Guide de la cybersécurité

6 analyses à l'usage des dirigeants

Faire face aux prises d'otage numériques, affronter les attaques insidieuses, être à l'écoute tant des autorités que de ses experts internes, combattre la complexité… Suite aux dernières cyberattaques médiatiques, voici quelques pistes pour devenir un acteur à part entière de la protection de son entreprise.

« La cybersécurité, un sujet de Comex »

Les chefs d'entreprise assistent, tout comme leurs collaborateurs, à la médiatisation croissante des enjeux de cybersécurité. ***Jean-François Louâpre****, vice-président du CESIN, le Club des experts de la sécurité de l'information et du numérique, explique pourquoi les dirigeants doivent travailler main dans la main avec leurs responsables de la sécurité de l'information.*

PROPOS RECUEILLIS PAR DORIAN MARCELLIN

Attaque sur TV5 Monde ou plus récemment sur l'*Office of Personnel Management* de la Maison Blanche. Les grands médias généralistes français évoquent de plus en plus les enjeux de cybersécurité. Est-ce une bonne nouvelle ?

Je remonterais même à l'exemple de la cyberattaque sur Bercy, en 2011. C'était la première fois que la cybersécurité faisait une apparition au journal télévisé de 20h avec Claire Chazal ! Cette médiatisation concourt clairement à une prise de conscience généralisée de la population et donc des dirigeants d'entreprise. Avec deux messages clés : la sécurité n'est pas qu'une affaire de spécialiste et une cyberattaque peut arriver à tout le monde. Si l'on reprend tous les grands exemples rendus public, on retrouve ainsi des médias, des ministères, des grands groupes de distribution, des acteurs industriels ou encore des entreprises d'audiovisuel. Tous les secteurs sont concernés. Pendant longtemps, le *top management* des entreprises a adopté une posture qui consistait à se dire : ce genre de problèmes n'arrive qu'aux autres… jusqu'à ce qu'il soit trop tard. C'est en train de changer. De plus en plus de dirigeants prennent désormais conscience de la dépendance de leurs activités à leur système d'information et dans ce cas, la cybersécurité peut devenir un sujet de Comex.

« Il est possible d'être des acteurs à part entière de la sécurité de l'entreprise même sans aucun bagage technique. »

Jean-François Louâpre
Vice-président du CESIN

Qu'est-ce qui a changé pour les responsables de la sécurité des systèmes d'information (RSSI) dans les entreprises ces dernières années ?

Concernant leur position dans l'entreprise, il y a finalement assez peu de changement. Environ 60% sont toujours rattachés à la DSI. Les autres se répartissent entre la direction générale (notamment pour les entreprises de taille modeste), la direction de la sûreté ou celle des risques (pour les plus grandes) sans qu'il soit possible de définir une réelle tendance. Petit à petit, le RSSI est moins vu comme un simple expert technique et plus comme un acteur à part entière de la gestion opérationnelle du risque. Une réputation qu'il acquiert avec plus de facilité quand il évolue hors de la DSI. Depuis 20 ans, les RSSI sont de plus en plus présents dans les entreprises – en commençant par les grands groupes. Cependant cela peut parfois générer un effet pervers où l'on va se défausser entièrement sur lui de la question de la cybersécurité. Or, il n'est qu'un chef d'orchestre qui va mettre en musique les contributions de l'ensemble des collaborateurs, du stagiaire jusqu'à la direction générale. A ce titre, l'adoption de bonnes pratiques par chacun est primordiale.

Qu'en est-il justement de la relation de ces experts avec les dirigeants ?

La sensibilisation à la cybersécurité est l'une des responsabilités principales du RSSI. Mais il n'est pas toujours facile pour eux de toucher le *top management*. C'est une question de légitimité transversale qu'il faut construire, avec les bons arguments. Pour se voir ouvrir la porte des dirigeants et leur faire comprendre tout l'enjeu de la cybersécurité, les RSSI doivent pouvoir produire des analyses de risques, intégrant les mesures de l'impact métier/business des sujets, tout en assurant la coordination avec les équipes techniques et en s'assurant de la cohérence entre les pratiques de l'entreprise et sa politique de sécurité. Avantage : la majorité des RSSI ne sont plus ces « empêcheurs de tourner en rond » qu'on leur a souvent reproché d'être. Ils sont au contraire aux premières loges pour accompagner leurs dirigeants dans la transformation numérique de l'entreprise et la diffusion de ces pratiques d'innovation.

Jean-François Louâpre, vice-président du CESIN

Comment cela ?

La mission d'un RSSI est de faire passer les responsables dans l'entreprise d'un sentiment de peur, un peu flou et parfois irrationnel, à une démarche de gestion raisonnée des risques. Or, la gestion des risques et la prise de décision en conséquence, sont l'une des premières responsabilités d'un chef d'entreprise ! Pour saisir toutes les opportunités du numérique, il faut réfléchir en connaissance de cause, connaître les avantages comme les risques. Il en va ainsi pour des sujets comme le cloud ou la mobilité, porteur d'ouverture, de changement et donc bien évidemment de certains dangers. Mais qui doute par ailleurs qu'une force de vente mobile et connectée est aussi un avantage concurrentiel majeur ? Aujourd'hui, le message qu'un RSSI doit pouvoir adresser à son patron est : *Il faut innover, il faut avancer.* Principalement parce que le RSSI sait que les préoccupations, légitimes, en matière de sécurité, ne sont pas une raison suffisante pour rester attentiste et immobile dans un monde où tout change. Le RSSI doit aider les dirigeants à trouver le bon équilibre entre opportunités et risques.

