale un problème de droits d'accès à une application métier »,* se souvient Cédric Hamelin, responsable adjoint à la sécurité du système d'information du CHU de Rouen. Peu après, tombe le diagnostic de la direction des systèmes d'information (DSI) : un rançongiciel vient de chiffrer une grande partie des postes de travail et serveurs du CHU. C'est la paralysie. Le CHU de Rouen n'est pas le seul. Industrie (Fleury-Michon), Média (M6)... La contamination par rançongiciel s'étend à tous les secteurs d'activité. Y compris les entreprises de transport et de logistique.

Isoler la machine du réseau

Et le groupe Vingeanne (32 millions d'euros chiffre d'affaires, 230 salariés) n'y fait pas exception. Cette entreprise cumule 50 pistolets laser pour scanner les colis, 80 ordinateurs de bord dans les camions, 80 postes de travail, 150 smartphones et 40 serveurs virtuels répartis sur 3 serveurs physiques. Un seul grain de sable dans cette belle mécanique et c'est la paralysie. Un scénario catastrophe qui a bien failli arriver.

« À 7 heures du matin, une personne a mis son ordinateur en route. Par mégarde, elle a ouvert la pièce jointe d'un mail. C'était un cryptolocker (rançongiciel). Immédiatement, il s'est mis à chiffrer les répertoires que cette personne stockait sur certains serveurs virtuels, explique Kevin Le Chevalier, administrateur réseaux et systèmes du groupe Vingeanne. *Elle a bien réagi puisqu'elle a tout de suite appelé le directeur informatique. »* Le groupe ne dispose pas de directeur sûreté-sécurité. C'est donc le directeur informatique qui a géré la crise liée à cette cyberattaque. *« Il a demandé à la personne de débrancher son ordinateur du réseau bureautique en retirant la prise Ethernet. Et, surtout, de ne pas l'éteindre »,* reprend Kevin Le Chevalier. En effet, il aurait autrement été impossible de récupérer les données car le redémarrage accélère l'infection du cryptolocker.

Mais sans couper le courant

C'est justement l'erreur qu'a commise Alexandre Patte, gérant de BEF Sarc, également attaquée par un rançongiciel. Basée à Viabon (Eure-et-Loire), cette PME cumule les fonctions d'école de pilotage d'avion et d'importateur d'avions. *« J'ai dû remplacer tous nos disques durs et tout réinstaller. Au passage, j'ai perdu un grand nombre de données »,* confie le chef d'entreprise.

À l'inverse, comme chez Vingeanne, le CHU de Rouen s'est empressé de couper les accès à Internet. Et même au réseau interne.

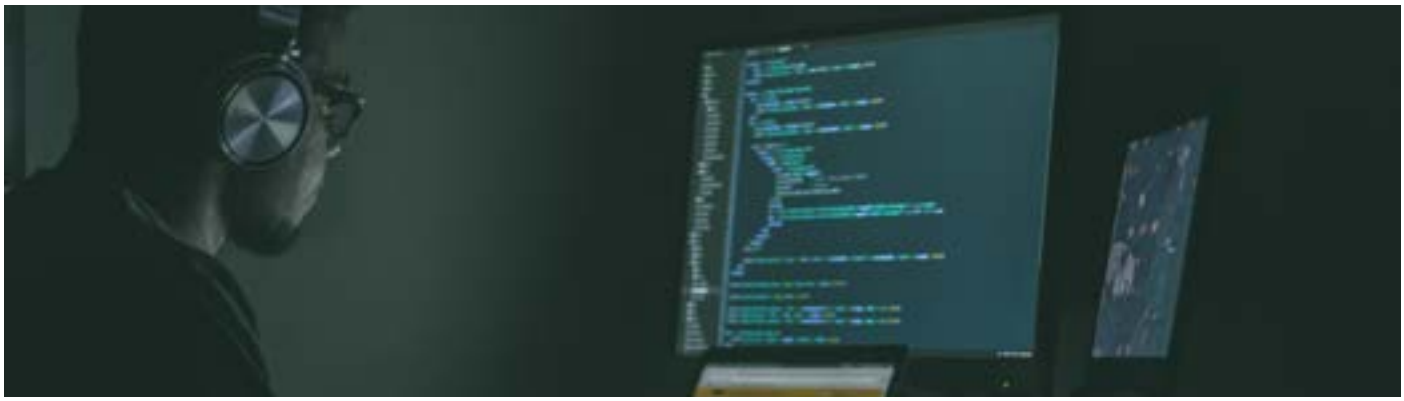
Puis, les équipes ont isolé tous les composants non impactés. *« Notamment les sauvegardes, les bases de données ainsi que les baies de stockage »*, détaille Cédric Hamelin dans une étude de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

La vertu des serveurs virtuels

Pour sa part, le groupe Vingeanne n'a pas autant souffert. *« L'infection a été très limitée. Elle n'a touché que les fichiers auxquels la personne avait accès sur son instance de serveur virtuel. Les droits d'accès avec mots de passe forts pour chaque salarié constituent déjà une première barrière de sécurité »*, reprend Kevin Le Chevalier. Le responsable informatique a dû diagnostiquer les 40 serveurs du serveur physique. *« Les serveurs virtuels sont plus faciles à isoler, à sauvegarder et à gérer. Notamment parce que nous avons un pare-feu sur la machine physique ainsi qu'un système UTM (Unified Threat Management, système unifié de traitement des menaces). Ce qui offre une sorte de pare-feu virtuel pour chaque serveur virtuel. Il y a donc deux pare-feux à traverser »*, poursuit Kevin Le Chevalier.

