CIO.FOCUS

CYBERSÉCURITÉ :

Menaces évidentes, menaces cachées

EN BREF

Les entreprises sont menacées lorsque leur SI l'est. Si certaines menaces sont évidentes, d'autres le sont moins ou sont négligées. Et les risques encourus sont alors importants. Les très classiques attaques DDOS (par déni de service) ou les exploitations de failles pour pénétrer le SI demeurent d'actualité. Mais les cybercriminels usent aujourd'hui d'ingénierie sociale pour pousser les utilisateurs à la faute.

Pour faire le point sur le sujet, CIO a organisé une Matinée Stratégique « Cybersécurité : Menaces évidentes, menaces cachées » le 28 février 2017 à Paris.

Pour toute demande concernant CIO.focus :
contact-cio@it-news-info.com

Une publication de IT NEWS INFO :
40 bd Henri Sellier 92150 Suresnes

Rédacteur en chef :
Bertrand Lemaire
blemaire@it-news-info.com
Tél. : 01 41 97 62 10

Principaux associés :
Adthink Media et International Data Group Inc.

Président et Directeur de publication :
Bertrand Gros

Directeur général : Jean Royné

Président du groupe Adthink Media : Sylvain Morel

CIO est édité par **IT NEWS INFO**,
SAS au capital de 3000000 €

Siret : 500034574 00029 RCS Nanterre

SOMMAIRE

Le 28 février, CIO a organisé une Matinée Stratégique « Cybersécurité : menaces évidentes, menaces cachées » à Paris.

/ STRATÉGIE

Cybersécurité : contrer les menaces évidentes comme les menaces cachées

En partenariat avec HP, Ivanti, Juniper, Level 3, VMware et Nomios, CIO a organisé une Matinée Stratégique « Cybersécurité : menaces évidentes, menaces cachées » le 28 février 2017 à Paris. Témoins et experts sont intervenus pour présenter les meilleures pratiques déployées en entreprises.

Les indispensables bonnes pratiques en matière de cybersécurité ont été présentées lors de la Matinée Stratégique « Cybersécurité : menaces évidentes, menaces cachées » organisée par CIO à Paris le 28 février 2017 en partenariat avec HP, Ivanti, Juniper, Level 3, VMware et Nomios. Experts et témoins RSSI s'y sont succédés, présentant tour à tour un état de l'art mais surtout la réalité concrète dans les grandes entreprises exemplaires.

Malheureusement, les bons exemples ne sont pas toujours suivis. C'est ce qu'ont montré les résultats de l'étude Cybersécurité : quelles mesures pour contrer quelles menaces ? réalisée en ligne par CIO auprès de ses lecteurs. Ceux-ci ont été présentés en avant-première en ouverture de la conférence.

La transformation digitale change la donne

Et, en plus des problématiques classiques, la transformation digitale en cours vient ajouter sa pierre dans la question de la cybersécurité. Ghaleb Zekri, NSX Senior Systems Engineer EMEA chez VMware, intervenant pour VMware et Nomios, a constaté : « les entreprises veulent le meilleur des deux mondes : une meilleure expérience utilisateur (interne ou clients) mais aussi un business sécurisé. » l'IT dans les entreprises évolue de simple moyens et ressources vers un vecteur business et de compétitivité, ouvrant les possibilités aux applications métiers (traditionnelles ou nativement cloud) à être hébergés on premise, dans un cloud privé,

Ghaleb Zekri, NSX Senior Systems Engineer EMEA chez VMware, intervenant pour VMware et Nomios, a expliqué : « Pourquoi la transformation digitale nécessite une transformation de la sécurité ? »

Michael Bittan, associé France Cyber Risk Services Leader chez Deloitte Conseil a présenté des « Chiffres et cas avérés en cyber-sécurité : faire face aux risques cyber ».

« Cybersécurité : les nouvelles menaces, comment s'en protéger ? » a interrogé Alain Khau, Director Security Sales Specialist South EMEA chez Level 3.

dans un cloud managé ou dans un cloud public pour être consommées par les utilisateurs au travers de de tout types de terminaux. Le challenge est que, une fois que tout est mis en oeuvre, la sécurité est souvent « la dernière invitée » comme l'a déploré Ghaleb Zekri. Enfin, comparaison faite par rapport aux attaques modernes qui se distinguent en quatre phases (infitration, propagation, extraction et exfiltration des données), le modèle de sécurité traditionnelle reste périmétrique : 80 % du budget sont consacrés à lutter contre l'infiltration, 20 % sur les 3 dernières phases d'une cyber-attaque (propagation, extraction, exfiltration). De ce fait, comme il l'a pointé : « dès le périmètre franchi, c'est open-bar pour les attaquants. C'est la raison pour laquelle il faut transformer la sécurité pour permettre une protection de bout en bout, au plus proche de l'application en gardant une indépendance du système qui la porte (pour éviter le cas échéant un risque d'être compromise si ce dernier est attaqué). L'hyperviseur représente l'environnement idéal pour appliquer ce nouveau modèle d'architecture de sécurité appliquant le principe de micro-segmentation sans compromettre l'agilité. »

Les innombrables attaques massives auxquelles les entreprises doivent faire face ont été décrites par Michael Bittan, associé France Cyber Risk Services Leader chez Deloitte Conseil. Pour lui, un leitmotiv s'impose : « la sécurité doit être intégrée au business, pas être une surcouche qui tente de dire non alors que le ComEx a dit oui. »

Nouvelles menaces, nouvelles approches

Parmi les menaces, certaines sont nouvelles par leur approche. Quand on est un opérateur, pouvoir revendiquer de voir passer 60 à 70 % du trafic Internet mondial à un moment donné sur ses infrastructures, on les voit forcément passer... et on se doit de les arrêter, tout comme les attaques classiques. Par exemple, Alain Khau, Director Security Sales Specialist South EMEA chez Level 3, a cité le blocage de serveurs de Commande et Contrôle qui pilotent les réseaux de zombies. Au travers de l'étude

du trafic sur les réseaux, « nous avons une visibilité en temps réel sur les cybermenaces » a-t-il précisé car, pour lui, « on ne peut pas se protéger de ce que l'on ne voit pas ». Il faut donc identifier et stopper les ennemis avant qu'ils n'atteignent le coeur des infrastructures.

