L’intelligence artificielle au secours de la cybersécurité

Face à la multiplication et à la sophistication des nouvelles menaces, les entreprises doivent revoir leur stratégie de cybersécurité. De nouvelles solutions à base d’intelligence artificielle permettent notamment d’assurer une protection plus efficace.

Le constat dressé par le dernier baromètre du cabinet PwC et de l’institut Ipsos fait froid dans le dos. Si, à l’échelle mondiale, la cybersécurité est devenue l’une des quatre préoccupations les plus importantes pour les dirigeants d’entreprise, la menace semble minorée en France. 29 % des sociétés seulement perçoivent la cybersécurité comme un enjeu prioritaire et cette prise de conscience est surtout le fait des grands comptes (52 %). Plus gênant encore, seule une entreprise sur deux a mis en place une stratégie dédiée pour lutter contre les cyber-risques.

Pourtant, la menace est tout sauf virtuelle. Selon une autre étude, celle du Cesin, le club des RSSI, 92 % des entreprises sondées affirment avoir été attaquées une ou plusieurs fois. Depuis un an, une sur deux observe même une augmentation de 48 % du nombre d’attaques. Arrêt de la production, indisponibilité du site internet, perte de chiffre d’affaires… Pour un quart d’entre elles, des impacts sur le business ont été ressentis.

Selon la formule consacrée : la question pour les dirigeants d’entreprise n’est plus « est-ce que je vais me faire attaquer ? » mais « quand ? ». Ils doivent, de plus, faire face à des menaces protéiformes. Au-delà des « classiques » attaques en déni de service (DDos), de défiguration de site web, de vol d’information ou de fraude externe, de nouveaux fléaux sont apparus. Dans le sillage des attaques WannaCry et NotPetya qui ont mis le monde en émoi en 2017, le ransomware est devenu la cyberattaque la plus fréquente.

Avec cette technique, encore appelée rançongiciel, les pirates exigent une rançon pour déverrouiller les données que leur malware a préalablement chiffrées. Avec un coût médian de 175 000 euros (rançon, temps d’arrêt, prestations…), la France a été, l’an dernier, le deuxième pays le plus touché par ce fléau juste derrière les Etats-Unis d’après un rapport de Sophos.

Directeur des Stratégies de Sécurité pour Symantec France,, Laurent Heslault observe même une explosion du phénomène ransomware ces derniers mois. « *Alors qu’il concernait par le passé essentiellement des particuliers, la menace touche désormais les entreprises dans une proportion de 50/50. On note aussi un glissement des ransomwares vers le mobile, essentiellement sur Android. La prochaine génération pourrait attaquer les objets connectés, des smart TV ont déjà été corrompues*. »

Laurent Heslault, Symantec France

Multiplication des nouvelles menaces

Pour Philippe Trouchaud, associé, à la tête de la cyber intelligence chez PwC, le crime organisé opère sa transformation numérique. « *Les attaques physiques de banque baissent au profit du ransomware. Il n'y a pas besoin d'hommes mais d'ordinateurs. Les risques sont moins grands. Si les pirates se font pincer, la justice sera plus clémente* ». La défense contre ces ransomwares, c'est bien sûr de faire des sauvegardes régulières sur un site distant. *« Des PME ont mis la clé sous la porte faute d'avoir eu ce réflexe de base »,* déplore Laurent Heslault.

Philippe Trouchaud, PwC

Autre menace « tendance », le cryptomining ou cryptojacking. Les pirates utilisent la puissance de calcul d'ordinateurs ou de serveurs pour effectuer le travail de minage nécessaire pour l'extraction de crypto-devises. En février dernier, des milliers de sites administratifs étaient infectés par du code malveillant. Avec ce concept né de la folie spéculative autour du Bitcoin et autres crypto-monnaies, les hackers volent non pas de la donnée mais de la CPU et de la Ram. Les dommages sont donc moins importants.

Le cryptojacking consomme néanmoins de l'électricité, de la bande passante et fait vieillir prématurément des machines en situation de surchauffe. Il a aussi un impact sur l'empreinte carbone et la productivité de l'entreprise. « *Démarrer Excel avec ou sans tâche de mining en toile de fond augmente de 5 à 10 le temps de lancement* », constate Laurent Heslault. Variante du cryptojacking, le cloud account hijacking consiste à récupérer des instances cloud d'entreprise pour faire du minage.

