IMPÔTS : L'ANNÉE BLANCHE ? • CYBERSÉCURITÉ : LA MENACE FANTÔME

Forbes

CLASSEMENT
LES MEILLEURS AÉROPORTS

DOMINIQUE DESSEIGNE
LAURA FLESSEL
DOMINIQUE CERUTTI
ISABELLE KOCHER
BERTRAND PICCARD
ANNE-SOPHIE PIC

LA REDOUTE
DEUX ENTREPRENEURS LA RESSUSCITENT

SPORT BUSINESS
LES STARS LES PLUS RENTABLES

RONALDO • MESSI • NEYMAR • GRIEZMANN • POGBA • MBAPPÉ

EMMANUEL MACRON • DONALD TRUMP
NATHALIE COLLIN • CLARA GAYMARD
GUILLAUME POITRINAL • VITALIE TAITTINGER • JEAN TODT

Belgique : 9,50 € - Luxembourg : 9,50 € - Suisse: 16,20 CHF
M 03507 - 3H - F: 9,00 € - RD

La cybermenace fantôme

Le cybercrime paie, plus que jamais. Le piratage de musiques et de films est largement dépassé. Le but aujourd'hui peut être de détourner des millions lors de transactions financières, d'obtenir le paiement de rançons très élevées, de fabriquer frauduleusement de la cryptomonnaie, de nuire à des concurrents, de truquer des élections voire de discréditer un gouvernement.

PAR **PIERRE MANGIN**, FORBES

OH, LES 'RANSOMWARES' (OU RANÇONGICIELS), comme le célèbre WannaCry, bien que stabilisés ou en baisse, n'ont pas disparu et les sommes récoltées ne sont pas négligeables. Ainsi, durant l'été 2017, d'après la société canadienne Cytelligence, une grande firme nord-américaine a accepté de payer 425 000 dollars canadiens en bitcoins pour récupérer ses données[1]. Leur propagation est due à un 'botnet' (un réseau 'robot' constitué d'ordinateurs zombies, contaminés par un 'trojan' ou cheval de Troie). C'est le cas de Necurs, qui aurait déjà infecté 5 millions d'ordinateurs dans le monde. Une singularité à noter : ce dernier ne s'exécute pas lorsque le poste visé est paramétré en… russe.

En juin 2017, plusieurs institutions d'Ukraine ont été victimes de cyber-attaques, dont celles utilisant 'NotPetya' contre des sites web mais ressemblant à des 'ransomwares'. Le pays a mis en cause son voisin, la Russie. En février 2018, parallèlement à l'affaire de l'empoisonnement de l'ex-agent russe Sergueï Skripal, Londres a explicitement repris cette accusation contre la Russie, accusant l'armée russe d'être « *très probablement responsable de la cyber-attaque* ». Les Etats-Unis lui ont emboîté le pas, ainsi que l'Australie, la Nouvelle Zélande et le Canada. La France s'est abstenue (comme elle le fait généralement).

La dimension internationale est de plus en plus souvent mise en avant et brouille la distinction entre cybercriminalité et cyberguerre. L'agence de presse allemande DPA a révélé fin février 2018 que des cybercriminels avaient réussi à pénétrer le réseau informatique du Bundestag, le parlement fédéral à Berlin. Ce réseau porte les échanges entre le parlement, la chancellerie, la Cour des comptes, les ministères et les services de sécurité. Les attaquants, désignés sous les noms de Fancy Bear, APT28 / 29, TURLA ou Tsar Team, seraient liés au renseignement russe. Ces entités auraient attaqué TV5 Monde, mais également la convention démocrate lors de l'élection présidentielle américaine et déjà en 2015, le Bundestag. La Russie a toujours nié.

PC, smartphones, scanners IRM, casques VR…

Les cyber-attaques d'Etat suivent les aléas des tensions diplomatiques. Lors de l'inauguration des JO d'hiver de Pyeongchang en Corée du Sud, le site web, dont l'infrastructure était gérée par le français Atos, a été durement éprouvé durant plusieurs heures. Les soupçons se sont portés plutôt vers la Russie (quasiment exclue des JO pour dopage) que vers la Corée du Nord. Le malware identifié, baptisé 'Olympic Destroyer' utilisait en effet un mode de

1 Ces ransomwares muent. Les dernières versions s'introduisent via des PDF. La moyenne des paiements obtenus en 2017 serait de 522 dollars.

propagation proche de BadRabbit et NotPetya, généralement attribué à la Russie…

L'univers de la finance reste régulièrement visé par ces attaques DDOS (sortes de bombardements de requêtes mettant à genoux les serveurs d'accès) mais l'univers high-tech n'y échappe pas. Ainsi, en France, à plusieurs reprises depuis septembre 2016, l'hébergeur OVH a fait l'amère expérience de charges atteignant 1,5 To/s (soit 1 500 Gigas/s !) provenant de 10 000 sources différentes issues de 1 600 systèmes autonomes. Beaucoup proviennent des botnets Pbot ou Mirai, mais des dérivés plus sophistiqués apparaissent (Reaper, IOTroop).