Yann Pugi (CISO de Monext, vice-président du Clusir PACA), Stéphanie Buscayret (RSSI groupe Latecoere) et Farid Illikoud (CISO du PMU) ont ensuite participé à la première table ronde de la matinée. Ils ont chacun témoigné sur les méthodes mises en oeuvre dans leurs entreprises pour se protéger des menaces nouvelles sans négliger les classiques.

Lutter contre l'ennui

L'un des risques majeur en matière de cybersécurité, c'est l'ennui. Car l'ennui entraîne la négligence. Et la négligence permet au loup d'entrer dans la bergerie. Et quoi de plus ennuyeux que des imprimantes ? Après tout, les multifonctions actuels ne sont guère que de véritables ordinateurs avec disque dur, micrologiciel (BIOS), des panneaux de configuration, des ports USB, des possibilités de scanner des documents papier dont la version électronique seule est protégée... Pour contrer l'ennui, il faut recourir à des surveillants qui ne s'ennuient jamais, c'est à dire qu'il faut robotiser la surveillance. « Et les Legacy Printers, les vieilles imprimantes, ont juste des failles dans le BIOS qui sont connues mais aux correctifs jamais appliqués » a dénoncé Alex Huart, consultant pour HP Inc.

Alex Huart, consultant pour HP Inc., a détaillé « Comment sécuriser ses périphériques d'impression ? »

La sécurité est comme une assurance

La cybersécurité, cela peut sembler coûteux. « C'est comme une assurance : parfois on se demande pourquoi on paye, jusqu'à ce qu'un problème survienne » a déclaré Vincent Peulvey, EMEA South Pre-Sales Manager d'Ivanti. Il a donné un exemple qui a fait les gros titres : Yahoo vient de perdre 350 millions de dollars sur sa revente à cause de ses incidents de cybersécurité. Pourtant, quelques contrôles doivent simplement être réalisés, tels que : l'inventaire des biens matériels autorisés ou non, l'inventaire des logiciels autorisés ou non, la sécurisation des configurations logicielles et matérielles, l'évaluation et la correction continues de la vulnérabilité et le contrôle de l'utilisation des privilèges. Pour Vincent Peulvey, il faut comprendre avant de protéger, détecter et agir.

« Sécurité : évitez de faire les gros titres ! » a conseillé Vincent Peulvey, EMEA South Pre-Sales Manager d'Ivanti.

Grand témoin de la matinée, Olivier Ligneul, CTO et Group CISO chez EDF, a présenté la « vision des vrais RSSI » regroupés au sein du CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) dont il est le vice-président. Il est bien placé pour le faire car son employeur affronte à la fois les problèmes de cybersécurité « grand public », liés aux interactions clients B2B comme B2C, mais aussi ceux plus « industriels », en lien avec l'outil de production électrique.

Automatiser une réponse 360°

Face à toutes les facettes de la cybersécurité, comment traiter tous les problèmes potentiels ? « Une des réponses est l'automatisation pour les tâches quotidiennes récurrentes sans valeur ajoutée mais avec un fort risque d'erreur humaine » a plaidé Ramyan Selvam, expert cybersécurité Juniper Networks. Parmi les automatisations possibles, il y a les mises en quarantaines des terminaux soit suspects soit effectivement infectés, non seulement sur leur adresse IP mais aussi sur leur adresse MAC afin d'éviter qu'un terminal à isoler ne « riposte » en basculant sur un autre réseau (un wi-fi domestique par exemple). Enfin, la Matinée Stratégique a été conclue par une table ronde « Les nouvelles réponses à apporter par le RSSI » ayant réuni Arnaud Tanguy (CISO d'AXA Investment Managers), Philippe Fontaine (RSSI du Groupe SMA) et Farid Illikoud (CISO du PMU).

Les sponsors de la conférence (HP, Ivanti, Juniper, Level 3, VMware et Nomios) et les participants ont pu échanger à l'accueil, à la pause de mi-matinée et au cocktail déjeunatoire autour des stands de chaque partenaire et des buffets.

UN ARTICLE RÉDIGÉ PAR
Bertrand Lemaire, Rédacteur en chef de CIO

Olivier Ligneul, CTO et Group CISO chez EDF, Vice-Président du CESIN, a réalisé une intervention sur « La cybersécurité chez EDF, l'opinion du CESIN »

« Automatisez la détection, automatisez la contre-mesure » a plaidé Ramyan Selvam, expert cybersécurité Juniper Networks.

La table ronde « Les nouvelles réponses à apporter par le RSSI » a réuni, de gauche à droite, Arnaud Tanguy (CISO d'AXA Investment Managers), Philippe Fontaine (RSSI du Groupe SMA) et Farid Illikoud (CISO du PMU).

/ STRATÉGIE

Michael Bittan (Deloitte) : « Il ne s'agit pas d'être anxiogène, mais de bien montrer l'étendue des nouvelles menaces ».

Lors de la Matinée Stratégique « Cybersécurité : menaces évidentes, menaces cachées » organisée par CIO le 28 février dernier à Paris, Michael Bittan, associé et directeur de la practice cybersécurité de Deloitte Paris, a analysé la situation en ouverture.

Michael Bittan, associé et directeur de la practice cybersécurité de Deloitte Paris, a témoigné sur la Matinée Stratégique CIO consacrée oar la cybersécurité.

En ouverture de la Matinée Stratégique sur la cybersécurité organisé par CIO, Michael Bittan, résumait ainsi son intervention : « Il ne s'agit pas d'être anxiogène, mais de bien montrer l'étendue des nouvelles menaces ». Ce qu'il fit, un brin provocateur, en déroulant chiffres, exemples et analyses. Des chiffres issus de différentes études françaises, internationales, concernant aussi bien les PME que les grands groupes.

Premier chiffre, livré par le ministre de la défense Jean-Yves Le Drian, celui des cyberattaques externes bloquées en France en 2016 : 24 000. Une entreprise sur deux perçoit les attaques de plus en plus puissantes et 92% d'entre elles ont fait l'objet d'une intrusion au cours des cinq dernières années. C'est clair, notre quotidien est fait de cybersécurité.

« Pour réagir, il y a des fondamentaux, comme l'anticipation, la meilleure défense c'est bien l'attaque, on doit anticiper et analyser pour se préparer à répondre, de manière simple, et à prendre des mesures aussi bien organisationnelles qu'humaines.