Si ransomware ou cryptojacking se répandent en masse, d'autres menaces plus sophistiquées sont conçues pour une cible donnée. Ces attaques dites concertées, ou APT, pour « advanced persistent threat » vont s'étaler sur des semaines voire des mois. « *A la différence de la pêche au filet, les APT vont exploiter toutes les faibles du système et utiliser l'ingénierie sociale* », explique Michel Lanaspèze, directeur marketing de Sophos pour l'Europe de l'Ouest. L'objectif est de s'ancrer durablement dans le système d'information et d'exfiltrer des données au fil de l'eau. Le tout, sous le radar de la DSI. Selon un rapport de FireEye il s'écoule en moyenne 175 jours entre le début de l'intrusion et le moment de sa découverte.

Cloud, le maillon faible

La transformation numérique expose également les entreprises à des nouveaux risques. Appelés à se multiplier, les objets connectés sont autant de portes d'entrée à leur système d'information (SI). Ces objets peu ou pas sécurisés conservent souvent le mot de passe constructeur de type « admin » ou « 12345 ». En octobre 2016, le botnet Mirai constitué de caméras IP zombies avait paralysé l'activité d'OVH et du fournisseur de DNS américain Dyn des heures durant. Depuis, de nombreuses variantes de Mirai ont émergé, la dernière en date s'appelle Torii.

Pour l'heure, les menaces autour de l'IoT concernent surtout l'industrie qui, conformément au concept d''usine du futur, a multiplié les capteurs sur ses lignes de production dans un environnement dit Scada (Supervisory control and data acquisition). *« Comme on ne peut pas mettre un antivirus et un pare-feu devant chaque objet connecté, il faut prévoir un cloisonnement dans l'architecture réseau pour que leur vulnérabilité potentielle n'ait pas d'impacts sur le SI traditionnel »,* conseille Alain Bouillé, président du Cesin et RSSI du groupe Caisse des Dépôts.

En revanche, la généralisation du cloud concerne toutes les entreprises. *« Avec le cloud, le SI est exposé à tous les vents,* poursuit Alain Bouillé. *Avant, les données étaient au chaud dans le datacenter, elles sont aujourd'hui éclatées dans le nuage*. » Les applications officielles en mode SaaS ne sont que la partie visible de l'iceberg.
Selon une récente étude du Cesin et de Symantec, une entreprise utilise en moyenne cinquante fois plus d'applications et de services cloud qu'elle n'en a recensés. Les salariés font notamment grande consommation des webmails de type Google Mail ou Yahoo Mail et des applications de partage de fichiers comme Dropbox ou WeTransfer.

Alain Bouillé, président du Cesin

Pour Alain Bouillé, *« ce shadow IT montre que l'offre proposée aux utilisateurs n'est pas à la hauteur des besoins. Il faut classer les usages par type, par exemple le transfert de fichiers, prendre un ou deux outils du marché et interdire les autres ».* Il conseille aussi de mettre en place une solution de type CASB (Cloud access security brokers). Elle va cartographier les flux, contrôler les entrées et sorties, et distinguer un trafic réseau anodin d'un flux de données sensibles.

Le cloud renvoie aussi au concept d'entreprise étendue, le SI étant ouvert aux partenaires, fournisseurs, sous-traitants ou clients. *« Les entreprises doivent évaluer la résilience de leur écosystème*, reprend Laurent Heslault. *Les tiers n'ont pas forcément le même niveau de protection. Ils constituent potentiellement un point faible. »*
L'attaque de Target est, à cet égard, un cas d'école. Les pirates ont ciblé un prestataire chargé de la surveillance à distance des systèmes de chauffage et de climatisation. Ce sous-traitant avait accès au système de facturation de Target, lui-même relié à son SI. Il suffisait alors aux hackers de déposer un malware sur les terminaux de paiement en magasins.