Les smartphones ne sont pas épargnés – de nombreux utilisateurs en France ont été la cible du malware Locky, capable d'envoyer des emails avec des pièces jointes piratées, ou du logiciel espion Skygofree qui aspire les données et permet la prise de contrôle (accès 'root'). Même les appareils médicaux - appareils de radiographie, scanners IRM - peuvent être infectés. Depuis 2015, c'est la spécialité d'un groupe de hackers, Orangeworm. Pour des activités d'espionnage visant des sociétés multinationales, il installe le 'malware' 'Kwampirs'. Le but premier, selon Symantec, serait d'apprendre comment ces appareils fonctionnent.

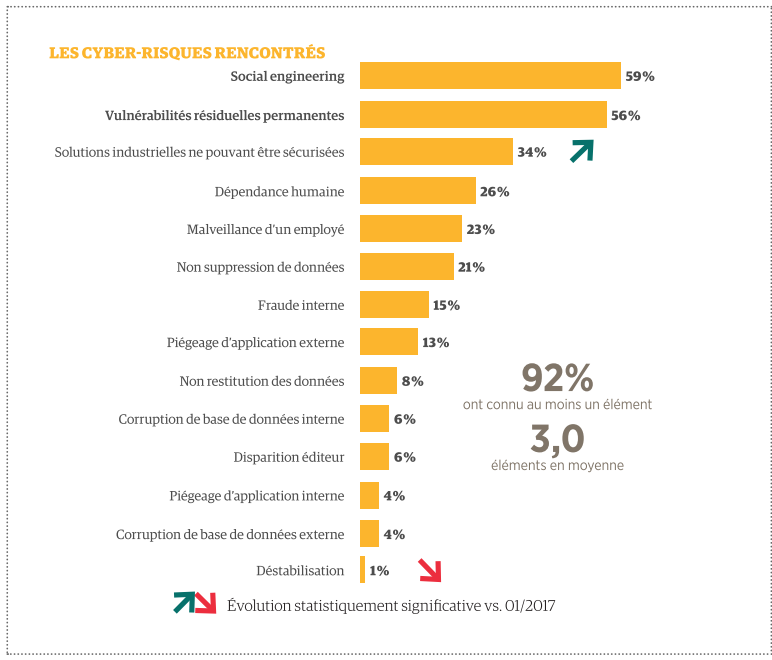
Les casques de réalité virtuelle sont, eux aussi, victimes de vulnérabilités dans le kit de développement 'OpenVR'. Il y a là aussi danger : les contenus affichés au joueur, dont la délimitation de l'espace physique, pourraient être modifiés à son insu.

… et surtout, crypto-monnaies

Mais depuis quelques mois, les cybercriminels se sont massivement orientés vers le nouveau terrain de jeu que sont les crypto-monnaies ou 'crypto-actifs' (terme recommandé par la Banque de France). Selon Ernst & Young, plus de 10% des fonds provenant de levées de fonds en crypto-monnaie ou ICO (Initial coin offerings) - forme de 'crowdfunding' qui utilise la 'blockchain' (comme le fait le Bitcoin) – ont été perdus ou volés par des pirates informatiques. Le seul fonds 372 ICO a perdu 400 millions de dollars sur les 3,7 milliards collectés entre 2015 et 2017.

« *En moyenne, les pirates volent 1,5 million de dollars de crypto-monnaie chaque mois* », constate le rapport Sécurité 2017 de Symantec.

Parmi les éléments suivants liés à la cyber-sécurité, quels sont ceux auxquels votre entreprise a été concrètement confrontée au cours des 12 derniers mois (142 répondants) SOURCE: CESIN



« *L'essentiel des vols est dû à du 'phishing'* » (ou hameçonnage).