La stratégie et la gouvernance des risques cyber est importante. « Mais beaucoup de ces stratégies ne sont pas forcément très pragmatiques, le but est que la stratégie soit très concrète et fasse l'objet d'une étude de maturité de l'entreprise. Elle ne doit pas être un frein, passer sous un empilement de couches de produits. Aujourd'hui, les boards des grandes entreprises nous posent la question de l'empilement de différentes solutions. L'analyste a affirmé : « on travaille sur une stratégie où le RSSI met les budgets là où il en a vraiment besoin ».

Anticiper et faire évoluer

La formation est aussi très importante et doit faire partie de la stratégie et de la gouvernance. Souvenons-nous de l'exemple de Grooping Elephant qui a réussi à dérober les données sensibles en exploitant du social engineering et du malware. Mais le maintien en conditions opérationnelles, les mesures de sécurité efficaces ne sont possibles que si on anticipe et on a la capacité à les faire évoluer au quotidien.

Quelques chiffres marquants pour parler de violation de données. Selon Verizon, 63% des violations de données se font avec usurpation d'identités, en utilisant la faiblesse des mots de passe, leur vol, ou bien l'utilisation de mots de passe par défaut. Selon le même rapport, 66% des mauvais usages concernent les abus de privilèges. La cybersécurité est bien le premier rempart, et la gestion des identités la clé, ce qui implique de modifier les process et l'organisation de l'entreprise, et d'impliquer les RH avec une conduite du changement. Trop de mots de passe finissent sur des post it ou à proximité, mais il faut être en capacité de simplifier la vie des utilisateurs.

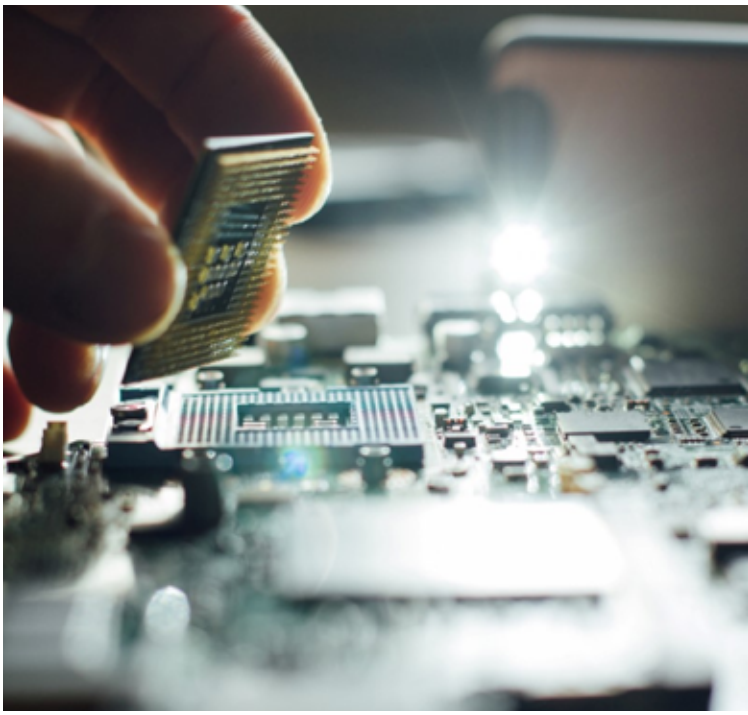
« Autre sujet, évidemment, la transformation digitale, qui est extrêmement galvaudée : on veut avoir accès par des tablettes et des smartphones aux applicatifs, ce n'est possible que si une gestion des identités est suffisamment forte dans votre entreprise » a-t-il continué. Des attaques DDOS en 2016 ont par exemple rendu l'accès à Airbnb ou à Spotify difficile, l'utilisation de l'IoT peut se révéler problématique en termes de sécurité.

La sécurité ne peut être un frein

« J'enfonce encore une porte ouverte », glisse parfois Michael Bittan dans son intervention. Une personne dans l'assistance l'interpelle d'ailleurs : « ça fait dix ans que vous, ou d'autres, dites la même chose et rien ne change ». « Effectivement, ça ne change pas, ça évolue et ça grossit, les usages et les besoins évoluent, le business aussi. La sécurité ne peut être un frein au développement des activités et business ».

Le niveau de sécurité doit être adapté, on doit s'adapter, à la transformation, aux usages, au business et aux RH qui peuvent être potentiellement attaqués et corrompus, on ne doit pas les bloquer, on doit accompagner le business et en anticipant ce qui peut se produire, faire l'analyse de la sécurité applicative.

On a aussi la partie cyberintelligence, ce que vous trouvez comme informations sur le darknet, le social engineering. Tout celà peut se faire dans des labs, les grands groupes se structurent autour d'un lab, les collaborateurs font par exemple de l'audit de codes, des tests d'intrusion, ils veulent un accompagnement différent avec un scénario lié aux métiers, aux techniques et au social engineering, mais avec des scénarios propres à leur activité.



En vente sur le darknet

La compromission de données est également prégnante avec 1093 compromissions de données personnelles enregistrées en 2016, uniquement sur des évènements rapportés. Autre chiffre, 36,6 millions de données personnelles sont ne vente sur le darknet, mais 50,7% des compromissions de données personnelles connues ne référencent pas le nombre d'enregistrements ayant été exposés. En fait, on se fait attaquer, on perd des données et on ne sait pas précisément ce qu'on a perdu.

Sujet d'actualité, le GDPR est évidemment au premier plan. « Nul ne peut ignorer la loi ! Les RSSI et leurs entreprises doivent faire face à nombre de règlementations, comme la Loi de programmation militaire, la LMP pour les OIV. Concernant GDPR, dont la dead line se rapproche, il faut garder en tête la nécessité de préserver le patrimoine informationnel, il faut absolument une vision pas seulement cyber ou SI, il faut pouvoir accompagner les différents métiers et le business, il faut une vision technique d'abord, mais aussi RH, juridique, data, et une vision globale dans l'entreprise de la compliance ».

Finalement, quel rôle joue vraiment la cybersécurité dans l'entreprise ? Quelques chiffres : 18% des organisations ont expérimenté un défaut dans leur SI en ligne interne ou externe dans les derniers 12 mois, 79% des décideurs redoutent une crise d'ici 12 mois, 59% des décideurs ont déjà géré une crise dans leur organisation, et 10% de ces organisations anticipent un défaut de sécurité dans leur SI, en ligne ou interne dans les douze prochains mois.

