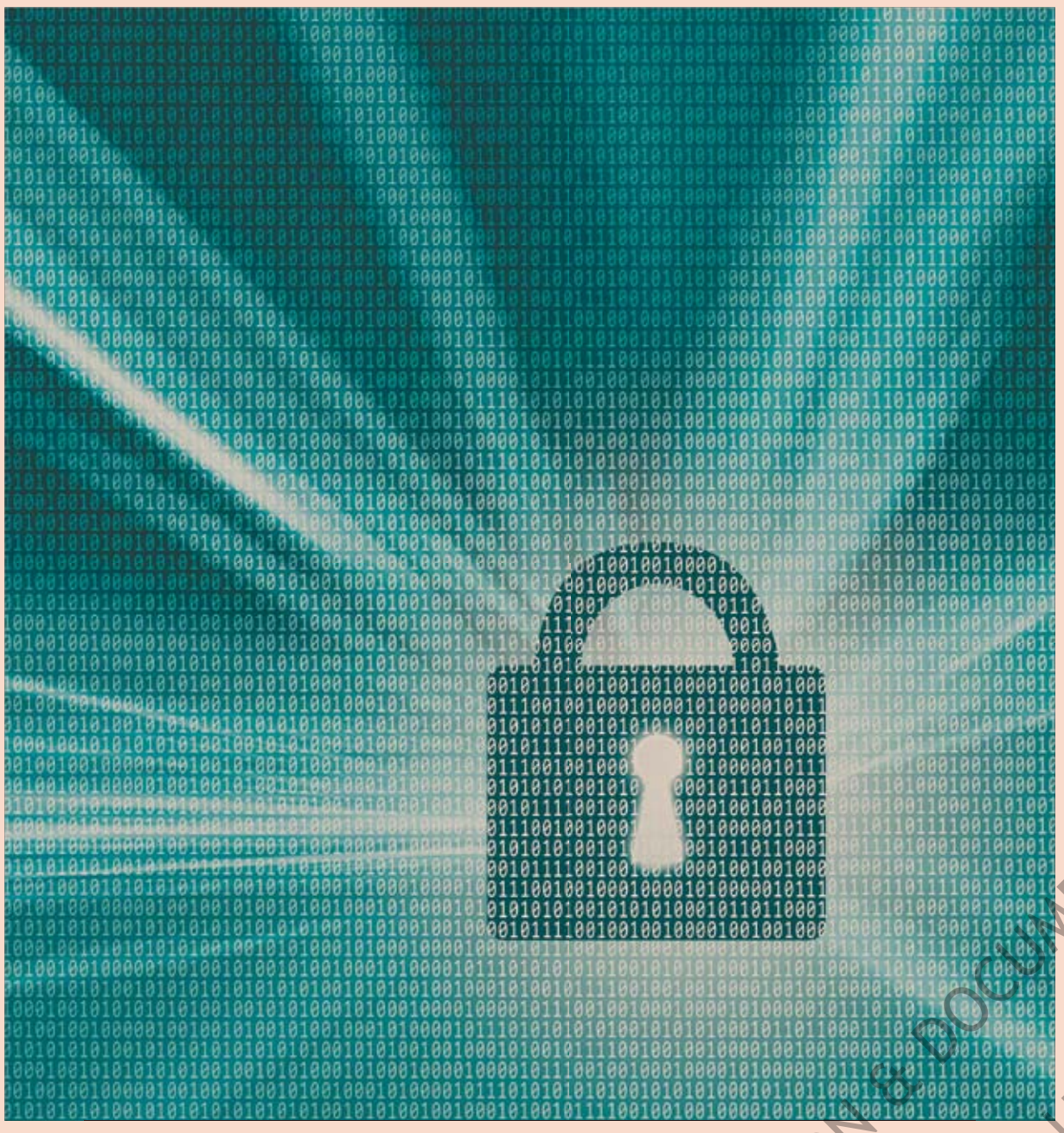

Cybersécurité et transformation numérique

Château fort ou douaniers ?