Quels conseils donner aux dirigeants d'entreprises en matière de cybersécurité ?

D'abord, que le sujet n'est pas aussi complexe qu'ils le croient. Il est possible d'être des acteurs à part entière de la sécurité de l'entreprise même sans aucun bagage technique. C'est même une nécessité. En effet, les meilleurs outils et logiciels de protection sont inefficaces sans des usages adaptés et des comportements sûrs. Pour prendre un exemple très terre à terre : il est inutile de doter son entreprise d'une batterie de systèmes de cybersécurité si un collaborateur ou un dirigeant utilisent des mots de passe aussi peu sécurisé que « 12345 ». Aujourd'hui, réduire le risque d'une attaque par e-mail n'est pas qu'une affaire de technologie, c'est aussi du bon sens ! Un dirigeant exemplaire en matière de comportement sûr, entrainera dans son sillage toute l'entreprise.

Ensuite, le point fondamental pour assurer la protection de l'entreprise est la volonté managériale de le faire. Ce n'est pas qu'une question de budget, car il est devenu illusoire de vouloir protéger à 100% l'intégralité d'un système d'information, de plus en plus ouvert et complexe. Il s'agit d'évaluer de quel niveau de protection ont besoin les différents points clés de son activité. C'est une vision stratégique – en connaissance de cause des divers risques existants – qu'il faut déployer dans l'entreprise. Et c'est bien au *top management* de faire ces choix. Le RSSI lui, travaillera à traduire concrètement cette vision et à y sensibiliser tous les autres acteurs de l'organisation.

Incontournable RSSI, bras droit du dirigeant

Rude année 2014 pour le grand retailer américain Target. Après avoir subi un vol massif de données clients durant l'hiver, la DSI est poussée vers la sortie dès le mois de mars. Mais l'affaire n'est pas qu'informatique : Gregg Steinhafel, alors PDG, finit par démissionner lui-aussi au mois de mai. Stormshield (Arkoon/Netasq) explique pourquoi la cybersécurité est un sujet de dirigeant. ■ D.M

« *La cybersécurité ? Un domaine de purs techniciens.* » Cette vision généralisée en entreprise réduit la sécurité à des silos d'activité, confère une approche « rustine » à un sujet qui est pourtant un levier majeur et transversal de l'exercice entrepreneurial, et qui concerne jusqu'aux RH ou direction générale.

S'il n'y avait qu'un conseil à donner, ce serait : « *Chef d'entreprise, faites du RSSI votre bras droit !* » Cette confiance est nécessaire pour dépasser les antagonismes internes naturels : chaque service voit le sujet par le bout de sa lorgnette et peu se parlent. Alors, par exemple, la personne en charge de définir la politique de sécurité a rarement la maîtrise des solutions implémentées. Situation surprenante qui favorise un morcellement impropre à une défense « en profondeur ».

Les récentes attaques pointent – au-delà de la dimension technique – un manque flagrant de communication interne dans les entreprises concernées. Les premières déclarations des dirigeants ont révélé la nécessité pour eux de mieux appréhender les enjeux, de développer leur clairvoyance, car, au-delà de la technique, il est question de maintien d'activité économique et d'image de l'entreprise.

Alors, oui. La cybersécurité est une contrainte pour l'entreprise, il ne saurait en être autrement. Le but est d'intégrer ce constat et de travailler sa résilience. D'où la nécessité d'un référent impartial, le RSSI, qui puisse prendre en compte toute la chaîne de la sécurité, de la technique jusqu'aux usages. Et le dirigeant doit peser de son poids pour permettre à cette fonction de s'imposer, comme pour parodier la vision actuelle, tout en paraphrasant Clémenceau : « La cybersécurité est un sujet trop grave pour être confié (uniquement) à des techniciens ».

Petit à petit, la législation et les états d'esprit évoluent. Un exemple a fait date : l'affaire Target, durant l'hiver 2013-2014, a été révélatrice de cette nouvelle responsabilité pour le chef d'entreprise. Suite au piratage du système d'information et à la perte de millions d'identifiants de cartes bancaires, ce n'est pas seulement le DSI du groupe américain qui a été remercié, mais également son PDG, du fait d'une « faute de gestion ». *Dura lex, sed lex*, leur responsabilité est légitimement engagée, car, quand une entreprise est attaquée, outre les dégâts en propre qu'elle subit, elle impacte, par rebond, ses contacts commerciaux. L'exemple prouve que la protection du Système d'Information. est un enjeu écosystémique, donc une mission de dirigeant bien entouré. La cybersécurité prend du galon et devient sujet à part entière de la gestion de l'entreprise, de TOUTE l'entreprise.