Ainsi, les cybercriminels s'exercent désormais au cryptojacking, qui consiste à lancer des exécutions de « *minage* » ou fabrication de crypto-monnaie, à l'insu des possesseurs d'ordinateur - le minage ('mining') résultant de longues opérations d'encryptage/décryptage et nécessitant des ressources informatiques conséquentes. Or, détourner des ordinateurs pour faire du 'mining' est plus simple que d'installer des virus. Et même les ordinateurs relativement bien protégés peuvent être « *agrippés* » lors d'une simple visite sur un site web, comme Showtime (pour fabriquer la crypto-monnaie Monero). Apple vient de retirer de l'AppleStore l'application Calendar 2 qui permettait de « *miner* » de la monnaie subrepticement. Pour l'utilisateur, cela se traduit par un ralentissement de l'ordinateur et une surchauffe subite de l'appareil et de sa batterie, assez vite repérable.

Tous les ordinateurs sont des cibles potentielles. En février, Securityweek relatait qu'un logiciel d'exploitation de stations d'épuration en Europe, d'origine General Electric, était porteur d'un agent pirate de crypto-monnaie. ●

EN MOYENNE, **LES PIRATES VOLENT 1,5 MILLION DE DOLLARS** DE CRYPTO-MONNAIE CHAQUE MOIS

Forbes ARRIVE EN FRANCE

BULLETIN D'ABONNEMENT

Forbes Magazine

Je m'abonne à Forbes Magazine, Edition française
Parution trimestrielle

☐ **1 an / 4 numéros** : 30 € au lieu de 36 €

☐ **2 ans / 8 numéros** : 50 € au lieu de 72 €

Je règle par chèque à l'ordre de :
360 BusinessMedia (société éditrice de Forbes France)

Mes coordonnées

☐ Mme ☐ Mlle ☐ Mr

Nom : .....

Prénom : .....

Société (facultatif) : .....

Adresse : .....

.....

Code Postal : .....

Ville : .....

E-mail : .....

Tél. : .....

A compléter et à envoyer accompagné de votre réglement à :
Forbes France - 33 rue Galilée - 75016 Paris
E-mail : info@forbes.fr

Protéger les données et les processus critiques : vers une Security By Design

Le RGPD nous impose et nous apprend à penser la « privacy by design ». Si les points de vue de l'entreprise et celui des « personnes concernées » peuvent différer, les mesures de protection convergent, dans l'intérêt de tous. Cause commune donc pour le security and privacy by design !

PAR **MYLÈNE JAROSSAY**, CISO DU GROUPE LVMH

L'ENTREPRISE ÉTENDUE A **BESOIN DE PARTAGER UN SYSTÈME D'INFORMATION** SÉCURISÉ ET FIABLE

LA CYBERSÉCURITÉ a pour principal objectif de protéger l'information qui a de la valeur pour l'entreprise, parce qu'elle soutient sa stratégie, parce que cette protection est nécessaire à la conformité réglementaire, mais aussi parce que cette protection, lorsqu'elle concerne des individus, apporte la confiance nécessaire à la relation entre l'entreprise et ces personnes. Si l'information était divulguée ou altérée, cela aurait un impact négatif sur la réputation de l'entreprise, sur le lien tissé entre l'entreprise et ses clients, ses salariés, ses actionnaires, ou encore ses partenaires.

Même si l'effervescence autour de l'application du RGPD fait que les efforts du moment se concentrent sur la protection des données, la cybersécurité se doit aussi de protéger les processus critiques de l'entreprise car ceux-ci sont de plus en plus intimement liés au système d'information. Des incidents sur le SI peuvent entraîner de très fortes dégradations de ces processus. Cette dépendance au SI dépasse d'ailleurs les frontières de l'entreprise. Il faut considérer l'entreprise étendue, un écosystème avec des partenaires et sous-traitants au niveau des métiers et du SI lui-même, notamment des offreurs de solutions dans le nuage. Cette entreprise étendue a besoin de partager un SI sécurisé et fiable.

Dans un contexte complexe

Le challenge actuel est de protéger des processus et des données qui s'appuient sur des systèmes morcelés, disséminés, éparpillés, avec une surface d'attaque considérablement augmentée, une dimension spatiale et organisationnelle telles que les cartographier devient trop complexe.