La multiplication des points d'entrée dans l'entreprise liée à la transformation numérique impose une nouvelle approche de la cyberprotection

Face au risque croissant de piratage informatique, les entreprises doivent redoubler de vigilance pour se protéger des hackers qui trouvent sans cesse de nouvelles failles où s'engouffrer. terminaux mobiles, objets connectés, applications web, cloud: la menace provient désormais de ces vecteurs externes, nouveaux talons d'Achille de la sécurité informatique. Alors que le nouveau Règlement européen sur la protection des données (RGPD) fait de la sécurité une exigence "par défaut", les organisations doivent réviser leur stratégie de défense pour protéger leurs données et celles de leurs clients, avec à la clef un objectif majeur: parvenir à concilier sécurité informatique et accélération numérique.

MARION GODEFROY

Entre le 18 et le 23 septembre dernier, OVH, le plus gros hébergeur européen, était victime de la plus violente attaque par déni de service (DDoS) jamais enregistrée dans l'histoire du web. En cause: un réseau de 145000 caméras de surveillance connectées et non protégées, infectées par des cybercriminels pour envoyer jusqu'à un térabit de trafic sur les infrastructures de l'hébergeur. Si l'épisode a pu être maîtrisé par l'entreprise nordiste, il a créé un précédent on ne peut plus inquiétant, et a confirmé une tendance qui se dessine depuis quelques années déjà: les pirates s'immiscent désormais dans les entrailles des serveurs grâce à des vecteurs externes que sont les objets connectés, les smartphones et tablettes, le cloud ou les applications web. *"Le digital encourage l'ouverture des entreprises et c'est une bonne chose. Mais en multipliant les points de connexion, on agrandit la surface d'attaque et le nombre de cibles potentielles"*, explique Étienne Chevillard, responsable sécurité chez Sigma Informatique.

"Le digital encourage l'ouverture des entreprises et c'est une bonne chose. Mais en multipliant les points de connexion, on agrandit la surface d'attaque et le nombre de cibles potentielles"

De nouveaux chemins d'attaque

Le télétravail, la mobilité, la dépendance aux applications web de type SaaS et l'utilisation décomplexée du cloud et des réseaux sociaux constituent autant de nouveaux usages qui se sont développés au sein des entreprises et qui ont rendu floues les frontières entre intérieur et extérieur, entre sphère professionnelle et privée. *"Ce qui est nouveau, ce n'est pas tant le type de cyberattaques que les chemins empruntés, puisqu'on a multiplié les points d'entrée en multipliant les environnements de connexion"*, explique Stanislas de Maupeou, directeur stratégie et marketing pour les activités systèmes d'information critiques et cybersécurité chez Thales. Selon lui, ces nouveaux usages ont rendu presque obsolètes les solutions de sécurité informatique traditionnelles: *"la défense de nature périmétrique est toujours utile, mais ne répond pas aux usages de nos outils communicants. Il faut penser aux autres cas d'usage: cloud, mobilité… Il devient essentiel de protéger la donnée quel que soit l'environnement"*.

La fin du modèle du château fort

Pour se protéger de ces nouvelles menaces, Loïc Guézo, stratégiste cybersécurité chez Trend Micro, évoque un changement de méthode pour passer du modèle du château fort *"avec une barrière unique à l'entrée entre l'entreprise et l'extérieur"* à celui du *"douanier"*. *"Aujourd'hui, les pirates ne tentent plus de pénétrer par la grande porte, mais par les trous que l'on a faits dans les murs. Il faut organiser une défense en profondeur, avec un contrôleur pour chaque ordinateur ou tablette qui ouvre le courrier avant qu'il ne pénètre dans nos machines, et décide de livrer ou pas le contenu au destinataire."* Ce système élaboré d'ouverture et de test de courrier repose sur le mécanisme du "sandbox" (bec à sable en anglais), qui permet l'exécution de code tout en préservant le système d'exploitation. Le sandboxing permettrait de détecter les 2 à 3 % de messages corrompus que les anti-spam et anti-virus ne sont pas capables d'identifier. Selon Loïc Guézo, ce sont aujourd'hui ces 2 % de messages qui portent 98 % du danger, *"parce qu'ils sont particulièrement crédibles et personnalisés. La technologie sandbox va permettre de regarder ce que fait le programme une fois lancé dans un environnement virtuel et repérer tout indice suspicieux comme une connexion à un serveur externe"*.