« La cybersécurité est dorénavant vue comme un sujet à part entière de la gestion de l'entreprise. »

Pierre Calais
directeur général de Stormshield (Arkoon - Netasq)

Faire collaborer les hommes, et les outils

La collaboration est clé en cybersécurité. Dans la paradigme de la guerre moderne, une unité militaire tire sa force des communications sophistiquées entre ses membres. La transmission de l'information est vitale, aucun soldat ne doit être isolé, même séparé de son groupe. Il en va de même pour le système d'information de l'entreprise et les logiciels « soldats ». Un Système d'Information subira des attaques, c'est certain. La protection à 100% est peut-être un leurre, mais privilégier une réponse rapide et agile fera la différence en cas d'attaque. Les systèmes de protection ont vocation à dialoguer entre eux (*Multilayer Collaborative Security*), du réseau jusqu'au poste utilisateur, pour offrir la meilleure parade et une véritable défense en profondeur.

Attaques insidieuses : les directions en première ligne

« APT », le terme commence à être bien connu. Associé aux cyberattaques les plus insidieuses, c'est notamment une campagne menée par des hackers d'origine chinoise, pendant près de 4 mois contre les réseaux du New York Times*, qui a révélé le concept au grand public. L'entreprise de services numériques (ESN) SPIE Communications (groupe SPIE), décrypte ce que doit savoir un dirigeant sur la protection de son réseau. ■ D.M*

Avec le besoin d'être toujours plus compétitif et les enjeux de transformation digitale, les systèmes d'information des entreprises sont de plus en plus imbriqués avec ceux de leurs fournisseurs, partenaires et clients. Ce sont d'autant plus d'opportunités d'accès et d'exploitation de vulnérabilités pour les cybercriminels.

En cela, les APT (*Advanced Persistent Threat* ou attaques persistantes avancées) se caractérisent par un schéma d'attaque structuré, qui vise à nuire à une entreprise ciblée. Elles sont complexes à détecter dans la mesure où elles n'utilisent pas de méthode de diffusion générale et que les programmes malveillants sont masqués. Ces attaques peuvent s'appuyer sur différentes méthodes d'intrusion (infection d'une page web, d'un intranet partenaire, d'un fichier ou d'un lien web joint à un e-mail, infection via un fichier sur une clef usb…). L'objectif est de compromettre une première machine pour rebondir sur d'autres, et *in fine*, déployer le plan d'attaque final.

« Les APT sont complexes à détecter dans la mesure où elles n'utilisent pas de méthode de diffusion générale et que les programmes malveillants sont masqués. »

Pascal Mavric
responsable des activités infrastructures IP et sécurité, SPIE Communications

Envisager différemment la sécurité informatique

Pour répondre à cette nouvelle génération de cybercriminalité, il est nécessaire d'infléchir l'approche conventionnelle consistant à sécuriser les infrastructures réseaux « en silo ». En effet, la méthode de sécurisation très spécialisée « point par point » est limitée à la capacité intrinsèque de chaque système de sécurité (détection d'intrusion réseau, passerelle messagerie, proxy Web, …). De plus, elle ne propose pas de parade pour agir de façon rétroactive sur un programme malveillant qui aurait franchi les barrières de sécurité. En effet, cette possibilité doit faire l'objet d'une attention particulière. En raison de l'aspect protéiforme des attaques, aucune solution de sécurité ne peut prétendre être la parade absolue. Il est donc nécessaire d'intégrer cette donnée d'entrée pour réagir au plus vite et identifier rapidement l'impact de l'attaque en décryptant sa trajectoire.

Protéger le patrimoine et les infrastructures : du pragmatisme avant tout !

La sécurité des infrastructures doit être pensée comme un écosystème général, fonctionnel et vivant. Le sujet est donc intimement lié aux réalités quotidiennes et à la stratégie, aux spécificités, d'une entreprise. Il est donc recommandé aux directions d'entreprise de s'emparer du sujet, en faisant appel à des services sur mesure basés sur 3 points clés qui permettront d'assurer une sécurité permanente :

- Cartographier en temps réel tous les systèmes connectés au réseau de l'entreprise pour disposer d'une vision globale du contexte ;
- Disposer de systèmes de sécurité interactifs pour corréler dynamiquement l'activité observée avec le contexte et détecter les attaques ;
- Enregistrer l'activité des systèmes pour améliorer la connaissance sur les événements survenus et agir de façon rétroactive.

La mise en place de ces systèmes de sécurité pourra être réalisée sur site, à distance, de manière mutualisée ou en cloud selon les enjeux techniques, organisationnels ou réglementaires d'une entreprise. Cette capacité d'adaptation aux spécificités de chacun est une force pour un dirigeant qui souhaite protéger son organisation : les technologies de cybersécurité savent s'adapter à ses contraintes, lui permettant de se concentrer sur sa vision stratégique.