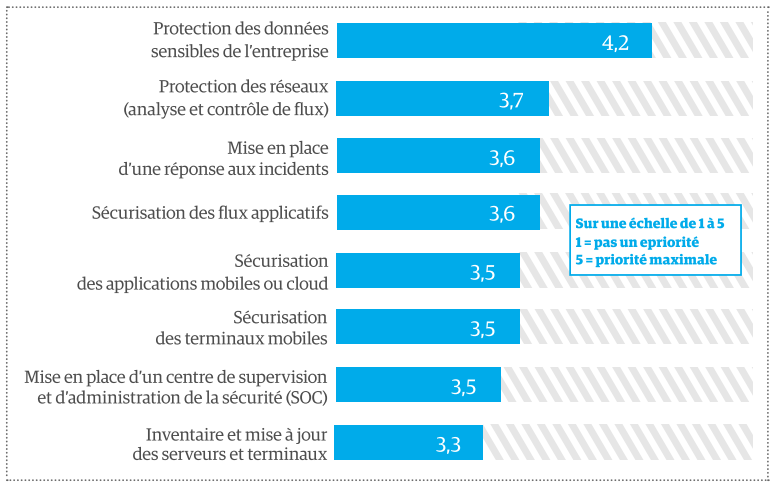
En ajoutant l'axe temporel de la transformation digitale, qui construit des solutions sur des cycles très courts, il devient illusoire de pouvoir faire le tour complet du propriétaire avant de juger de la protection la mieux appropriée.

D'autant qu'il n'est question, ici, que de protéger ce qui est connu, sans intégrer, par définition, le « *shadow IT* ». Même flous, les contours de ce dernier laissent présager que nombreux sont ceux qui succombent aux sirènes des offreurs de systèmes d'information à monter soi-même, dont le modèle économique premier consiste à capter les données, souvent illégitimement et quelquefois illégalement.

La bonne nouvelle, peut-on penser, est qu'une

© THANANIT

Priorité des entreprises en matière de sécurité pour les 18 prochains mois SOURCE: IDC/IBM, 33 GRANDS COMPTES FRANÇAIS (07/2017)



constellation de « *petites* » solutions préserve d'une dépendance à un système unique, avec des impacts potentiels forts s'il était corrompu ou indisponible. Sauf que ces solutions s'appuient souvent sur une intégration plus ou moins maîtrisée de la sécurité des briques d'infrastructure des mêmes poids lourds du cloud public avec leur propre écosystème, étendu et complexe. Double peine d'une intégration dangereuse et de la dépendance.

L'exercice difficile consiste à identifier, retrouver et protéger ses pépites du moment, dans une topologie inextricable et mouvante. Les attaquants profitent largement de l'allure indescriptible de cet ectoplasme informationnel et de l'asymétrie intrinsèque entre eux et les défenseurs. Entre deux lutteurs à mains nues, les armes étaient égales. Le défenseur d'un village avait fort à faire pour bloquer toutes les issues sans compter les menaces internes qu'il fallait débusquer. Sur des SI désormais protéiformes aux multiples points d'entrée, l'attaquant est nettement avantagé par rapport au défenseur. Sans compter que le défenseur doit aussi réagir à des attaques dont il n'est pas la cible première, juste un dommage collatéral, colocation dans le cloud oblige.

Les outils de la défense

Pour répondre à ce contexte de risques, la cybersécurité s'appuie sur du contractuel et sur des organisations, des processus et des moyens techniques. Plus les systèmes sont répartis auprès d'acteurs du cloud, plus la part contractuelle prend son importance, car il s'agit d'acheter un service et non plus de bâtir des architectures en propre. L'évaluation de la maturité en matière de sécurité des prestataires et des solutions ainsi que la sécurisation des contrats sont essentielles et vertueuses. Elles concourent à l'amélioration continue des solutions et permettent d'écarter celles qui présentent des risques inacceptables. Néanmoins, les moyens contractuels peuvent parfois se heurter à des questions de niveaux de responsabilités pour les petits prestataires et de capacité de contrôle des plus gros.

Les stratégies de défense se déroulent selon trois grandes phases, premièrement avec des moyens de prévention et protection, puis des mécanismes de surveillance et de détection, et enfin des dispositifs de réponse à incident et de résilience pour rétablir l'activité nominale. Du vaccin au traitement de choc, en passant par un suivi diagnostique régulier.

La prévention et la protection constituent une part fondamentale indispensable. A condition de s'efforcer de bien isoler et protéger les actifs les plus critiques car la surface d'attaque ne permet plus une couverture complète. Il ne faut >>>

SUR DES SYSTÈMES D'INFORMATION PROTÉIFORMES AUX MULTIPLES POINTS D'ENTRÉE, **L'ATTAQUANT EST NETTEMENT AVANTAGÉ** PAR RAPPORT AU DÉFENSEUR.