La limite des solutions périmétriques

A nouvelles menaces, nouvelles protections. Avec l'explosion du nombre de vulnérabilités – 14 714 signalées en 2017, contre 6 447 un an plus tôt selon CVE Details – les antivirus, les anti-spams, les anti-malwares et autres dispositifs anti-intrusion montrent leurs limites. A ce premier rideau de protection end point et anti exploit, d'autres briques sont venues s'ajouter. On a parlé du CASB pour la protection des données dans le cloud. Le DLP (data loss prevention) qui trace les données sensibles connaît un beau succès avec l'entrée en vigueur du RGPD.

Le régulièrement européen a aussi popularisé le chiffrement de bout en bout au risque de rendre aveugle les outils de supervision « *Rendus opaques, les échanges peuvent laisser passer des flux illégitimes »,* déplore Laurent Heslault. Également tendance, l'analyse comportementale consiste à placer un fichier dans un environnement sécurisé (sandboxing) pour étudier son comportement. Elle permet de lutter contre les ransomwares, le phishing ou la fraude au président.

Cette approche best of breed conduit toutefois à un empilement des solutions. « *Les entreprises*

peuvent avoir 30, 40 voire 70 fournisseurs de sécurité différents, constate Laurent Heslault. *Ce qui peut conduire à une sécurité disjointe. Les dispositifs doivent pouvoir discuter entre eux »* Dans ce but, Symantec est en train de créer un bus applicatif pour échanger des données de télémétrie, orchestrer et automatiser un certain nombre de tâches.

Changement de paradigme avec l'IA

Les cybercriminels étant passés maîtres dans l'art de modifier leurs malwares et de contourner les systèmes de protection traditionnels, le marché de la sécurité a opéré, il y a quelques années, un changement de paradigme en faisant appel aux mécanismes du machine learning et du deep learning. Il s'agit de casser le modèle classique qui consiste une fois un virus détecté, de créer son vaccin et sa signature. Les patchs arrivant avec un train de retard, cette approche bute contre les attaques avancées et les « zero day ».

« Avec l'intelligence artificielle, il n'y a plus besoin de connaître la menace pour la bloquer ni de faire des mises à jour en permanence, se réjouit François Baraer, ingénieur commercial Europe du Sud chez Cylance. *Le modèle repose sur une approche statistique. Il va analyser jusqu'à un million de caractéristiques d'un fichier, son éventuelle signature, sa taille, son code, toutes ces suites de bits qui se répètent. A partir de là, un score lui sera attribué pour savoir si un fichier peut s'exécuter ou non. Le système mettra ainsi en quarantaine un ransomware, un ver, un trojan ou un key logger.»* L'entraînement du modèle permet de réduire les faux positifs.

« Ce que l'IA sait bien faire, c'est lire des paquets réseaux à grande vitesse et les comparer à des modèles de comportement, complète Grégory Cardiet, ingénieur avant-vente de Vectra. *Est-ce que cette machine a un comportement d'attaque ? Certains malwares sont inconnus au bataillon. Ils n'ont été créés que pour ce client, le vol d'information est silencieux*. » Pour l'expert, l'IA peut être aussi un moyen de pallier la pénurie de compétences en cybersécurité. De toutes façons, l'être humain ne peut matériellement pas analyser l'intégralité des données engrangées dans un système de supervision. « *L'IA va effectuer l'analyse de premier niveau et décharger les opérateurs qui doivent lire des centaines de lignes de logs. Un travail ingrat. Là, ils vont se concentrer sur les événements essentiels L'IA apporte aussi une aide à la décision aux experts confirmés. »*

Faiblement consommateurs en ressources CPU et Ram par rapport aux antivirus traditionnels et ne nécessitant pas nécessairement de connexion internet, les modèles IA peuvent protéger des machines qui ne l'étaient pas ou plus comme des imprimantes, des objets connectés ou des postes sous Windows XP.

Dans ce concert de louanges sur les apports de l'IA, il y a quelques sons dissonants. Alain Bouillé dénonce le matraquage des éditeurs dont toutes les solutions sont désormais « IA inside ». Pour certains experts, l'IA pourrait aussi paradoxalement renforcer la cybercriminalité. Dans l'éternel combat de l'épée et du bouclier, des hackers utilisent, eux aussi, des algorithmes complexes pour automatiser certaines tâches, valider et complexifier leurs outils, faire des simulations pour voir si leur malware passe.