Le dirigeant face à la prise d'otage numérique

Une demande de rançon numérique ? Dévoilées dès 2011 avec le cas marquant du « Virus Gendarmerie » qui laissait penser à la cible que son ordinateur était bloqué par les autorités, ces attaques « ransomware » n'ont cessé d'évoluer jusqu'à devenir l'une des principales menaces ciblant particuliers et entreprises en 2015. Le spécialiste en cybersécurité Trend Micro analyse l'exemple de CryptoLocker, un malware champion du genre. ■ D.M

CryptoLocker est un *ransomware* de nouvelle génération qui contourne les politiques de sécurité des entreprises. Il a pour caractéristique de prendre les PC en otage jusqu'à ce que les utilisateurs payent une rançon ou obéissent à certaines instructions. CryptoLocker restreint en effet l'accès au système et affiche, de manière répétée, des messages incitant l'utilisateur à payer une rançon ou à réaliser une action spécifique. D'autres variantes chiffrent les fichiers du disque dur afin d'obliger les utilisateurs à payer pour pouvoir déchiffrer les fichiers importants auxquels ils souhaitent accéder.

CryptoLocker est donc ce qu'on appelle un *crypto-ransomware*, c'est-à-dire qu'il a pour objectif de chiffrer les fichiers. Pour ce faire, il utilise de nombreuses techniques et vecteurs (HTTPS, P2P, TOR…) pour masquer ses communications Command-&-Control (C&C).

De manière générale, cette attaque est menée en utilisant la méthode du *spear-phishing*, via un email contenant une pièce jointe infectée. Dans certains cas, l'infection s'effectue également via un site Web malveillant qui assure le téléchargement furtif du *malware* lorsqu'il est consulté. Lorsqu'exécuté, ce *malware* se connecte à différentes URL pour télécharger le crypto-ransomware et chiffre ensuite la quasi-totalité des documents de l'utilisateur. Il affiche alors une fenêtre avec un compte à rebours indiquant combien de temps il reste à la victime pour payer la rançon. Passé ce délai, la clé de chiffrement est soi-disant détruite.

Mais attention, un paiement ne garantit cependant en aucun cas la récupération des fichiers originaux. Certaines variantes permettent aux victimes de récupérer leurs fichiers, tandis que d'autres rendent la restauration des fichiers chiffrés quasiment impossible, même après que les cyberdélinquants aient récupéré la rançon. L'une des variantes du *malware* (TROJ_CRYPCTB.XX) offre par exemple aux utilisateurs la possibilité de déchiffrer 5 fichiers gratuitement, pour ainsi prouver que le déchiffrement et la récupération des fichiers sont possibles. Les utilisateurs disposent d'un délai de 96 heures, au lieu de 72, pour régler la rançon.

« La sensibilisation des utilisateurs est essentielle pour une défense pro-active. »

Loïc Guézo
Evangéliste Sécurité de l'Information pour l'Europe du Sud, Trend Micro

Comment réduire les risques ?

La meilleure approche face à ce type d'attaque est la prévention, notamment en maintenant l'environnement informatique à jour et en limitant ainsi le risque d'exploitation de vulnérabilités.

La sensibilisation des utilisateurs est essentielle pour une défense pro-active. Il faut en effet toujours vérifier l'email de l'expéditeur, rester vigilant vis-à-vis des emails contenant des pièces jointes (et ce même s'ils émanent ou semblent émaner de contacts connus) et éviter de cliquer sur les liens présents dans les emails.

Il pourra également s'avérer utile de disposer d'une solution de sauvegarde/restauration. Dans la majorité des cas, les fichiers cryptés sont perdus même si l'utilisateur règle la rançon. La restauration à partir d'une sauvegarde est la meilleure façon de retrouver ses fichiers originaux et non altérés.

Il est par ailleurs essentiel de disposer de solutions de sécurité proposant à la fois des fonctions anti-malware, d'analyse comportementale et de réputation Web. Neutralisant les emails malveillants ou suspects et en bloquant l'accès aux sites Web pirates, ces dernières empêcheront la diffusion du malware et protégeront les environnements qui ne sont pas encore infectés. En cas d'infection, il est également conseillé d'empêcher la réception ou l'ouverture de pièces jointes pour limiter les risques de nouvelles infections au sein de l'environnement.

En outre, il est important de tirer parti de la fonction de *sandbox* et d'analyse comportementale proposée par certaines solutions, qui détecteront ainsi les attaques CryptoLocker, les *ransomware*, les attaques ciblées, ainsi que les *malware* inconnus et leurs variantes.

Un projet d'informatisation des processus métiers

Babou choisit Trend Micro pour sécuriser tous les volets de son infrastructure informatique

Babou, enseigne spécialisée dans le discount, compte près de 100 magasins en France et au Portugal, totalisant 240 000 m² de surface de vente. La croissance de l'entreprise est à l'origine d'un vaste projet visant à adosser les opérations de l'enseigne à une informatique de nouvelle génération. En effet jusqu'en 2009, les processus métiers n'étaient pas informatisés, ce qui compromettait la visibilité de l'enseigne sur ses opérations.

La sécurité : au cœur du projet d'informatisation des processus métiers

En 2009, un projet pluriannuel est ainsi initié afin de recueillir l'ensemble des besoins et de définir un schéma directeur. Après des investissements logiciels destinés à accompagner les fonctions métiers (achats, stock, comptabilité, etc.), un data center privé est ensuite déployé en 2011 pour centraliser et virtualiser les postes de travail et capacités serveurs, mais également offrir les garanties essentielles en termes de disponibilité. Les magasins connaissent par ailleurs une refonte de leur environnement informatique aboutissant début 2013, aux premiers inventaires automatisés.