>>>

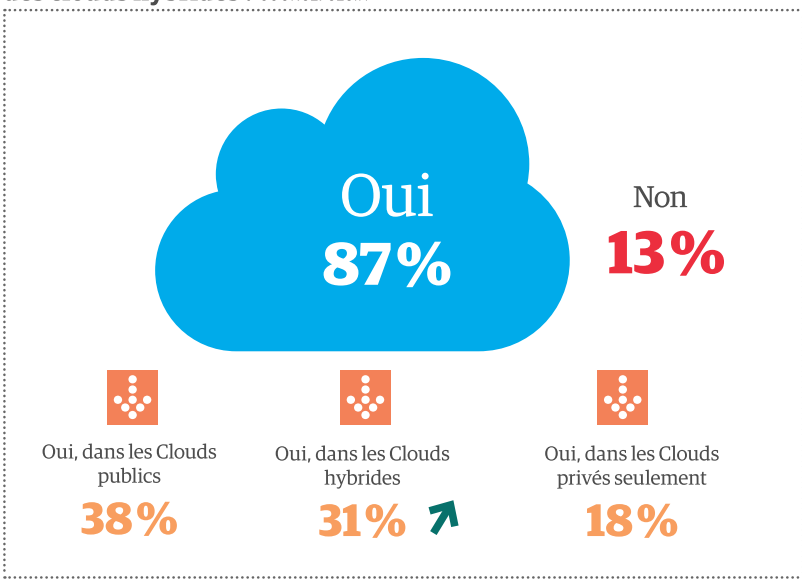
pas diluer ses dispositifs de protection et prendre le risque de l'homéopathie et de la perméabilité.

La surveillance et la détection, à travers la mise en place de Cyber SOC, jouent un rôle de plus en plus déterminant dans les stratégies de défense. Repérer les signaux faibles et prendre le remède dès que le symptôme est là pour être en mesure de faire le bon diagnostic et apporter une réponse immédiate et ciblée plutôt que se protéger au hasard.

En aval, les mécanismes de réponse à incident et de cyber-résilience sont les derniers remparts pour sécuriser les activités métiers. Lorsque les SI étaient des monolithes hébergés dans des infrastructures majoritairement locales ou privées, l'effort se concentrait sur la construction de datacenters redondants. La réplication permettait de basculer, dans le meilleur des cas, d'un datacenter sur son clone en cas de sinistre. Les nouveaux SI mettent à mal les traditionnels plans de reprise d'activité.

Il s'agit maintenant de savoir maintenir son activité si tel ou tel composant critique du SI disparaissait complètement sous une cyber-attaque destructrice. Il s'agit également de repérer les intersections sensibles entre différents composants. Il s'agit enfin de répartir ses ressources avec des solutions alternatives indépendantes et fondées sur des technologies autres. La proposition de la cyber-résilience est en ligne avec les nouveaux SI disséminés qu'elle protège. Elle joue la carte de la dispersion et de la diversification. Ceci afin de pouvoir rebondir avec agilité d'une solution sur une autre, sous le pilotage d'un RSSI urgentiste.

Certaines des données de votre entreprise sont-elles stockées dans des clouds hybrides ? SOURCE: CESIN



Vers une security by design

L'essentiel pour tous ces dispositifs de sécurité, quel que soit le moment pendant lequel ils entrent en jeu, est qu'ils soient pensés dès qu'un nouveau projet est envisagé. La « *security by design* » est l'atout maître du défenseur. Déterminer les enjeux et la bonne prescription dès le début, avec une implication du propriétaire métier concerné, permet de faire de la sécurité un élément natif de la solution. Cela permet de mettre des moyens proportionnés et pertinents au regard des risques, de bien régler le curseur au plus près des enjeux métiers. Cela permet aussi d'éviter une sécurité tardive qui risque d'agir comme un couperet, face à l'innovation.

Il se trouve que les dispositifs de sécurité tendent à être en ligne avec les solutions qu'ils protègent. Ils sont souvent réalisés dans le cloud, peu intrusifs et agiles, faciles à monter et démonter. Ils exploitent des grandes quantités de données, notamment des journaux d'activité, en s'appuyant sur des techniques de big data. Ils recourent à des ressources distribuées et à la demande. Les programmes de bug bounty en sont une illustration. Enfin, ils utilisent des techniques de renseignement et de profilage. L'analogie se poursuivra si les promesses du machine learning et de l'intelligence artificielle sont tenues.