Gérer l'imprévisible

La cybersécurité apporte une solution à l'imprévisibilité, on peut être pro actif, assurer la continuité d'activité et la gestion de crise, mais sans regarder uniquement la technique. L'humain est très présent, comment on déplace ses collaborateurs ? Comment faire face aux attaques virales ? RPCA et RSSI se parlent-ils ?

Avant un datacenter était une garantie, maintenant le fait de basculer vers ces centres ouvre beaucoup d'incertitudes, en propageant plus facilement d'éventuelles failles. La gestion de crise entre également ne ligne de compte, une faille si elle est connue peut déboucher sur une amplification médiatique.

Souvenons-nous de Sony, une intrusion dans les serveurs a entraîné la compromission de 25 millions de comptes utilisateurs. Ces serveurs hébergeaient des jeux de rôles multi-joueurs. Plus tard, les services du réseau Playstation et Qriocity ont été compromis, faisant 77 millions de victimes. Ce qui a nécessité trois semaines de suspension d'activité et une perte financière de 171 millions de dollars.

Dernier thème traité par Michael Bittan, celui de l'industrialisation du piratage. Avec des facilités d'attaques et de surfaces sans cesse plus importantes. Un outil de hacking simple coute 1367 dollars, à la portée d'un groupe d'étudiants. Les systèmes industriels connectés sont vulnérables à 92%. Et nous aurons 50 milliards d'objets connectés d'ici cinq ans !

UN ARTICLE RÉDIGÉ PAR
Didier Barathon, Journaliste

Michael Bittan, associé et directeur de la practice cybersécurité de Deloitte Paris, a témoigné sur la Matinée Stratégique CIO consacrée oar la cybersécurité.

/ STRATÉGIE

2016 s'est plutôt bien passée pour les RSSI

Lors de la Matinée Stratégique « Cybersécurité : menaces évidentes, menaces cachées » organisée par CIO le 28 février 2017, trois RSSI, ceux de Latécoère, Monext, et du PMU ont livré leur vision des menaces lors d'une première table ronde.

Comment avez-vous vécu l'année 2016 ? Avec quelles menaces nouvelles et quelles ripostes ? Trois RSSI étaient conviés à livrer leur perception du sujet et leur retour d'expérience lors de la première table-ronde lors de la Matinée Stratégique « Cybersécurité : menaces évidentes, menaces cachées » organisée par CIO le 28 février 2017 : Stéphanie Buscayret, responsable de la sécurité du système d'information du Groupe Latécoère, Farid Ilikoud, Chief information security and compliance officer au PMU ainsi que Yann Pugi, Ciso de Monext et vice-président du Clusir Paca (il a été récemment promu RSSI Groupe du Crédit Mutuel Arkéa).

Trois cas dans trois secteurs différents : un industriel, Latécoère, une grande entreprise de jeu dédiée au grand public, le PMU, une entreprise traitant les moyens de paiement, Monext.

Tout va plutôt bien, en fait...

« Au risque de faire le rabat-joie, lance d'emblée Stéphanie Buscayret, l'année 2016 c'est très bien passée. Je risque de ne pas paraître assez anxiogène pour les vendeurs de produits, mais bon, ça s'est plutôt bien passé parce qu'on avait anticipé, on voit beaucoup de choses comme les ransomwares ou les DDoS. On les avait anticipés, notamment les ransomwares qui sont très basiques. On fait aussi des choses très simples, par exemple chez moi les ports USB des PC sont tous bloqués, il y a quelques exceptions sur des devices utiles pour les métiers, mais chez moi les clés USB ne se connectent pas sur mes machines ».

Latécoère présente également un profil à part, avec des préoccupations très industrielles. La société a seulement cinq clients, évidemment des grands de l'aéronautique. Si on pénètre dans l'entreprise on entre chez ses clients. « C'est contraignant. On a fait beaucoup de pédagogie, toujours dans la logique de prévention du ransomware. On a fait ce qu'on peut appeler « démapper » les lecteurs réseaux de nos utilisateurs, pour retrouver « leurs petits » dans les fouillis de leurs filers on leur a fait changer leurs habitudes pour trouver des raccourcis. Donc, il est désormais moins facile pour les ransomwares de se propager. En 2016, on a eu, en tout et pour tout, quatre occurrences de ransomwares. Quatre uniques, trois sur des PC portables de commerciaux et un sur un PC de la production. On n'a pas eu d'interruption de production. Les ransomwares on les détecte une fois qu'ils sont là, après, on ne peut plus travailler. Au final, pour répondre à votre question, en 2016 on n'a pas connu de déni de service, pas de gros problème, je suis désolé, ça s'est bien passé » !

Le tryptique : technologie, humain, process

Pour sa part, Farid Illikoud, chief information security and compliance officer, au PMU, est sur la même ligne. « Globalement, beaucoup de choses ont été dites, je les partage. On ne dit pas que les menaces n'existent pas, on investit beaucoup sur la technologie, mais nous sommes surtout attentif au tryptique : la technologie, l'humain, le process. Sans les trois, on ne va nulle part. Ensuite, effectivement, quand je dis l'humain c'est pour faire le lien avec l'ingénierie sociale et l'humain reste (encore) le maillon faible de nos organisations. On ne fait pas de sensibilisation sur un terrain anxiogène, mais en lui apportant une métaphore, pour lui montrer comment il agirait dans la vraie vie. Exemple, si toute la boite mail est « pourrie » par un ransomware, si on n'y accède plus, tout de suite on lui met l'image de ses comptes bancaires et de ses photos de famille, ou de vacances, volées, on amène l'utilisateur sur le terrain de sa vie privée, ce qui permet de faire 50% du chemin. Autre sujet, on a parlé très vite tout à l'heure de PCA, au sens plan de continuité d'activité, nous c'est un chantier sur lequel on a beaucoup investi l'année dernière. La continuité d'activité est un élément critique dans le cadre du SI, et le PCA cyber diffère du PCA, c'est autre chose, on parle de l'intégrité de la donnée, de la confidentialité des données dans le PCA cyber, c'est spécifique au risque de sécurité ».