En 5 ans, Babou est ainsi passé à l'ère de la *Business Intelligence* : visibilité en temps réel des directeurs sur l'activité de leur point de vente, gestion du réassort de plus de 35 000 références d'articles en magasin, ou encore consolidation des données de performances de chaque magasin, consultables à distance, notamment depuis l'étranger. Alors que les projets de sécurité informatique sont souvent lancés de manière réactive et dans l'urgence, Babou inscrit la sécurisation des projets informatiques dès la définition de son schéma directeur. Dès 2009 David Legeay, DSI de Babou, choisit ainsi la solution OfficeScan de Trend Micro pour assurer la sécurité de près de 1 000 postes de travail fixes, dont les caisses autonomes présentes au niveau des magasins.

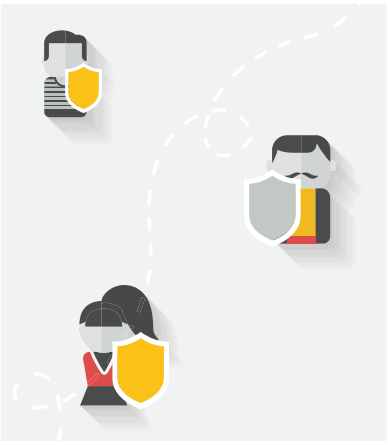
S'immuniser au plus tôt contre les attaques ciblées, capables de contourner les outils de sécurité classique

En 2013, Babou commandite un audit externe de sa sécurité pour valider le bien-fondé de ses investissements. Parmi les recommandations formulées : la nécessité de se prémunir contre les intrusions liées aux attaques ciblées. Après avoir étudié les offres du marché, Babou retient Deep Discovery Inspector de Trend Micro. Cette plateforme propose des moteurs de détection et des *sandbox* personnalisées qui analysent et identifient les *malware*, les communications C&C (Command & Control), ainsi que les comportements furtifs des assaillants non détectés par les outils classiques de sécurité. Favorisant la réactivité en cas d'attaque ciblée, la solution offre une défense personnalisée et en temps réel contre les assaillants. « *L'automatisation de l'analyse des logs constitue pour notre équipe IT, composée de 6 personnes, un gain de temps et d'efficacité considérable* », reconnaît David Legeay.

De la technologie, mais aussi une relation de confiance avec Trend Micro

Le renouvellement du contrat avec Trend Micro et PICA (partenaire de Trend Micro) pour une durée de 3 ans, étend par ailleurs la collaboration à la sécurisation de l'ensemble de l'infrastructure informatique de Babou de bout en bout. Babou opte alors pour la solution Deep Security au sein de ses environnements virtualisés, qui comptent près de 400 serveurs et 250 postes de travail. Protégeant les applications et données d'entreprise contre les risques de fuite de données et d'interruption d'activité, cette plateforme, ne nécessitant pas d'agent logiciel, permet de neutraliser les tentatives de piratage et d'augmenter ainsi la sécurité au niveau de chaque machine virtuelle.

« *Depuis plus de 4 ans, nous bénéficions d'un accompagnement de premier ordre de la part de Trend Micro, qui fait la différence sur un terrain essentiel : la relation client. L'entreprise a en effet su adapter son offre à l'ensemble de nos besoins, et cette flexibilité est totale, puisque nos contraintes budgétaires ont également été parfaitement respectées. D'autre part, la sécurité signée Trend Micro nous permet de faire évoluer nos technologies* », commente David Legeay.



Quand les entreprises laissent les pirates tirer parti des avantages mis à leur disposition

La célèbre cyberattaque sur TV5 Monde pourrait être l'œuvre de pirates beaucoup moins expérimentés que l'on ne le pense. En cause, des « tickets d'entrée » pour devenir un agresseur toujours moins chers, des « kits clés en main » pour mener des cyberattaques, ou encore l'automatisation de l'exploitation des failles répandues. Cyberwatch détaille comment les pirates tirent parti des informations que les autorités mettent à disposition des entreprises… et que celles-ci n'utilisent pas. ■ D.M

En 2014, les autorités comme l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ont publié près de 8000 alertes sur les failles informatiques. Ces alertes rejoignent la liste des « vulnérabilités connues » : ce sont des failles dans les logiciels les plus répandus, tels que les systèmes d'exploitation ou les sites internet utilisés par les professionnels. Ces alertes, publiques, contiennent les détails sur les vulnérabilités avec les méthodes d'attaque et les préconisations pour s'en protéger. Ces listes de vulnérabilité aident ainsi les autorités à lutter contre les cyberattaques en informant les usagers de leurs risques informatiques, et en indiquant comment se défendre. Pourtant, les statistiques montrent que ces alertes ne sont pas suffisamment suivies par les entreprises : sur un échantillon de 600 000 serveurs vulnérables à la faille Heartbleed, les experts d'Errata Security ont prouvé en 2014 que 300 000 n'étaient toujours pas protégés plus de deux mois après la publication de l'alerte. Cette faille majeure permettait de voler des données sensibles sur les serveurs, comme les mots de passe et codes de cartes bancaires. Or se protéger contre Heartbleed est une opération simple décrite par les autorités : le problème n'est donc pas dans l'accessibilité des alertes, mais dans le fait que trop peu d'usagers les consultent et appliquent les recommandations. Si les entreprises ont accès aux alertes pour se protéger, les pirates les consultent quant à eux pour améliorer leur arsenal. En septembre 2014, le groupe Solutionary a ainsi montré que les pirates sont capables de créer des robots d'attaque automatisés et de scanner Internet à la recherche de serveurs vulnérables moins de 24 heures après publication par les autorités…