Sécuriser les mobiles

Avec une moyenne de *"140000 nouveaux logiciels malveillants par jour"* et de nouvelles attaques qui ciblent les mobiles, Philippe Rondel, directeur technique France de Check Point, en est convaincu, *"les usages mobiles en croissance exponentielle imposent une autre approche de la sécurité informatique"*. La réponse se trouverait en partie dans le cloud: *"pour que les collaborateurs bénéficient de la même protection à l'extérieur qu'à l'intérieur du réseau de l'entreprise, on peut installer une passerelle de sécurité dans le cloud, à laquelle on ajoute une offre de chiffrement pour les documents les plus sensibles"*. En outre, pour sécuriser les connexions en cas d'usages nomades, l'entreprise peut ajouter au système classique VPN (réseau privé virtuel) une offre de ségrégation des données,

Un changement de méthode pour passer du modèle du château fort "avec une barrière unique à l'entrée entre l'entreprise et l'extérieur" à celui du "douanier", avec un contrôleur pour chaque terminal

"Pour que les collaborateurs bénéficient de la même protection à l'extérieur qu'à l'intérieur du réseau de l'entreprise, on peut installer une passerelle de sécurité dans le cloud." Philippe Rondel, Check Point.

"Aujourd'hui, les pirates ne tentent plus de pénétrer par la grande porte, mais par les trous que l'on a faits dans les murs. Il faut organiser une défense en profondeur, avec un contrôleur pour chaque ordinateur." Loïc Guézo, Trend Micro.

afin de séparer l'utilisation professionnelle et l'utilisation personnelle du mobile. On peut aussi compter sur les solutions d'authentification adaptative: *"il s'agit de faire varier les exigences d'authentification selon le contexte, si le collaborateur est dans l'entreprise, chez lui ou dans un lieu public, le niveau de sécurité pour se connecter au réseau ne sera pas le même"*, explique Olivier Morel, directeur avant vente d'Ilex International, spécialiste de la gestion des identités et des contrôles d'accès. Pour faire face aux nouvelles attaques qui ciblent les mobiles, des solutions dédiées apparaissent aussi, comme le Mobile Threat Prevention (MTP), sorte d'anti-virus version mobile qui analyse en temps réel le contenu du smartphone ou de la tablette.

La gouvernance et l'humain en tête

Dans un monde où les entreprises sont interconnectées, les échanges et le partage d'informations n'ont jamais été aussi nombreux et encouragés, entre collaborateurs mais aussi entre partenaires et fournisseurs, multipliant à l'envi les points de sortie de données et les points d'entrée pour les cybercriminels. S'il n'est pas question pour eux de lutter contre l'émulation et l'accélération numérique, les experts pointent unanimement du doigt le phénomène du Shadow IT, qui recouvre les infrastructures informatiques et systèmes d'information mis en œuvre dans l'entreprise sans l'approbation des responsables SI. *"Les directions de services informatiques doivent reprendre le contrôle, identifier tous les points de sortie dans le périmètre de l'entreprise et les prestataires concernés, et organiser une prise de conscience des collaborateurs sur le sujet"*, préconise Loïc Guézo. *"Notre meilleure mesure de sécurité se trouve entre la chaise et le clavier: c'est l'utilisateur"*, renchérit Henri Codron, vice-président du Club de la sécurité de l'information français (Clusif). Ce club, qui regroupe plus de 300 professionnels de la cybersécurité, conçoit notamment des outils de sensibilisation à destination des entreprises et du grand public: sa prochaine fiche portera sur les ransomwares, *"cette nouvelle forme d'attaque avec demande de rançon a beaucoup évolué en 2016 pour cibler les entreprises"*, précise-t-il. Selon Étienne Chevillard, de Sigma Informatique, *"il y a un grand besoin de responsabiliser les collaborateurs sur ces sujets, dans les grands groupes comme les PME. Il faut rappeler régulièrement les règles de bon sens, informer sur les nouvelles menaces, varier les formats – fiches, formations, serious games – et insister sur les risques liés au télétravail et à la mobilité"*.