« Troisième élément, dans le monde du jeu, notre principale menace c'est le déni de service, très clairement, si nous subissons une heure d'interruption de service, c'est 20 ME de CA perdus, c'est juste inacceptable. Chez nous, et plus globalement dans la e-economie, le client est volatile, il va chez le meilleur offreur lorsqu'il souhaite jouer, et n'hésitera pas à aller vers la concurrence ».

« Dernier point qui nous aide, c'est la règlementation. Nous, dans le jeu en ligne, on dépend d'une autorité de régulation qui nous impose des audits, avec un cahier des charges très précis qui comprend environ 190 exigences, on n'a pas réinventé la roue, on s'appuie sur les standards existants, donc sur l'ISO, tout cela fait qu'au bout d'un moment, la sécurité e st dans l'ADN de l'entreprise. La confiance de nos clients et la préservation des flux monétiques sont des enjeux majeurs ».

Le RSSI ne vit pas dans sa tour d'ivoire

« La cybersécurité reste encore nébuleuse dans l'esprit des gens et des clients, j'ai donc sensibilisé nos collaborateurs sur le cas d'un hôpital aux Etats-Unis où les médecins n'avaient plus accès aux dossiers patients qui attendaient une opération. Le vrai risque est donc un risque de vie ou de mort, là les gens comprennent, d'autant que se profilent une possible perte d'activité et au bout une perte d'emplois. Le risque cyber on en parle depuis 10 ou 15 ans, il faut trouver des budgets et accéder au Codir, mais le RSSI ne vit pas dans sa tour d'ivoire, les équipes agiles sont au coeur de cette transformation, et c'est un vrai levier pour les RSSI d'être ainsi au coeur de l'activité ».

Pour Yann Pugi, CISO de Monext et vice-président du Clusir Paca, troisième à prendre la parole, le ton est le même, « j'aimerai bien dire le contraire, mais non c'est pareil, on est assez encadrés par des normes comme PCI DSS ou de type ISO, et comme tout le monde on a eu les mêmes menaces, les ransomware et la personne qui clique sur la pièce jointe, ça existe toujours, et ça existera encore, les attaques DDoS, on les a vu se multiplier, les ondes s'affolent mais ce n'est pas catastrophique. ».

« En revanche, moi j'ai vu des phénomènes loin des sujets cyber et de leur aspect technique, c'est tout ce qui est fraude au Président, au Cerfa qui sont devenus à la mode, tout ce qui est, entre guillemets, « papier PDF », toutes les arnaques autour, avec des gens qui ne savaient pas comment réagir, on a vu beaucoup de choses comme ça, j'ai envie de dire, les attaques changent un peu d'angle, mais il reste l'aspect humain, soit par les réseaux sociaux, soit par le social engineering, qu'on arrive pas à cibler ».

Quand le pirate prend un minimum de risques

« Le maillon faible c'est l'humain, par curiosité, ou pour bien faire, on voit des gens qui ouvrent une facture croyant bien faire, alors qu'ils n'ont jamais reçu une facture de leur vie. Mais là, si c'est marqué urgent ou important, ou en période de congé, il ouvre, on joue avec ça, c'est encore plus facile pour le pirate qui prend un minimum de risques », lance Yann Pugi.

Même sentiment chez Latécoère, où de nouvelles attaques arrivent. Trois à quatre appels par jour pour le RSSI sur des fraudes au président, au niveau international certes, mais quand même. « On a blindé les process, c'est la clé de la non fuite des données, on essaie aussi de leur donner de l'information. Nos autorités de tutelle nous font du reporting sur la sophistication croissante des attaques, par exemple les demandes de changements de RIB et de numéros de téléphone. On essaie de travailler beaucoup en direct avec les métiers, de se servir de nous pour des informations clients et des attaques concurrentielles, les technologies chez nous sont des technologies de souveraineté ».

« Le travail le plus compliqué, c'est de ne pas rester dans nos petits bureaux, à faire le grand écart entre les usines et le 2è étage, le siège du comité de direction, témoigne Stéphanie Buscayret. Je suis un RSSI qui reporte au Comex.

Etre au courant des projets stratégiques, pour nous c'est nouveau, le Comex m'a demandé de venir parler plusieurs fois par an de l'état de la cybersécurité du groupe et en échange (entre guillemets) on a plus d'informations sur la stratégie du business et c'est ça l'enjeu. Pas forcément simpleLes métiers voulaient que je vienne avec eux faire le profil cybersécurité de deux nouvelles usines dans les pays de l'est, sauf que quand on creuse, certes je pars avec eux dans l'avion, mais qu'est-ce qu'on met dans l'usine, on ne sait pas encore, donc on pèche un peu par excès de zèle».

Le cloud n'est pas une menace

Les nouveaux sujets comme l'Iot, le digital, le cloud, sont effectivement de nouveaux sujets. « Depuis trois, quatre mois, les équipes métiers sont venus me voir pour demander conseil, elles m'ont dit qu'on a envie de mettre des données dans l'Iot sur des solutions personnelles Iot. Le cloud n'est pas une menace, l'Iot non plus, la façon dont on les aborde est importante, ce serait un non-sens de les bloquer, on ne va pas mourir en bonne santé ! Il faut accompagner l'IoT, qui n'est pas conçu de manière très sécurisée».

« Le cloud, oui, est un outil formidable, mais on l'accompagne, on réfléchit, on qualifie, j'explique aux métiers s'ils veulent un contrat dans le cloud, c'est comme du McDo vous choisissez pas le menu, vous n'allez pas au McDo demander un boeuf bourguignon, si vous voulez du cloud, il faut être prêt à prendre ce que donne le cloud. Pour cela, on fait une task force avec des juristes et des acheteurs, c'est un changement de paradigme, c'est le RSSI 3.0, voire plus ».

« Chez Monext, ça fait partie du quotidien, beaucoup d'acteurs nous sollicitent, pour des besoins divers et variés, des besoins internes aussi. Salesforce c'est magnifique pour les commerciaux, moins pour nous ! Quel est le devenir du RSSI ? On est parti d'un aspect très technique, c'est fait, maintenant, il faut qu'on bascule vers des aspects comme la compliance. Nous sommes encadrés par des lois et des standards. Aujourd'hui, la difficulté c'est de discuter avec les achats et le juridique pour traduire ces contraintes de sécurité dans un langage commun, vulgariser ces contraintes. On le voit dans le big data, la manière dont on va cadrer le contrat, rajouter des clauses d'audit, voire notre limite de responsabilité, c'est notre quotidien, on vient rarement me voir sur des produits, ou sur un patch ».