« Si les entreprises ont accès aux alertes pour se protéger, les pirates les consultent quant à eux pour améliorer leur arsenal. »

Maxime Alay-Eddine
président, Cyberwatch

Heureusement, les entreprises disposent d'outils pour mieux se protéger contre les failles. Les plus répandus sont les scanners de vulnérabilité comme Nessus ou Nexpose, qui déterminent si un serveur est concerné par une alerte de sécurité. En cas de problème détecté, le scanner donne un lien vers les préconisations des autorités. L'utilisateur doit néanmoins effectuer lui-même l'opération de correction, ce qui demande quelques compétences en informatique.
Plus récemment, de nouveaux outils plus complets émergent : les correcteurs de vulnérabilité. Ceux-ci déploient directement les correctifs de sécurité appropriés contre chaque menace.
Ces solutions sont particulièrement intéressantes pour les entreprises qui souhaitent passer peu de temps sur le traitement des vulnérabilités, ou qui ne disposent pas d'un service informatique en interne.

Pour conclure, il existe maintenant des solutions simples et efficaces pour lutter contre les vulnérabilités. Ceci est particulièrement important dans un contexte législatif en mutation, qui obligera bientôt toutes les entreprises à communiquer les incidents et attaques informatiques dont elles seront victimes : la prévention sera alors la clé d'une bonne réputation.

Ne pas confondre vulnérabilité et virus

Contrairement à ce que l'on peut penser, les anti-virus et pare-feux ne protègent pas contre les vulnérabilités informatiques !
Les pirates profitent de cette erreur commune pour attaquer des cibles qui se croient protégées.
Pour se protéger contre les vulnérabilités, il faut connaître l'ensemble des technologies utilisées dans son entreprise et suivre les alertes des autorités, ou utiliser des outils de correction automatique.

Pour être efficace, luttez contre la complexité

A la question « comment mieux protéger son entreprise ? », chaque dirigeant peut avoir sa petite idée. De l'attaque sur le ministère de l'Economie en 2011 jusqu'à celle sur TV5 Monde en 2015, il ne fait aucun doute que les principales faiblesses d'une organisation sont dues à la complexité de son système d'information, à la fragmentation des solutions proposées, des responsabilités et de la gouvernance en place. Plutôt que de décrire une solution technique, le spécialiste Sophos préfère adresser aux dirigeants d'entreprise un encouragement à toujours penser la cybersécurité en termes de simplicité. ■ D.M

Des menaces de plus en plus pressantes

Il se passe rarement un mois sans que l'actualité nous rappelle la montée des menaces à la sécurité informatique : les intrusions touchant les sites Web ou la continuité de service, les fuites d'informations bancaires ou sensibles, les pertes de données dues aux *ransomwares* tels que CryptoLocker sont la partie visible des centaines de milliers d'attaques lancées chaque jour par les cybercriminels.

Bonne gouvernance et conformité

La plupart des attaques réussies pourraient être évitées par une bonne gouvernance en matière de sécurité informatique. Il faut s'assurer que tous les systèmes disposent d'une protection à jour, y compris les postes Mac, téléphones portables, tablettes et serveurs, vérifier que les derniers correctifs de sécurité sont bien déployés partout, bloquer les applications grand public à l'origine de failles de sécurité, mettre en place des accès Wi-Fi sécurisés, tester que les réseaux, les serveurs Web et la messagerie disposent de protections à l'état de l'art et garantir la confidentialité des données sensibles.

Le dirigeant peut et doit demander à ses services informatiques la mise en place d'une protection étendue, mais surtout des comptes réguliers sur la bonne application de la politique de sécurité.

Sécurité complète et simplicité sont les clés du succès

Devant la complexité et l'ampleur de la tâche, le manque de ressources et de temps est souvent à l'origine de défauts de conformité, sources d'intrusions. Beaucoup de PME et d'ETI n'ont qu'une seule personne en charge de la sécurité informatique, souvent aussi responsable de toute l'informatique. Même dans des structures disposant d'équipes sécurité conséquentes, nombre de fonctionnalités de sécurité importantes ne sont pas déployées partout, car trop complexes.

En matière de sécurité, la simplicité est donc essentielle.

Les interfaces d'administration doivent simplifier les tâches de gestion pour éviter les erreurs de configuration. Elles doivent faire gagner du temps, pour que l'administrateur puisse se concentrer sur ce qui est essentiel.

Les composants doivent être étroitement intégrés, pour offrir des processus fluides et une interface d'administration unique. Une gestion à travers le cloud, pour ceux qui le souhaitent, permet de gagner encore en simplicité, en s'affranchissant de la nécessité d'avoir à maintenir un serveur d'administration.

Le système de licences doit aussi être simple, pour accompagner les nouveaux usages. Une licence par utilisateur, quel que soit le nombre et la variété des systèmes utilisés, apporte une souplesse maximale dans un contexte de consumérisation de l'informatique (BYOD).