Ne pas payer la rançon

« Nous n'avons pas eu besoin de payer une rançon car, à 7 heures du matin, il n'y avait pas grand monde dans la société. Les dommages ont donc été très circonscrits » précise Jean-Claude Plâ, PDG du groupe Vingeanne. *Par ailleurs, dans un autre bâtiment, des serveurs de réplication configurés de la même façon que les premiers reçoivent chaque nuit les sauvegardes de tous les serveurs. Résultat, il n'a fallu qu'une demi-journée pour remplacer les fichiers endommagés ».*



Sauvegarder les données toutes les heures

Pas de quoi porter plainte à la gendarmerie. Cependant, Vingeanne a pris tout un train de mesures de prévention. À commencer par l'anti-spam Open Source MailCleaner. Puis le rythme des sauvegardes est passé de quotidien à horaire. Concernant les réplications sur les serveurs distants, elles se font désormais toutes les six heures. Un réseau local virtuel sécurisé de niveau 3 sur fibre optique relie les deux ensembles de serveurs, sans possibilité d'y accéder de l'extérieur. Enfin, le groupe a adopté la solution d'intelligence artificielle Sophos Intercept X. Point fort, celle-ci comprend et bloque les attaques aussi bien automatiques que manuelles – ainsi que les cryptolockers. Même sur les smartphones. D'une manière générale, il faut aussi maintenir à jour le système d'exploitation des machines ainsi que les logiciels, et en particulier les anti-virus.

Campagnes de sensibilisation

Reste à maintenir le personnel dans un esprit de sensibilisation aux règles de cybersécurité. Mots de passe forts, ne pas ouvrir de pièces jointes des mails non identifiés… À cet égard, le groupe Vingeanne recourt à un service interactif de Sophos. Lequel permet d'organiser en interne des fausses campagnes de phishing et de rançongiciels. L'intérêt ? Voir si les salariés tombent dans le piège. Morale de l'histoire : ceux qui se font ainsi avoir ne recommencent pas !

Preuve que la cyberprévention est avant tout une question de culture d'entreprise. Dans le sillage de cette acculturation, il reste nécessaire de former les développeurs d'applications d'entreprise à la démarche de Security by Design. Autrement dit, celle du DevSecOps. De la même manière, les responsables informatiques ou sécurité devront privilégier les équipements de sécurité électronique qui respectent l'intégration de la sécurité à la conception.

• *Erick Haehnsen*

Glossaire

• **API (Application Programming Interface ou interface de programmation) :** ensemble de définitions et de protocoles qui facilite le développement des applications.

• **Bug Bounty (prime aux bogues) :** récompense qu'une entreprise propose aux personnes qui trouvent des failles dans la sécurité de son système informatique.

• **Cesin (Club des Experts de la Sécurité de l'Information et du Numérique) :** association avec des objectifs de professionnalisation, de promotion et de partage autour de la sécurité de l'information et du numérique.

• **Cloud :** utilisation de serveurs informatiques distants au travers des réseaux Internet.

• **Conteneurs :** unité standardisée qui regroupe l'ensemble des composants et des dépendances d'une application (temps d'exécution, code, bibliothèques...)

• **Continuous Delivery (livraison continue) :** concept de développement de logiciels consistant à améliorer le code à l'aide d'outils automatisés.

• **CryptoLocker :** logiciel malveillant (Malware) chiffrant les fichiers sur les ordinateurs Windows.

• **DdoS (Distributed Denial of Service) ou « attaque par déni de service » :** attaque qui prend pour cible un système informatique en l'inondant de messages ou requêtes de connexion dans le but de provoquer un déni de service.

• **DevOps :** ensemble des tâches qu'effectuent les équipes d'une entreprise chargées du développement des applications (Dev) et de l'exploitation des systèmes (Ops).

• **Docker :** logiciel permettant d'automatiser le déploiement d'applications.

• **DSI :** Directeur des systèmes d'information

• **FOVI (fraude par faux ordre de virement ou « arnaque au président ») :** cyberattaques dont le but est de pousser un salarié à effectuer un virement bancaire en usurpant l'identité de son directeur.

• **IoT (Internet Of Things ou « Internet des Objets ») :** écosystème des objets (physiques ou virtuels) connectés à internet grâce aux technologies de l'information et de la communication.

• **Rançongiciel ou Ransomware :** logiciel malveillant visant à bloquer l'accès à l'ordinateur ou à des fichiers et à réclamer à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.

• **RSSI :** responsable de la sécurité des systèmes d'information.

• **Shadow IT** : systèmes d'information mis en œuvre dans une organisation sans approbation du DSSI.

• **UTM (Urchin Tracking Module) :** paramètres d'URL utilisés pour mesurer l'efficacité des campagnes de marketing en ligne à travers les sources de trafic et de l'édition multimédia.

• **VDI (Virtual Desktop Infrastructure) : t**echnique de virtualisation informatique, permettant à l'utilisateur d'accéder à une interface de PC virtualisée sur un serveur distant via le cloud.

• **VPN (Virtual Private Network ou « réseau privé virtuel) :** système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.

• **WAF (Web Application Firewall) :** type de pare-feu qui protège le serveur d'applications Web dans le backend contre diverses attaques.

Ce contenu vous a plu ?

Abonnez-vous à nos newsletters et recevez chaque semaine les dernières actualités de votre secteur, mais aussi des dossiers, enquêtes et interviews en exclusivité !

Je m'abonne

Ce dossier a été rédigé par Erick Haehnsen exclusivement pour Infoprotection.
Photos non contractuelles.