« Au PMU, les métiers avaient peur de venir nous voir, pour leurs projets dans le cloud. Une DSI même avec son legacy, voit le cloud comme une occasion, il faut y aller. Nous, le Big Data on l'a démarré en interne il y a deux ans. Tout projet, interne ou cloud, doit être accompagné, avec un cadre de référence de sécurité et ses fondamentaux, une PSSI, mais surtout l'analyse de risque qui permet de bien comprendre les enjeux métiers du projet et d'apporter le niveau de protection raisonnable et nécessaire. Il est évident que la posture du RSSI doit évoluer, et ça c'est fondamental pour nous, je passe mon temps avec des acheteurs et des juristes, ils ont compris qu'on était là pour les aider et sécuriser le business, ils ont vu qu'on on faisait notre job, pour les accompagner au plus vite. On fait de la sécurité, là où elle est nécessaire, faire une analyse de risque, c'est donner le bon signe sur ce qu'on va in fine apporter ».

UN ARTICLE RÉDIGÉ PAR
Didier Barathon, Journaliste

/ STRATÉGIE

Olivier Ligneul (CESIN) : « les cyber-attaques sont de plus en plus complexes et de plus en plus rapides »

Le 28 février à Paris, CIO a organisé une Matinée Stratégique « Cybersécurité : menaces évidentes, menaces cachées » dont le grand témoin était Olivier Ligneul, vice-président du CESIN. Problématiques des SI industriels ou de gestion, contraintes réglementaires, référentiels de bonnes pratiques et baromètre des perceptions des RSSI ont ainsi été détaillés.

Grand témoin de la matinée, Olivier Ligneul, CTO et Group CISO chez EDF, Vice-Président du CESIN, a réalisé une intervention sur « La cybersécurité chez EDF, l'opinion du CESIN ».

Lors de la matinée stratégique « Cybersécurité : menaces évidentes, menaces cachées » organisée par CIO le 28 février 2017 à Paris, le Grand Témoin a été Olivier Ligneul. Celui-ci est non seulement CTO et Group CISO chez EDF mais il est également vice-président du CESIN (Club des Experts de la Sécurité de l'Information et du Numérique). Il a donc abordé la question de la cybersécurité avec cette double vision, particulière et générale. 140 RSSI (dont la moitié dans des entreprises de plus de 10 000 personnes) membres du CESIN ont été interrogés pour l'établissement du Baromètre Annuel du CESIN qui a ainsi été présenté à cette occasion. « Je ne vais pas vous présenter des données de vendeurs qui veulent vous orienter mais ce que pensent de vrais RSSI » a, d'entrée de jeu, précisé Olivier Ligneul.

Le SI d'EDF est triple. Il y a le SI de gestion : plus de 1000 applications, 230 000 utilisateurs et 155 postes de travail avec un millier de réseaux locaux. Le SI scientifique (avec plusieurs supercalculateurs) ne concerne que quelques milliers d'utilisateurs avec des réseaux locaux très haut débit. Enfin, le SI industriel est lié à chaque métier de l'entreprise, avec à chaque fois ses règles propres. Il concerne 93 000 utilisateurs. Bien entendu, chaque SI communique avec les deux autres.

Une réglementation très importante

Mais la politique de sécurité du SI (PSSI) est globalisée et s'applique à toutes les entités et donc chacune des trois branches du système d'information. Les problématiques gérées

par cette PSSI tient à la fois du B2C/B2B à cause des 35 millions de clients du groupe, entreprises comme particuliers, et de l'industriel, sans oublier les fonctions supports et les infrastructures.

Pour une entreprise importante pour l'économie nationale, des règles très particulières viennent s'appliquer. Elles sont issues de la Directive Européenne « Network and Information Security » (NIS) comme de la loi française de programmation militaire. Mais les règles générales s'appliquent également, en particulier, quand on parle de données de millions de clients, le Règlement Général européen sur la Protection des Données (RGPD, en anglais GDPR). Enfin, les entreprises ayant à gérer un important patrimoine de données scientifiques ont, en plus, le dispositif réglementaire du 3 juillet 2012 à respecter au sujet de la Protection du Potentiel Scientifique et Technique (PPST).

Des problématiques de sécurité de plus en plus complexes

Malgré toutes ces règles, une grande entreprise ne peut qu'accompagner des phénomènes comme le BYOD. Et elle ne peut qu'accepter d'entrer dans des filières sectorielles au sein desquels, entre sociétés différentes, il y a de nombreux échanges de données et d'importantes connexions entre clients et fournisseurs. Le cloud est devenu une réalité. Ce n'est pas encore assez ? « Si vous gérez des ascenseurs, des codes d'accès à des immeubles, via une gestion technique de bâtiments, il y a aussi des risques à gérer » a rappelé Olivier Ligneul. Il existe de nombreuses études sur ces types de risques.

Pour respecter toutes les contraintes, un RSSI peut s'appuyer sur des référentiels. Olivier Ligneul a notamment promu ceux de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) qui permettent d'aborder autant la phase amont d'étude de risques que la supervision ou le traitement des incidents. D'autres référentiels sont plus sectoriels. « On y aborde aussi des sujets basiques, communs aux SI de gestion et aux SI industriels, comme la politique de gestion de mots de passe ou de fermeture de ports » a relevé Olivier Ligneul.

Sécurité et sûreté ne doivent pas s'opposer

« Les attaques sont de plus en plus complexes et de plus en plus rapides »

Et les entreprises doivent affronter des risques de plus en plus importants. Olivier Ligneul a déploré : « il y a des attaques de plus en plus complexes et de plus en plus rapides. » On est passé d'attaques en jours à des attaques en heures et, aujourd'hui, en secondes. Les cybercriminels utilisent des méthodes industrielles pour atteindre une performance de plus en plus grande.

Côté entreprise, un SI de production est là pour faire ce qu'on lui a demandé de faire en permanence. « Il y a donc une obligation de sûreté de fonctionnement » a constaté Olivier Ligneul. Cela implique que les mesures prises ne doivent pas, en elles-mêmes, être une menace pour le fonctionnement du SI. Olivier Ligneul a pointé un exemple significatif : « si un anti-virus isole ou détruit une DLL nécessaire au SI de production, le SI de production ne marche plus. Avec toutes les conséquences induites. » Sûreté et sécurité ne doivent pas s'opposer et les priorités être bien prises en compte. « Dans un SI industriel, d'abord vous mettez en sûreté puis vous traitez les questions de sécurité » a insisté Olivier Ligneul. A l'inverse, dans un SI de gestion, l'attaque sera d'abord confinée et traitée.