Enfin, le support technique doit être disponible, compétent et simple d'accès, car quand la sécurité est en jeu, la réactivité est indispensable.

En matière de sécurité, la simplicité est une vertu cardinale.

« Devant la complexité et l'ampleur de la tâche, le manque de ressources et de temps est souvent à l'origine de défauts de conformité, sources d'intrusions. »

Christian Pijoulat
vice-président Europe de l'Ouest, Sophos

Si on vous demandait où en est votre sécurité, que répondriez-vous ? Aujourd'hui, avoir une infrastructure de sécurité ne suffit plus... Vous devez vous ASSURER d'une SÉCURITÉ OPTIMUM. Une sécurité qui vous prémunit des attaques zero-day et protège vos données. Une sécurité qui garantit le meilleur taux de détection des menaces, en un temps record. Une sécurité qui assure la protection de vos données où qu'elles soient.

Cette SÉCURITÉ est offerte par CHECK POINT.

Check Point®
SOFTWARE TECHNOLOGIES, LTD.
WE SECURE THE FUTURE

En savoir plus ?

Sécurité des réseaux & infrastructures
Sécurité applicatives & des données
Sécurité mobile
Audit & recherche
Conseil & politique de sécurité

6cure
6cure est une société spécialisée dans le domaine de la détection et de la réaction aux cyberattaques, notamment les attaques DDoS. Grâce à sa solution Threat Protection®, 6cure garantit la disponibilité et la qualité des services de ses clients.
Françoise Clerc
sales@6cure.com / 06 64 08 28 75
www.6cure.com

Stormshield (Arkoon-Netasq)
Arkoon Netasq, une filiale à 100% d'Airbus Defence and Space, opère la marque Stormshield et propose tant en France qu'à l'international des solutions de sécurité de bout-en-bout innovantes pour protéger les réseaux, les terminaux et les données.
Sophie Schroeder
sophie.schroeder@stormshield.eu
06 86 66 12 76
www.stormshield.eu

Check Point
Check Point propose des solutions de pointe qui protègent les entreprises des cyberattaques, avec un taux de blocage inégalé des logiciels malveillants et autres types d'attaques, ainsi qu'une architecture de sécurité complète pour les réseaux et les appareils mobiles.
info_fr@checkpoint.com / 01 55 49 12 00
www.checkpoint.com

Cyberwatch
Cyberwatch est une entreprise de sécurité informatique créée en 2015, spécialisée dans l'audit et la gestion des vulnérabilités. Cyberwatch développe le premier logiciel de correction automatique de vulnérabilités sur les serveurs, disponible à partir de 29€/mois.
Maxime Alay-Eddine
maxime@cyberwatch.fr / 01 85 08 69 79
www.cyberwatch.fr

DenyAll
DenyAll est un expert en sécurité applicative de nouvelle génération, s'appuyant sur 15 années d'expérience dans la sécurisation et l'accélération des applications et services Web. Ses produits détectent les vulnérabilités informatiques, protègent les infrastructures contre les attaques modernes et connectent les utilisateurs aux services Web.
Gilles d'Arpa
gdarpa@denyall.com / 01 46 20 96 08
www.denyall.com

F-Secure
F-Secure est une société finlandaise spécialisée dans la sécurité informatique et le respect de la confidentialité. Son offre « Protection Service for Business » assure la protection, la sécurité et le patch management de tous les équipements de l'entreprise.
Olivier Mouly
olivier.mouly@f-secure.com / 06 33 60 58 87
www.f-secure.fr/business

GlobalSign
Créé en 1996, GlobalSign est une AC innovante et la 1ère établie en Europe. Ses solutions de sécurité numérique couvrent la protection des transactions, la gestion des identités (IoE) l'authentification des contrôles d'accès, la sécurisation des e-mails et les échanges de documents sur Internet.
Etienne Bertrand
ventes@globalsign.fr / 09 75 18 32 00
www.globalsign.fr

LINKBYNET
LBN Shield favorise la croissance de ses clients et garantit la Disponibilité, l'Intégrité et la Confidentialité de leurs données. LINKBYNET met en œuvre, supporte et administre des solutions fiables et innovantes qui s'adaptent à votre environnement.
Kareen Frascaria
k.frascaria@linkbynet.com / 01 48 13 00 00
www.linkbynet.com

Nware
Intégrateur en Infrastructure & Cybersécurité, Nware propose Nsecure360 contre les attaques via les collaborateurs et applicatives via le web, monitorant l'ensemble avec tableaux de bord pour des alertes temps réel. Intégrant des logiciels certifiés Anssi, NSecure couvre 25% des 40 principes d'hygiène informatique.
Evelyne Bourderioux
evelyne.bourderioux@nware.fr
06 82 80 76 62
www.nware.fr

Rubycat-Labs
Editeur de logiciels spécialisé dans la traçabilité numérique et le contrôle d'accès au SI. L'offre PROVE IT complète votre politique de sécurité en incluant la traçabilité et le contrôle des utilisateurs à privilèges, via la supervision et la consolidation du déroulement des connexions sensibles.
Cathy Lesage
contact@rubycat-labs.com / 02 99 30 21 11
www.rubycat-labs.com

