150

Novembre 2017

Cybersécurité : nouvelles menaces, nouvelles solutions

En bref

Les RSSI réagissent-ils aussi vite que les hackers ? Cette question est posée. Et les participants à la conférence CIO du 21 Novembre 2017 y ont répondu en présentant les meilleures pratiques.
Philippe Loudenot (Fonctionnaire de Sécurité des Systèmes d'Information, Ministères Sociaux), Stéphane Nappo (Global Chief Information Security Officer & Board Advisor, Société Générale IBFS), Henri d'Agrain (Délégué Général, CIGREF), Mahmoud Denfer (Global Chief Information Security Officer, Vallourec) et José Perez (Chief Information Security Officer France & Afrique, Allianz) ont apporté leurs témoignages. Le Grand Témoin de la matinée a été Alain Bouillé, Directeur Sécurité des SI Groupe de la Caisse des Dépots et Président du Cesin.

Sommaire

Cybersécurité : les RSSI réagissent-ils aussi vite que les hackers ?

Sur la CIOnférence du 21 novembre 2017, les participants se sont interrogés sur les possibilités de réponses aux nouvelles cybermenaces.

Le 21 novembre 2017, la conférence « Cybersécurité : nouvelles menaces, nouvelles solutions » a été organisée par CIO à Paris en partenariat avec Bitdefender, Datadome, HP, NTT Security, RSA et Zscaler et avec la participation du CESIN.

Les cybermenaces pèsent lourdement sur les entreprises mais, si les RSSI en sont bien conscients, les bonnes pratiques, même basiques, ne sont pas encore partout appliquées. Les témoins et experts qui se sont exprimés sur la conférence « Cybersécurité : nouvelles menaces, nouvelles solutions » ont présenté ces bonnes pratiques mais n'ont pu que regretter la persistance d'insuffisances et de dysfonctionnements mettant les entreprises en péril. Cette CIOnférence a été organisée par CIO le 21 novembre 2017 au Centre d'Affaires Paris Trocadéro en partenariat avec Bitdefender, Datadome, HP, NTT Security, RSA et Zscaler.
Les principaux résultats de l'étude réalisée par CIO *Quelle gestion des risques face aux défis de la cybersécurité ?*, basé sur une enquête auprès d'environ 300 répondants (chiffre variable selon les questions), a révélé les manquements des entreprises. Les bonnes pratiques, même parfois les plus basiques, ne sont pas appliquées.

Améliorer le service... et la sécurité ?

« Au cours d'un déplacement professionnel aux Etats-Unis, j'ai appris qu'un concert se déroulait dans la ville dans laquelle je me trouvais. J'ai donc réservé au dernier moment un billet pour le soir même grâce à mon smartphone... Au cours de cette étape, de nombreux warnings se sont imposés à moi » s'est souvenu Pierre-Yves Popihn, Directeur Technique France, NTT Security. Si la transformation numérique n'est que sous l'angle de l'amélioration du service et la facilitation de

l'expérience utilisateur, on oublie parfois un élément essentiel : la sécurité. Qu'un site e-commerce ne soit pas en HTTPS ou ne propose pas un paiement sécurisé en respectant PCI DSS, ce n'est tout simplement pas acceptable.
Les obligations légales ne sont parfois même pas respectées, comme celles bientôt imposées par le RGPD : le chiffrement du stockage des données personnelles ou encore la mise en place d'une procédure de gestion des incidents, etc. C'est le rôle des 1500 experts de la filiale sécurité du groupe japonais NTT d'accompagner les entreprises, partout dans le monde, autour de ces sujets. Et si la sécurité n'est pas intégrée comme une préoccupation dès le début du projet, elle n'en sera que plus coûteuse à implémenter car il faudra souvent repartir de zéro.

« Transformation numérique, CyberSécurité et Ed Sheeran : un triptyque improbable » a été le thème de l'intervention de Pierre-Yves Popihn, Directeur Technique France, NTT Security.

« La cybersécurité est aujourd'hui un sujet de direction générale » a indiqué Gérôme Billois, Partner Cybersecurity & Digital Trust chez Wavestone. En effet, les menaces sont de plus en plus visibles mais aussi de plus en plus complexes à étudier et à contrer.