Indispensable machine learning

Au-delà du buzz marketing, les premiers retours d'expérience d'entreprises protégées par des solutions à base d'IA commencent à venir. Saint-Gobain et Schneider Electric, clients respectivement de Vectra et Cylance, viendront témoigner aux Assises de la sécurité.

OpinionWay utilise, lui, la solution de Darktrace depuis trois mois. Directeur informatique de l'institut de sondage, Jean-Michel Bernard cherchait un scanner de vulnérabilités. *« L'analyse manuelle était trop fastidieuse. Nous sommes une PME de 85 personnes, limitée en ressources et sans équipe de sécurité dédiée. »*

Pour l'heure, il ne tarit pas d'éloges sur l'outil *« simple d'utilisation et paramétrable en moins d'une heure ». « Il fait face aux menaces protéiformes. Rien ne semble lui échapper. L'analyse de flux des réseaux n'a pas d'impact sur le fonctionnement des applications. Il n'y a pas de déploiement sur les postes de travail mais une appliance dans la salle serveurs. »* Le DSI a catégorisé les utilisateurs par profil métier pour réduire les alertes et les faux positifs. Il apprécie aussi de pouvoir remonter les trafics réseaux dans le temps, comme un film.

Pour Jean-Michel Bernard, le machine learning est le seul moyen de prévenir attaques avancées. *« Il n'est plus possible aujourd'hui de penser sécurité sans machine learning. »* La solution de Darktrace a, enfin, aidé OpinionWay à se mettre en conformité au RGPD en protégeant ses actifs, à savoir les données des enquêtes. *« Un sous-traitant a des obligations en matière de confidentialité des fichiers de données personnelles* », rappelle le DSI qui est également DPO.

L'enjeu organisationnel

Au-delà de ces parades techniques, la sécurité reste avant tout un enjeu organisationnel. La politique de sécurité du système d'information (PSSI) doit être régulièrement réévaluée à la suite d'audits de vulnérabilité et de tests d'intrusion. Pour être prête le jour J, une entreprise va simuler différents scénarii afin d'évaluer la chaîne de coordination et bâtir les plans de continuité d'activité (PCA) et de reprise d'activité (PRA). Les grands comptes possèdent aussi un centre de sécurité opérationnelle ou SOC (Security operation center) pour monitorer l'activité. Une supervision que les PME, qui n'ont ni le budget ni les ressources internes, peuvent externaliser.

Dans son étude, PwC pose quatre piliers de base pour une PSSI aboutie. Au-delà de l'investissement dans les outils de sécurité, le cabinet préconise de recruter une ou plusieurs personnes dédiées à la cybersécurité, d'élaborer une stratégie de défense et de prendre une assurance couvrant le risque de cyberattaques et ses dommages. Parmi les 600 entreprises françaises de toutes tailles sondées, seules 18 % ont pris toutes ces mesures.

« Ces 18 % d'entreprises consacrent de 8 à 10 % de leur budget informatique à la sécurité, fait remarquer Philippe Trouchaud. *Il faut plusieurs jours pour pénétrer leur SI. La moyenne est, elle, de 3 % du budget IT. Seules quelques heures suffisent. Si le RGPD a pu débloquer de façon opportuniste de l'argent pour des projets, il n'y a pas eu de saut quantique. Le règlement européen a surtout amélioré le niveau sensibilisation. »*

Ce que confirme Eric Devaulx, country manager de Sophos France. *« Le RGPD a remis le sujet de la*

protection des données sensibles au-dessus de la pile des dossiers. Mais, sur un budget estimé à 4 ou 5 milliards d'euros par an sur les prochaines années, l'essentiel de la dépense porte sur des prestations d'audit de la conformité. La seule augmentation significative sur les ventes concerne les solutions de chiffrement des données. »

Préparer la résilience de son entreprise

Dans un rapport que le Cigref rendra public en ce mois d'octobre, le club des DSI rappellera que la protection contre les risques cyber concerne l'ensemble de l'entreprise et pas seulement les SI. *« L'informatique envahit tout. Il est rare qu'un processus métier n'embarque pas des lignes de code, ce sont autant de vulnérabilités* », note Jean-Claude Laroche, DSI d'Enedis et président du cercle « Cybersécurité » du Cigref.