Dans tous les cas, la sécurité by design ne se fera pas sans expert. Il faut des experts pour faire de l'analyse de risques, pour des développements sécurisés, pour concevoir des architectures solides, pour bien configurer les outils, pour auditer, exploiter, surveiller, gérer les crises et réparer. Il faut des experts dans les équipes sécurité. Il faut aussi de l'expertise sécurité parmi ceux qui conçoivent les nouvelles formes de nos SI. La sécurité ne doit pas être seulement autour des solutions, mais également logée à l'intérieur. ●

LA « SECURITY BY DESIGN » EST **L'ATOUT MAÎTRE DU DÉFENSEUR**

Le dilemme du RGPD

Entré en vigueur depuis quelques jours, le Règlement européen de protection des données pose à toutes les entreprises une question cruciale. Comment gérer la transformation numérique des organisations dans un environnement réglementaire de plus en plus complexe ?

PAR **PHILIPPE COURTOT,** CEO ET PRÉSIDENT DE QUALYS

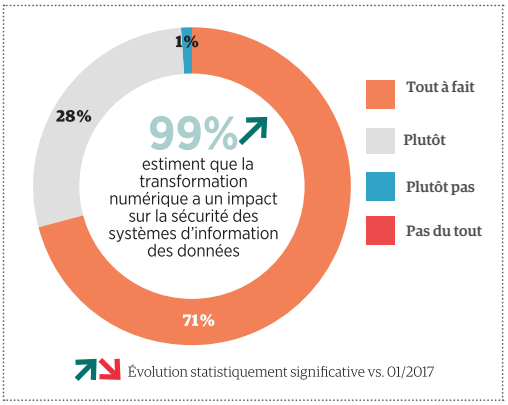
REDÉFINIR LES OUTILS DE PRÉVENTION ET D'ANALYSE

LA TRANSFORMATION NUMÉRIQUE DES ENTREPRISES – l'utilisation du cloud computing, de la mobilité, de l'internet des objets et d'autres nouvelles technologies pour rendre les organisations plus innovantes, agiles et flexibles – devrait mobiliser 6 000 milliards d'euros dans le monde, selon l'analyste IDC. Cet avènement est d'abord une chance, nécessitant toutefois anticipation, adaptation et vigilance car elle est en même temps source de vulnérabilités et de menaces multidimensionnelles considérables, capable de créer des crises mondiales.

Simultanément, les gouvernements élargissent la réglementation. Partout dans le monde, les organisations doivent désormais savoir quelles sont les données personnelles des résidents de l'Union Européenne, où elles sont stockées, avec qui elles les partagent, comment elles les protègent et à quoi elles les utilisent. Le règlement général de protection des données de l'Union européenne (RGPD) exige également une réponse rapide aux demandes des résidents européens, y compris la suppression, ou le transfert de leurs renseignements personnels. Les violations de données doivent être signalées dans un intervalle de 72 heures. Les organisations doivent également prouver qu'elles ont obtenu le consentement des citoyens dont elles traitent les données et s'assurer que les tiers avec lesquels ils partagent des données - fournisseurs, partenaires - se conforment aux exigences réglementaires.

La confluence de ces deux tendances oblige les organisations à accélérer leur transformation numérique et à repenser la sécurité comme un enjeu de performance qui peut s'avérer vital. Or, il n'est pas raisonnable de continuer à ajouter des solutions de sécurité pour chaque nouvel environnement ou réglementation.

Dans votre entreprise la transformation numérique a-t-elle un impact sur la sécurité des systèmes d'information et des données ? (142 répondants) SOURCE: CESIN



Il devient donc nécessaire de couvrir les nouveaux besoins réglementaires à partir d'une seule et même plate-forme qui apporte une vue unique aux responsables informatiques, aux équipes de sécurité et auditeurs de conformité. Cela suppose de redéfinir les outils de prévention et d'analyse en se tournant vers des architectures et des solutions basées sur des architectures cloud qui permettent de visualiser, partager et automatiser en permanence à la fois la posture de sécurité et de conformité.

Cette tâche est complexe car les initiatives de transformation numérique introduisent de nouvelles applications et des services Web en constante évolution qui génèrent, collectent et analysent des quantités massives de données client. La visibilité complète de leur environnement informatique hybride - sur site, dans le cloud et sur les terminaux mobiles - est désormais primordiale pour surveiller et sécuriser en continu ces ressources informatiques et afin de gérer les risques et la conformité. ●

La souveraineté des données : une nouvelle bataille perdue ?