Gérôme Billois, Partner Cybersecurity & Digital Trust, Wavestone, a amené son expertise sur « Cybersécurité et confiance numérique ».

La protection doit contrer 100 % des cyber-attaques, pas 99 %

99 % des attaques restent cependant assez classiques : malwares connus, utilisation de kits d'exploits, recours au phishing, exploitation de vulnérabilités... Les moteurs classiques, permettant l'analyse de signatures et l'analyse comportementale, sont

parfaitement aptes à gérer ce genre de cyber-attaques. Vincent Meysonnet, Responsable Avant-Vente chez Bitdefender, a pointé : « le problème, c'est le 1 % restant ». Pour contrer des attaques sans fichier (basées sur des exploits javascript dans les navigateurs...) ou polymorphiques, une protection multicouche de nouvelle génération est alors nécessaire.

« Sécurité de nouvelle génération : indispensable ou simple hype ? » s'est interrogé Vincent Meysonnet, Responsable Avant-Vente chez Bitdefender.

La dépendance au SI rend les attaques plus dangereuses

Mais l'approche périmétrique aussi est dépassée à l'heure où 30 % des données sont à l'extérieur de l'entreprise, dans le cloud par exemple. Or la dépendance business à l'IT, avec la transformation numérique, rend les cyber-attaques d'autant plus redoutables : si le SI est attaqué, c'est bien l'entreprise même qui peut disparaître. Le niveau de risque s'accroît. « Nous proposons donc une plate-forme de sécurité 100 % cloud pour que la sécurité soit extérieure aux infrastructures » a indiqué Ivan Rogissart, Directeur Avant-Vente Europe du Sud chez Zscaler.

Ivan Rogissart, Directeur Avant-Vente Europe du Sud chez Zscaler a répondu à une question bien d'actualité : « Cloud, Mobilité, Menaces Avancées : quels sont les impacts sur la sécurité du SI ? ».

« Réagir aux nouvelles menaces » a été d'ailleurs le thème de la première table ronde de la matinée. Celle-ci réunissait Philippe Loudenot (Fonctionnaire de Sécurité des Systèmes d'Information, Ministères Sociaux) et Stéphane Nappo (Global Chief Information Security Officer & Board Advisor, Société Générale IBFS) qui ont témoigné

de leurs pratiques.

La première table ronde, « Réagir aux nouvelles menaces », a réuni Philippe Loudenot (Fonctionnaire de Sécurité des Systèmes d'Information, Ministères Sociaux) et Stéphane Nappo (Global Chief Information Security Officer & Board Advisor, Société Générale IBFS).

Gagner la course

Le sous-titre de la conférence, « les RSSI réagissent-ils aussi vite que les hackers ? », a fait réagir Palakiyem Assish, Senior Pre-sales Engineer chez RSA Netwitness. Pour lui, malgré les outils en place, les compromissions sont souvent détectées par des tiers à l'entreprise victime. Il en a déduit : « notre objectif est de vous faire réagir plus vite que les hackers car plus le temps passe et plus les dégâts seront importants. » Bien sûr, il faut faire de la prévention (anti-virus, firewall...), de la détection (SIEM...)... mais il faut aussi analyser la fameuse « zone blanche », là où il n'y a pas de traces. Cela nécessite une visibilité totale, 360°, sur le trafic réel avec une étude de l'ampleur d'une attaque et de l'impact business induit. Seule cette visibilité peut supprimer le gap entre la vision business orientée impact sur le chiffre d'affaires et la vision technique.

Palakiyem Assish, Senior Pre-sales Engineer chez RSA Netwitness, a expliqué « L'évolution du SIEM au-delà des Logs ».

600 milliards de dollars

Cet impact a été chiffré par Christophe Demagny, Senior Security Consultant chez HP : 600 milliards de dollars en 2021. Il faut en effet comprendre l'évolution de l'adversaire, qui se professionnalise et s'organise, et des cyber-attaques toujours plus

sophistiquées. Les attaques se rapprochent ainsi toujours plus des niveaux bas, du matériel, via le BIOS ou les firmwares. Les imprimantes multifonctions étant en effet avant tout de véritables serveurs informatiques, il faut songer à les sécuriser, comme tous les autres terminaux, là où la plupart des attaques ont lieu.