SI industriels ou de gestion, il y a des différences et des points communs

Cartographie, inventaire, bonnes pratiques de développement, de cloisonnement, etc. , par contre, sont des problématiques communes aux SI de gestion et aux SI industriels. Mais les SI industriels ont des particularités. Il peut ainsi y avoir des flux peu identifiés utilisant des protocoles rares voire spécifiques à une seule entreprise ou un seul secteur.

Et l'analyse de risques est également différente. Un outil industriel va devoir subir, par exemple, des écarts de température et c'est une problématique inconnue des appareils destinés à fonctionner dans un bureau. « On peut avoir de vrais difficultés, pour un SI industriel, à répliquer dans un environnement de test ce qui se passe dans un environnement réel » a pointé Olivier Ligneul.

Cloud or not cloud, this is not the question

Une question récurrente en matière de sécurité est le cloud. Doit-on y aller ? Est-ce par principe exclu ? En fait, le cloud doit être abordé comme n'importe quelle externalisation. Il existe des problématiques réglementaires, juridiques (propriété des données, relation contractuelle...), de politique d'achat et, enfin, de sécurité informatique au sens strict.

La « propriété des données » renvoie ainsi au droit à les récupérer et surtout à être le seul à pouvoir le faire comme à des questions « informatique et libertés ». Olivier Ligneul a insisté : « le cloud ne peut pas s'envisager sans étudier toutes ces problématiques et il ne doit pas être vu comme un simple moyen de répondre au time to market de la direction générale. »

Les RSSI expriment leurs opinion dans le baromètre

Olivier Ligneul a conclu son intervention lors de la matinée en revenant sur le Baromètre du CESIN. Celui-ci donne l'opinion réelle des RSSI en activité, en dehors de toute contrainte issue des fournisseurs. Comme attendu, 80 % des entreprises ont effectivement connu une attaque l'année passée. Et, parmi ces attaques, l'une est bien installée en tête : le ransomware qui croît de 19 %. Les DDoS et les « attaques virales générales » complètent le trio de tête.

Face à un tel podium, la satisfaction vis-à-vis des solutions de sécurité du marché ne fait pas l'unanimité. 31 % des RSSI jugent les solutions du marché peu ou pas adaptées à leur entreprise et 40 % à la typologie des attaques. Mais si des solutions existent, la tendance est de les acheter grâce à une croissance des budgets et des effectifs dans la fonction « sécurité ». « Mais c'est aussi un problème car nous connaissons une pénurie de compétences dans ce domaine, chacun se battant pour récupérer ces bonnes compétences » a signalé Olivier Ligneul. Mais 48 % des RSSI ne se sentent pas en mesure de résister aux menaces actuelles.

Contrôler l'application des consignes

La sensibilisation des collaborateurs progresse et, aujourd'hui, la majorité respecte au minimum les consignes données. 57 % des RSSI contrôlent ce bon respect des consignes, la seule sensibilisation ayant montré ses limites. Celle-ci continue malgré tout d'être une préoccupation des RSSI. Surtout, la sensibilisation de la direction générale reste un point particulièrement sensible. A l'inverse, des mots clés à la mode comme blockchain ou IoT font peu tressaillir les RSSI.

UN ARTICLE RÉDIGÉ PAR
Bertrand Lemaire, Rédacteur en chef de CIO

La table ronde « Les nouvelles réponses à apporter par le RSSI » a réuni, de gauche à droite, Arnaud Tanguy (CISO d'AXA Investment Managers), Philippe Fontaine (RSSI du Groupe SMA) et Farid Illikoud (CISO du PMU).

/ JURIDIQUE

Les nouveaux rôles du RSSI en lien avec le GDPR

Le 28 février, CIO a organisé une Matinée Stratégique « Cybersécurité : menaces évidentes, menaces cachées » à Paris. Trois RSSI ont témoigné des nouvelles réponses qu'ils se devaient d'apporter, notamment par la transformation de leur rôle en lien avec le GDPR : Arnaud Tanguy (CISO d'AXA Investment Managers), Philippe Fontaine (RSSI du Groupe SMA) et Farid Illikoud (CISO du PMU).

La conformité réglementaire est traditionnellement un sujet pour le RSSI mais limité à des réglementation en lien strictement avec la sécurité des données. Déjà, l'obligation de sécurité des données personnelles les a confrontés à la CNIL. La prochaine entrée en application du GDPR (Règlement Général européen sur la Protection des Données) étend leur rôle dans ce domaine mais sans les dispenser de leurs autres obligations. Sur la Matinée Stratégique « Cybersécurité : menaces évidentes, menaces cachées », organisée par CIO le 28 février 2017, trois RSSI ont témoigné sur ce sujet lors de la deuxième table ronde : Arnaud Tanguy (CISO d'AXA Investment Managers), Philippe Fontaine (RSSI du Groupe SMA) et Farid Illikoud (CISO du PMU).

Les trois RSSI couvrent trois marchés très différents les uns des autres mais les contraintes nouvelles qui pèsent sur eux sont autant importantes. Ainsi, le PMU propose des paris hippiques et sportifs mais aussi du poker en ligne. SMA est une mutuelle du bâtiment qui assure notamment la moitié des garanties décennales en France mais qui a aussi une activité bancaire et assurancielle. Enfin, AXA Investment Managers est la filiale de gestion d'actifs du groupe Axa, gérant ainsi 600 milliards d'euros. Le groupe Axa est de fait le principal client d'Axa IM mais des institutions tierces (fonds privés ou publics) ont également recours à ses services, pour un total d'environ 2000 clients.