La souveraineté numérique n'est pas une préoccupation nouvelle mais force est de constater que, sur le plan du matériel, la bataille semble définitivement perdue tandis que sur le plan logiciel, même si quelques pépites européennes et françaises tentent de s'imposer, le paysage est largement dominé par les logiciels étrangers et singulièrement américains. Reste la souveraineté des données...

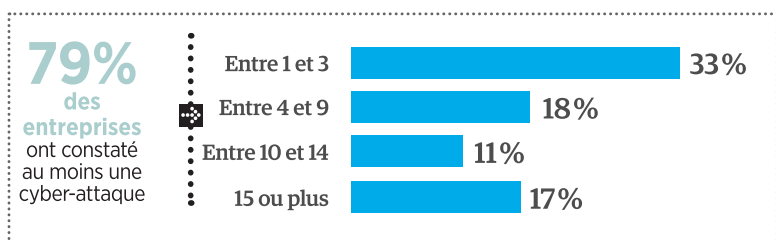
PAR **ALAIN BOUILLÉ,** PRÉSIDENT DU CESIN (CLUB DES EXPERTS DE LA SECURITE DE L'INFORMATION DU NUMÉRIQUE)

LA SOUVERAINETÉ DES DONNÉES est devenue une préoccupation forte au début de la décennie 2010 avec les affaires d'espionnage américain via le numérique. Chaque acteur averti pouvait se douter de leur existence mais les révélations du lanceur d'alerte Edward Snowden ont mis en lumière un véritable arsenal qui reposait sur une connivence des grands acteurs numériques avec les services secrets américains. Un des programmes révélés par Snowden en 2013, PRISM, indiquait que la NSA disposait d'un accès direct aux données hébergées par les géants américains des nouvelles technologies de l'époque et que l'on n'appelait pas encore les GAFAM, à savoir, Google et YouTube, Apple; Facebook, Microsoft, mais aussi Yahoo, Skype, AOL… La mise en œuvre de ce programme remontait à 2007, dans le cadre des mesures prises après les attentats du 11 septembre 2001. Le recours aux services du cloud public n'avait pas atteint, à l'époque, le niveau où nous le connaissons aujourd'hui. Même si les grandes entreprises ont été marquées par ces révélations, elles ne se sont pas, pour la plupart, senties concernées, n'ayant pas encore confié massivement leurs données à ces acteurs. Les préoccupations se sont plutôt concentrées sur les données privées, que chacun d'entre nous avait déjà très largement confiées aux futurs GAFAM via les réseaux sociaux et les messageries essentiellement. Plus de dix ans après, cette collecte est désormais arrêtée, ou tout du moins présentée à l'arrêt — le programme PRISM est toujours en vigueur, mais sous une nouvelle forme.

La législation américaine, s'appuyant notamment sur le Patriot Act, le FISA Amendments Act et plus récemment le Cloud Act, impose désormais aux acteurs américains du numérique de fournir sur demande les données électroniques de personnes ou entités non américaines dont ils disposent. Un des articles du FISA Amendments Act s'applique particulièrement aux acteurs du cloud computing comme Microsoft, Google, Amazon… Il les contraint à fournir sur demande les données hébergées dans leurs datacenters, qu'ils soient localisés aux États-Unis ou ailleurs à l'étranger. Les annonces d'ouverture de datacenters en France ne diminuent en rien les risques car leurs opérateurs demeurent de nationalité américaine, certes soumis aux lois françaises mais aussi aux lois de leur pays d'origine. Cette situation est aujourd'hui considérée comme un risque majeur pour la souveraineté des données européennes par le Parlement Européen. L'expression « *colonie numérique* » concernant l'Europe vis-à-vis des États-Unis revient régulièrement dans les discours. Mais quand allons-nous passer du discours aux actes ? Depuis plusieurs années, >>>

UN VÉRITABLE ARSENAL, **QUI REPOSE SUR UNE CONNIVENCE DES GRANDS ACTEURS** NUMÉRIQUES AVEC LES SERVICES SECRETS AMÉRICAINS

Un grand nombre d'entreprises touchées par des cyber-attaques cette année SOURCE: CESIN