« Mise en place d'une stratégie Cyber Résiliente : Gérer la sécurité commence par le matériel » a insisté Christophe Demagny, Senior Security Consultant chez HP.

Le Grand Témoin de la Matinée a été Alain Bouillé, Directeur Sécurité des SI Groupe de la Caisse des Dépots et Président du Cesin. Il a pu présenter l'évolution des approches et des relations DSI-RSSI-métiers-DG.

Le Grand Témoin de la matinée a été Alain Bouillé, Directeur Sécurité des SI Groupe de la Caisse des Dépots et Président du Cesin.

Et le RGPD ?

Difficile de parler sécurité des données, à l'approche de mai 2018, sans aborder sérieusement le RGPD et la fameuse amende de 4 % du chiffre d'affaires encourue par les entreprises non-conformes. Or, parmi les éléments contre lesquels les utilisateurs doivent être garantis, il y a l'usurpation de compte ou d'identité, en anglais l'*account takeover*. A l'heure actuelle, des robots parcourent sans cesse le web, multipliant les attaques en force brute pour tester des centaines de millions de combinaisons identifiants/mots de passe et accéder aux parties privées des sites web, avec un taux de réussite de 8 %. « Un de nos clients a décidé de s'équiper d'une solution de protection contre les bots après avoir constaté des tentatives d'usurpation de compte très sophistiquées » a affirmé Benjamin Barrier, Partner & Chief Sales Officer chez

Gérôme Billois : « La destabilisation a été la plus grande motivation des cybercriminels en 2017 »

En ouverture de notre conférence sur la cybersécurité, Gérôme Billois dresse un état des menaces et des meilleures réponses possibles.

CIO a organisé une Matinée Stratégique, «Cybersécurité : nouvelles menaces, nouvelles solutions », le 21 novembre 2017, avec l'analyse de Gérôme Billois, Partner Cybersécurité et Digital Trust au cabinet Wavestone.

« *L'idée de mon intervention est de faire un état de ce qu'on voit sur le terrain coté menaces et côté évolution des réponses des CISO* » note Gérôme Billois en débutant son intervention lors de la CIOnférence consacrée à la cybersécurité, le 21 novembre 2017. Ces menaces sont de plus en plus visibles mais sortent du champ de vision habituel, pour atteindre par exemple les métiers. « *Je ne vais pas vous détailler tous les points de tous les incidents, vous pouvez les retrouver dans le panorama du Clusif en début d'année, mais on a maintenant des cas très complexes à analyser* ». Il faut voir quelles étaient les modalités des attaquants ? Se dire pourquoi, dans mon organisation ou dans mon métier, je peux être attaqué et par qui ? « *Donc si je regarde ces cas, cette motivation des attaquants, je vais bien identifier ce qui s'est passé ces derniers mois* ».

D'abord, on remarque des attaques produites pour des raisons idéologiques. Vous voyez l'actualité en Catalogne, elle s'accompagne d'attaques des deux camps sur les institutions, espagnoles ou catalanes. Chaque conflit aujourd'hui a un pendant sur le cyberespace. Il faut mentionner des révélations, comme celles de Wikileaks sur les attaques de la CIA. Shadow broker, dont on ignore toujours les vrais détenteurs, a mis la main sur les outils d'attaques de la CIA, des outils techniques et financiers qui

produisent les plus gros incidents.

Deuxième motivation des attaquants, l'argent. Quand on va sur le terrain gérer des réponses à incident on voit que la majorité des attaques sont motivées par des questions financières. Les pirates veulent attaquer pour revendre, pour bloquer des systèmes, ou effectuer des demandes de rançons. La plus célèbre a affecté la Banque du Bangladesh, 81 millions de dollars ont été volés sur un compte détenu par cette banque centrale.