L'inflation réglementaire doit être intégrée

« Il y a une véritable inflation réglementaire qui impacte lourdement l'activité de l'entreprise » a confirmé d'entrée de jeu Farid Illikoud. Au PMU, le réglementaire comprend aussi la conformité avec les règles de l'ARJEL (Autorité de Régulation des Jeux En Ligne). Il s'agit encore une fois, pour ce qui concerne l'IT, de règles de sécurité tant technologiques que procédurales. Farid Illikoud précise : « la finalité est la protection du joueur, y compris contre l'addiction ou la tentation de jouer alors qu'il n'en a pas le droit, parce qu'il est mineur par exemple ». Du coup, le PMU a l'obligation de s'assurer de l'identité des joueurs. Et l'ARJEL opère tous les ans un audit qui dure deux mois sur l'ensemble des processus de l'entreprise.

A cette spécificité sectorielle, le PMU ajoute toutes les contraintes générales. Au premier chef desquelles vient le GDPR (en Français, RGPD : règlement général européen sur la protection des données). La non-conformité entraîne le risque d'une amende se chiffrant à 4 % du chiffre d'affaires mondial. « Certes, c'est un chamboulement qu'on nous impose en deux ans, mais c'est une réglementation qu'on a vu venir » a modéré Arnaud Tanguy. Il restait les détails mais les grandes lignes étaient en effet connues depuis longtemps.

Deux aspects : juridique et technique

Pour lui, il faut travailler deux aspects. D'une part, il faut commencer par une étude juridique approfondie pour examiner en quoi l'entreprise est impactée par le GDPR, clause par clause. D'autre part, il faut en tirer les conséquences techniques. « La préoccupation, en matière de protection des données, est très proche de la sécurité traditionnelle des données » constate Arnaud Tanguy. Classification des informations, inventaires des applications... choses normales pour identifier ce qu'il faut protéger et comment.

Publicité

Philippe Fontaine a confirmé : « On suivait la promulgation du RGPD depuis le départ et c'était un sujet de discussion au ComEx, porté par le DSI auquel je suis rattaché ». C'est dès avant la promulgation que SMA a ainsi décidé de mener un audit avec Deloitte pour faire le point sur la situation des données personnelles au sein du groupe. Ce diagnostic a permis de ressortir les écarts potentiels. Le suivi de la mise en conformité a été ensuite assuré par une stagiaire du master spécialisé en formation continue de l'ISEP, juriste de formation initiale avec une expérience professionnelle dans ce domaine, mais avec la compétence informatique et liberté apportée par le master. Sa mission a été de construire le plan d'action pour être en conformité avant le 25 mai 2018. La mise en oeuvre du plan lui a également été confié au travers d'une embauche à l'issue du stage.

La sécurité, outil de la conformité

Au PMU, la démarche a débuté dès la promulgation du texte, à l'été 2016. « Il s'agissait déjà de comprendre le texte » a relevé Farid Illikoud. Il a fallu une collaboration entre la direction générale, la direction juridique et l'IT, en l'occurrence la sécurité informatique. Une analyse de la situation a permis d'isoler des écarts de conformité. Utilisant l'obligation de conformité, Farid Illikoud a lancé un chantier plus vaste : « classification des données, mise en place d'un DLP, etc. On en profite pour balayer tous les processus. La sécurité n'est qu'un moyen pour remplir des obligations essentiellement juridiques. »

Mais le chantier est en effet très vaste. Il faut de fait être en mesure d'identifier tout le circuit des données. Et le CIL est sans doute insuffisamment technicien pour y parvenir. Du coup, le sujet retombe sur le RSSI. « Nous n'avions pas forcément une cartographie précise de toutes les données, les contrats avec les fournisseurs impliqués, etc. Il y a donc un vaste chantier qui est naturellement confié au RSSI, celui qui est capable de parler avec les développeurs, les architectes, avec des juristes et des acheteurs » a pointé Farid Illikoud. Il a cependant précisé : « nous n'avons évidemment pas attendu GDPR pour protéger de la donnée client mais le risque pénal avec une amende de très fort montant est évidemment un facilitateur pour les discussions internes. « Dans des petites sociétés de gestion d'actifs, avec les RSSI desquels nous discutons, le GDPR est un bon levier pour faire adopter des démarches de sécurité » a relevé Arnaud Tanguy.

Le DPO en question

Des points peuvent rester en suspens. Par exemple, au PMU, le choix n'est pas encore arrêté quant à savoir s'il faut ou non un DPO (Data Privacy Officer). Celui-ci ayant une dimension technique, le RSSI semble devoir être en charge de cette nouvelle mission. D'autres penchent pour une dominante juridique pour le profil du futur DPO. Mais, en tel cas, une dimension technique serait manquante. Chez Axa IM, la conformité GDPR a été lancée sous la forme d'un vaste programme commun entre la sécurité informatique, le juridique et la conformité réglementaire sous l'autorité directe de la direction générale. « Nous opérons dans un secteur très réglementé à la base et nos équipes de conformité réglementaire sont assez fortes » s'est réjoui Arnaud Tanguy. Il n'est en effet pas rare, dans ce secteur, que la mise en oeuvre de réglementations impactant lourdement le statu quo doive se faire en un an. En l'occurrence, le RSSI apporte donc son concours à cette équipe bien rodée.

« La cartographie des traitements est le nerf de la guerre » a insisté Philippe Fontaine. Celle-ci peut être issue des déclarations des uns et des autres, responsables de tels ou tels traitements. Pour garantir l'exhaustivité, se rapprocher de CIL de sociétés comparables permet de comparer les relevés et ainsi de voir les écarts pour compléter les inventaires. Dans l'assurance, une réglementation sectorielle, Solvency 2, impose une qualité des données qui permet, à partir de l'inventaire, de remonter aux traitements. Le DPO sera probablement la chargée de mission actuelle qui devrait être rattachée hiérarchiquement au RSSI. Philippe Fontaine a aussitôt précisé : « qui dit rattachement hiérarchique ne signifie pas rattachement fonctionnel ».

Le DPO doit en effet rendre compte au seul responsable final des traitements et travailler en lien fort avec la direction juridique, d'où le choix, chez SMA, d'un profil juridique. Chez Axa IM, le profil du futur DPO n'est pas encore formellement choisi mais il serait logique qu'il appartienne à la cellule de conformité réglementaire, avec une expérience juridique et technique.

Cartographie des données et état des lieux semblent bien être au coeur de la démarche, comme l'a relevé en conclusion de la table ronde le Grand Témoin de la matinée, Olivier Ligneul, CTO et Group CISO chez EDF.

UN ARTICLE RÉDIGÉ PAR
Bertrand Lemaire, Rédacteur en chef de CIO