Le RGPD: un appel à investir

"Si la cybercriminalité est de mieux en mieux organisée, la réponse pour se protéger doit être de plus en plus étoffée", estime-t-on au Clusif. Ainsi, les professionnels du secteur saluent l'adoption du nouveau Règlement général sur la protection des données par le Parlement européen (RGPD). *"Cette nouvelle législation encourage les entreprises à investir dans la sécurité pour être aux normes, elles ne peuvent plus y échapper et c'est une bonne chose"*, martèle Henri Codron. En imposant les concepts de "Privacy by Design" (protection des données personnelles dès la conception) et de "Security by Default" (les données doivent par défaut être protégées) comme des règles obligatoires pour toutes les organisations, le RGPD adresse un signal fort à destination des dirigeants et des responsables SI: *"nous allons devoir renouveler nos méthodes et nos outils"*, affirme Stanislas de Maupeou, qui ajoute que pour les systèmes déjà en opération, le principe de sécurité par défaut va se traduire chez Thales par la pratique de la "sécurité par service", qui consiste à *"tester la sécurité de façon régulière par des méthodes d'intrusion, de test et de veille permanente des systèmes"*.

Néanmoins pour les experts en cybersécurité, ces nouvelles solutions ne doivent en aucun cas ralentir les systèmes: *"nous devons être capables de soutenir et d'accélérer la transformation numérique qui est vitale pour les entreprises, tout en sécurisant les données"* affirme Stanislas de Maupeou; d'où la nécessité selon lui de concevoir la sécurité comme un service: *"la clef de la réussite est d'avoir une approche UX (User Experience). Il faut que les solutions soient performantes et ergonomiques sur tous les supports et dans tous les environnements, pour que la sécurité ne soit pas vécue comme une contrainte dont les collaborateurs cherchent à s'affranchir"*. La sécurité par défaut et en tant que service, telles sont les lignes directrices qui doivent guider les entreprises en vue de l'entrée en application du RGPD, au printemps 2018. ■

Chiffres clés

Une hausse des investissements

En France, le nombre de cyberattaques détectées par les entreprises en 2016 s'élève en moyenne à 11 incidents par jour (4 165 incidents), soit environ deux fois moins qu'en 2015, où les entreprises françaises avaient recensé en moyenne 21 incidents quotidiens.

Au cours des 12 derniers mois, les entreprises hexagonales ont investi en moyenne 3,9 M€ dans la sécurité de leurs systèmes d'information. 59 % des dirigeants ont augmenté leurs dépenses de cybersécurité en 2016; 43 % déclarent que leur première priorité d'investissement se porte sur la sécurité des objets connectés.

Source: PwC, "The Global State of Information Security Survey 2017"

"Il faut rappeler régulièrement les règles de bon sens, informer sur les nouvelles menaces, varier les formats et insister sur les risques liés au télétravail et à la mobilité." Étienne Chevillard, Sigma Informatique.

Ces nouvelles solutions ne doivent en aucun cas ralentir les systèmes: "nous devons être capables de soutenir et d'accélérer la transformation numérique qui est vitale pour les entreprises, tout en sécurisant les données"

Général Marc Watin-Augouard

fondateur du Forum international de la cybersécurité (FIC)

Communiqué

"Demain il faudra tout regarder en même temps, aussi bien les vecteurs internes que les vecteurs externes de menace, ce qui exigera une approche sécuritaire entièrement globale"

Pouvez-vous présenter le FIC?