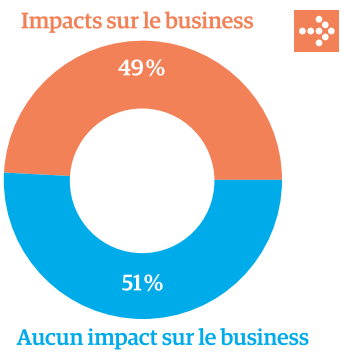


CONTRAINDRE LES ACTEURS AMÉRICAINS À METTRE EN PLACE UN CLOUD SOUVERAIN EUROPÉEN

>>> les services hébergés dans le cloud progressent fortement auprès des entreprises, de par les bénéfices qu'ils apportent : pas d'investissement initial, simplification de la gestion opérationnelle, flexibilité de tarification, scalabilité des infrastructures, richesse des traitements… Mais force est de constater qu'en la matière les offres souveraines ne sont pas légion et pour les services les plus prisés comme Office 365 proposé par Microsoft, la seule offre concurrente sérieuse est proposée par… Google !

Sans minimiser les problématiques de la protection des données privées des citoyens, le sujet de la protection des données sensibles des entreprises est de plus en plus préoccupant. Les citoyens peuvent encore choisir des opérateurs nationaux pour leurs messageries personnelles ; ils peuvent aussi décider de ne pas dévoiler leur vie privée sur les réseaux sociaux, mais quel choix se présente pour les entreprises en matière de solutions digitales modernes et évolutives? En septembre 2016, Microsoft indiquait que 32 groupes du CAC 40 avaient opté pour sa suite bureautique en mode cloud. Ces entreprises sont informées des risques d'espionnage, elles ont probablement mené des analyses de risques par leurs spécialistes sécurité qui ont envisagé des solutions de chiffrement voire des solutions hybrides où la part des utilisateurs la plus sensible de l'entreprise resterait « *on premises* » c'est-à-dire hébergée en interne. Mais la réalité est que les solutions de sécurisation diminuent drastiquement l'expérience utilisateur. Une donnée chiffrée avec des clés de chiffrement conservées par l'entreprise empêche l'hébergeur/éditeur d'y avoir accès. Du coup ce dernier ne peut plus indexer ces données pour offrir des services à valeur ajoutée et bien souvent la réaction de l'utilisateur est de déclassifier sa donnée pour profiter de tous les services proposés. De même, les solutions dites hybrides sont généralement là pour rassurer le dirigeant mais la réalité est que les deux mondes (celui sensible resté «*on premises*» et celui moins critique externalisé dans le cloud public) continuent à communiquer, et des informations sensibles se retrouvent ainsi dans le cloud public, la plupart du temps en clair.

Des cyber-attaques qui dans un cas sur deux ont un impact correct sur le business des entreprises touchées SOURCE: CESIN



Indisponibilité du site Internet pendant une période significative

Arrêt de la production pendant une période significative

Perte de CA

Retard sur la livraison auprès des clients

Autre

Impact jugé non significatif

Contraindre les GAFAM à créer des clouds souverains

Alors que faut-il faire ? Accepter les risques pour profiter pleinement des services offerts par les acteurs du cloud ? Les révélations de Snowden, les ingérences dans les processus électoraux qui ont bien involontairement mis récemment Facebook et son dirigeant dans la lumière interdisent toute naïveté. Mais est-il encore temps de développer des géants technologiques européens pour une véritable mise en concurrence ? D'ici là, leur restera-t-il des entreprises à servir ? Il convient peut-être de s'inspirer de ce qu'on fait les Chinois et, plus proche de nous, les Allemands, en contraignant les acteurs américains à mettre en place un cloud souverain.

Dans ce modèle, c'est un opérateur local obéissant à la seule loi locale qui opère pour le compte des éditeurs américains comme tiers de confiance des données, en prenant la responsabilité de protéger les données des clients. Toutes les données sont accessibles et traitées exclusivement par du personnel local, dans un datacenter local. Dans ce cas les acteurs américains n'auront donc pas accès à ces données, et seront dans l'incapacité de les fournir sur injonction des autorités américaines.

Encore faut-il que de telles solutions voient le jour au niveau européen : la souveraineté des données devrait se concevoir à l'échelle européenne et plus seulement nationale. Mais pour cela il faut un niveau d'implication fort des États européens avec des exigences claires en matière de souveraineté des données vis-à-vis des entreprises sensibles, et des pressions vis-à-vis des GAFAM bien plus contraignantes qu'elles ne le sont aujourd'hui. ●