Sophos
Sophos est le premier éditeur européen de solutions de sécurité informatique pour les entreprises. Nos solutions protègent les données, les systèmes, les mobiles, le Web, la messagerie et les réseaux de plus de 100 millions d'utilisateurs dans 150 pays.
Christian Pijoulat
info@sophos.fr / 01 34 34 80 00
www.sophos.fr

SPIE Communications
Entreprise de Services Numériques majeure pour la transformation digitale des ETI et des grands comptes, de l'environnement utilisateurs jusqu'au data center, SPIE Communications (groupe SPIE) facilite les usages informatiques, la productivité et l'exploitation des systèmes d'information.
Pascal Mavric
pascal.mavric@spie.com / 01 41 46 41 46
www.spiecom.com

Trend Micro
Leader mondial des logiciels et solutions de sécurité, Trend Micro sécurise les échanges d'informations numériques pour le grand public, les professionnels ou les institutions gouvernementales, que ce soit sur les équipements mobiles, les Endpoint, les passerelles, les serveurs et le Cloud.
sales@trendmicro.fr / 01 76 68 65 00
www.trendmicro.fr

50 acteurs de la cybersécurité à suivre

Bien que fragmenté, le marché de la cybersécurité a le vent en poupe. Les performances en Bourse des entreprises du secteur sont ainsi particulièrement saluées et Bank of America Merrill Lynch place le sujet au sein de ses 7 thématiques d'investissements phares pour 2015. La médiatisation grandissante des cyberattaques contribue par ailleurs à une prise de conscience généralisée des enjeux pour les entreprises… et leurs dirigeants. Appelés à se montrer de plus en plus proactif en la matière, ces derniers n'ont pas fini de voir le thème de la sécurité se mêler à la transformation numérique de leurs organisations.
Pour se familiariser avec ces sociétés qui entendent répondre aux inquiétudes des chefs d'entreprise, *Alliancy le mag*, dresse ci-dessous une liste de 50 acteurs à suivre.

Sécurité des réseaux & infrastructures · Sécurité mobile · Conseil & politique de sécurité
Sécurité applicatives & des données · Audit & recherche
Orange : nouveaux entrants sur le marché · ⊙ Prix de l'Innovation des Assises de la Sécurité 2014

3M	@3MScreens			●		
6cure	@6cure	●				
Akerva	@Akerva_FR	●	●		●	●
aleph-networks	@alephnetworks1	●	●		●	
Avast Software	@avast_FR		●	●		●
Balabit IT Security	@balabit	●				
Bitdefender	@BitdefenderFR	●	●	●		
BlueCoat	@bluecoat	●		●		
CheckPoint Software	@CheckPointFR	●	●	●		
CipherCloud	@ciphercloud		●			
Cisco Systems	@CiscoFrance	●				
Colombus Consulting	@colombus				●	●
CyberArk	@CyberArk	●	●		●	●
Cyberwatch	@cyberwatch_team	●				
Dell Software	@DellSoftware	●	●	●	●	●
DenyAll	@DenyAllSecurity		●			
Dimension Data	@DimensionDataFr	●	●	●	●	●
Drooms	@drooms_software		●			
EfficientIP	@efficientip	●				
Fortinet	@Fortinet	●				
F-Secure	@FSecureFrance	●	●	●		
GMO GlobalSign	@GlobalSign_FR	●	●	●		
HP	@hpsecurity	●	●	●	●	●
IDECSI ⊙	@Idecsi		●			
Intel Security	@IntelSecurity	●	●	●	●	●
Intrinsec	@Intrinsec_Secu	●	●	●	●	●

IS Decisions	@IS_Decisions	●	●			
Kaspersky Lab	@kasperskyfrance	●	●	●		
LEXSI	@lexsi	●	●	●	●	●
LogRhythm	@LogRhythm	●				
Mirca	@MIRCA_France				●	●
Nomios	@NomiosFR	●	●	●	●	●
NTT Com Security	@NTTComSec_FR	●	●	●	●	●
Nware	@Nware_Officiel	●	●	●	●	●
OZON	@ozon_io		●			
Prim'X Technologies	@ITSecurFeed	●	●	●		
Return Path	@ReturnPath_FR		●	●		
SCC	@SCC_info	●	●	●	●	●
Siemens SAS	@Siemens_France	●	●	●	●	●
Sophos	@SophosFrance	●	●	●		
SPIE Communications	@SPIEgroup	●	●	●		
Stormshield	@Stormshield_	●	●			
The GreenBow	@thegreenbow	●	●	●		
Trend Micro	@TrendMicroFr	●	●	●	●	
VASCO Data Security	@VASCODataNews		●	●		
Verizon Enterprise Solutions	@VZEnterprise	●	●	●	●	●
WatchGuard	@WatchGuard_FR	●	●	●	●	●
Wooxo	@Wooxo_		●			
Zepla	@Zepla		●			
Zscaler	@zscaler	●	●	●		

Un oubli ? Vous souhaitez figurer dans la prochaine liste « Les acteurs à suivre » ? Rendez-vous sur ALLIANCY.FR/50-acteurs-cybersecurite