J'ai fondé le FIC en 2007, avec la volonté de développer une coopération interservices et internationale pour mieux lutter contre les prédateurs du cyberespace. L'objectif était de décloisonner le public du privé, le français de l'étranger, l'État, les collectivités territoriales, et rassembler une fois des acteurs divers qui pouvaient s'emparer de cette question (centres de recherche, grandes écoles, collectivités territoriales, entreprises...). Depuis, le salon s'est développé, jusqu'à attendre plus de 240 partenaires sur un espace de 10 000 m² et plus de 2000 visiteurs. Cette année, nous mettons à l'honneur les nouvelles technologies et les nouveaux usages: comment l'espace numérique peut-il se développer en toute sécurité? Le forum, qui est ouvert au grand public, rassemblera des entreprises qui imaginent les solutions et systèmes de sécurité de demain.

Quels sont les enjeux pour l'année à venir en termes de cybersécurité?

Les questions de sécurité doivent désormais être intégrées "by design": une bonne partie des problèmes pourrait être réglée en ayant un dispositif cohérent pensé en amont dans la stratégie numérique de l'entreprise. Grâce aux bons outils, beaucoup de cyberattaques pourraient être prévenues et voir leur occurrence réduite. C'est l'un des défis pour 2017. L'autre grand enjeu est la question des "rançongiciels" (de l'anglais ransomware). Ces intrusions dans les systèmes d'information sont une tendance lourde et peuvent avoir de graves conséquences. Toute la question est d'y sensibiliser les entreprises.

Quelles sont les tendances en termes d'outils de protection?

La tendance qui se dessine, c'est le développement des objets connectés et donc des systèmes connectés: plus ces objets sont nombreux, plus la fragilité du système est forte. Cela pose une vraie question pour notre sécurité, non plus dans un rapport unique homme/machine mais dans un environnement machine/machine. Cette évolution va conduire à avoir une approche beaucoup plus systémique de la cybersécurité: demain il faudra tout regarder en même temps, aussi bien les vecteurs internes que les vecteurs externes de menace, ce qui exigera une approche sécuritaire entièrement globale.

Forum international de la cybersécurité
les 24 et 25 janvier 2017, Lille
https://www.forum-fic.com

Les limites de la cyber-assurance

Alors que le risque de cyberattaque a progressé de 51 % en France en 2015, les entreprises sont de plus en plus enclines à souscrire une cyber-assurance: selon une étude du cabinet PwC de janvier 2016, 52 % se disent ainsi prêtes à signer, pour garantir leur sécurité en cas de vol ou fuite de données. Reste que la cyber-assurance en est encore à ses balbutiements, comme le souligne Christophe Jourdet, Country Leader France chez NTT Security, filiale française du groupe japonais spécialisé dans la sécurité des systèmes d'information. *"Toute la complexité pour l'assureur aujourd'hui est de bien définir le risque concerné"*, analyse-t-il: en effet, on ne peut couvrir que ce que l'on peut estimer, et c'est justement là que le bât blesse. *"On sait bien que même si une entreprise prend toutes les mesures de prévention possibles, aucun système n'est infaillible à 100 %. Il faut donc démontrer que les mesures de sécurité ont été prises, prouver la conformité de la protection de son système d'information, et présenter un audit réalisé en amont qui montre les failles du système concerné"*, souligne l'expert.

Par ailleurs, le préjudice de l'entreprise victime d'une cyberattaque peut être très difficile à évaluer: *"il y a les termes financiers, mais également des éléments qu'on ne maîtrise pas, comme la réputation de l'entreprise, entre autres nombreuses façons dont elle peut être impactée"*, commente Christophe Jourdet. À noter qu'une grande partie du coût de la cyber-assurance contractée – *"50 %"*, estime-t-il – est liée aux frais d'intervention en urgence suite à une cyberattaque: *"il faut pouvoir remédier à un incident en quelques heures: fixer le problème en mobilisant des experts, et le résoudre. Vient ensuite le temps de l'estimation du coût des conséquences"*. L'essentiel pour une entreprise est ainsi d'avoir établi en amont un plan d'action de réponse aux incidents: *"il faut avoir en tête que l'on va être attaqué un jour ou l'autre. Si les situations d'urgence sont anticipées, que l'on a les bons contacts et la bonne assurance qui dépêchera les bons experts en temps voulu, alors on limite déjà les dégâts"*. ■

On ne peut couvrir que ce que l'on peut estimer, et c'est justement là que le bât blesse