Jean-Claude Laroche, Pdt du cercle « Cybersécurité » du Cigref.

Face à ce constat, le plan de traitement des risques cyber doit être, selon lui, global. « *Ce n'est pas le seul fait du RSSI. Une personne doit incarner le sujet auprès du comex ou du conseil d'administration. Enedis a fait le choix de nommer un directeur cyber. S'il est administrativement rattaché à moi, il est totalement indépendant. La fonction est transverse. Dans d'autres organisations, ce rôle peut être endossé par un spécialiste du risk management ou un RSSI de très haut niveau. »*

Mais quelle que soit la qualité de la politique de sécurité mise en place, les dirigeants doivent s'attendre un jour ou l'autre à avoir leur SI dans le noir. « *Il s'agit de préparer la résilience de son entreprise en imaginant le pire*, poursuit Jean-Claude Laroche. *Que se passerait-il lors d'une crise ultime ? Privé de messagerie et de téléphone, quels seraient les moyens de communication rustiques à mettre en œuvre ? Comment réunir sur un plateau les hommes clés de l'organisation pour faire face à cette situation ? Les entreprises qui ont subi WannaCry et NotPetya savent de quoi je parle. »*

Dans le cadre de la directive européenne NIS (Network and Information System Security), l'Agence nationale de la sécurité des systèmes d'information (Anssi) doit publier, le 9 novembre prochain, une première liste d'entreprises considérées comme des Opérateurs de services essentiel (OSE), une définition plus large que les Opérateurs d'importance vitale (OIV) introduits par la loi de programmation militaire de 2013. Ces OSE auront l'obligation de démontrer qu'elles ont sécurisé leurs systèmes les plus sensibles en les faisant auditer par des tiers de confiance référencés.

L’humain, facteur de risque n°1

Multiplier les dispositifs techniques et organisationnels ne sert toutefois à rien si on ne s’intéresse pas à l’homme, premier facteur de risque. « *Le maillon faible se situe entre la chaise et le clavier. L’ingénierie sociale existe depuis les débuts spam* », rappelle Michel Lanaspèze. Tous les experts interrogés dans ce dossier insistent sur la nécessaire sensibilisation de tous les collaborateurs aux règles fondamentales de sécurité. Entre autres, comment composer un mot de passe ou pourquoi il faut bannir les clés USB.

Les communications anxiogènes ou institutionnelles, noyées dans le flot des informations internes, donnent rarement de bons résultats. Les spécialistes conseillent d’opter pour des approches plus engageantes à base de jeux et de mises en situation. PwC propose notamment un serious game baptisé Game of Threats à destination des dirigeants. « *Dans ce jeu, les rôles sont inversés. Le DAF et le DG défendent, le RSSI attaque. On peut scénariser des attaques venues de l’intérieur, du crime organisé ou d’un pays hostile »,* explique Philippe Trouchaud.

La plateforme Sensiwave de Conscio Technologies permet, elle, de mener des campagnes de sensibilisation personnalisées auprès de populations à risque comme les collaborateurs nomades. Simuler des menaces en situation réelle permet aussi de frapper les esprits. Sophos propose de concevoir un exemple de faux phishing personnalisable à souhait. *« Si l’utilisateur tombe dans piège, il va devoir suivre un module d’e-learning de 20 minutes pour se dédouaner. Sinon l’administrateur avertit son manager. Ça marche très bien »,* estime Michel Lanaspèze. On veut bien le croire.

———————————————————————————————————————-

La 18ème édition des Assises de la Sécurité à Monaco *aura lieu du 10 au 13 octobre.*
Rendez-vous incontournable de la cybersécurité en France, les Assises vous proposent un programme dense et varié avec, notamment, 170 conférences, ateliers et tables-rondes, des espaces de networking et des milliers de OneToOne

(crédit photo © shutterstock)