Equifax : le plus grand cas de vol de données personnelles

Le dernier cas connu est celui d'Equifax. Une société qui fait de la gestion d'informations financières sur les américains, un métier qui n'a pas d'équivalent en Europe. Il permet de dire aux banques si les particuliers sont solvables ou pas. « *Ils ont réussi à perdre 145 millions d'identités d'américains, soit la moitié de la population. C'est le plus grand cas de vol de données personnelles et de données financières* ».

Plusieurs points sont Incroyables dans le cas Equifax. C'est d'abord la manière dont ils ont géré une crise. Il est toujours facile de le dire, mais si vous voulez analyser ce qu'il ne fallait pas faire, c'est leur cas qu'il faut examiner. Je vous donne un exemple, au lendemain de la perte de 145 millions de comptes, le dg fait une vidéo où il dit qu'il est déçu par ce qui s'est passé. C'était beaucoup trop faible comme réponse par rapport à la gravité de l'incident.

Ensuite, Equifax a lancé un service d'aide aux clients, pour leur proposer de surveiller leur identité et leur compte sur Internet. Sauf qu'il y avait une petite clause expliquant que si le client souscrit à ce service gratuit, il s'engage aussi à ne pas poursuivre Equifax ! « *Vous imaginez le tollé ! L'attorney général leur est tombé dessus. On continue ? Ils ont lancé un site web spécialisé pour gérer la crise, s'inscrire et trouver des informations. A chaque fois que vous avez ça, vous avez des petits malins qui font des sites proches pour capter les données. Le service communication d'Equifax a même relayé l'adresse d 'un faux site*.
Une dernière ? Il y a quinze jours, le dg a été convoqué au Sénat, deux mois après la crise, pour s'entendre demander si ses données étaient chiffrées. C'est la question °1 que posent les politiques. Le dg a répondu « je ne sais pas » ! Vous imaginez aisément l'impact sur la crédibilité de l'entreprise. »

La destabilisation de l'Ukraine a fait boule de neige

Troisième motivation, c'est celle qui a le plus attiré l'attention et déclenché les incidents majeurs. On a parlé des élections françaises et américaines, d'attaques qui ont révélé des informations sensibles, il y a aussi l'Ukraine un pays qui se fait destabiliser par des attaques cyber a peu près tous les six mois. Vous avez eu une coupure d'électricité suite à des attaques cyber. Une attaque Not Petya qui a touché1 500 entreprises dans le pays avant de se répandre dans le monde entier, touchant des groupes aussi célèbres que Merck ou Saint-Gobain. Ces entreprises ont été touchées uniquement parce qu'elles étaient des dégâts collatéraux de l'attaque initiale qui, tout le laisse à penser, visait l'Ukraine extrêmement mal entrainée, avec des dégâts assez incroyables.

L'exemple du laboratoire pharmaceutique Merck est marquant, ils estiment qu'ils vont perdre 620 millions de dollars suite à cette attaque, leur production est toujours impactée. Ils ont dû faire appel au stock stratégique de vaccins des Etats-Unis à la

rescousse, car ils n'étaient plus capables de reproduire des vaccins en nombre suffisant, donc, on voit comment un incident cyber impacte durablement et fortement l'activité d'une entreprise.

Et puis, dernier type d'incident, on en parle depuis des années, il est devenu vraiment réel, l'attaque sur des structures pour obtenir de nouvelles capacités d'attaques. Le cas n° 1 c'est Medoc, une société ukrainienne spécialisée dans les logiciels de comptabilité, une des deux recommandées par l'Etat pour déclarer ses impôts en Ukraine. Les attaquants ont pris le contrôle de ses serveurs pour s'emparer du mécanisme de mise à jour, et ainsi distribuer le malware. C'était donc un canal tiers, mais extrêmement efficace pour attaquer de manière ciblée, toutes les sociétés réalisant du business en Ukraine.

Même les régulateurs sont atteints

Autre cas, celui de CCleaner, plus grand public, un système de nettoyage d'ordinateur, lui aussi piégé en deux attaques pour viser au final de grands noms de l'IT. Dernier cas, il plaira aux banquiers, celui de l'Autorité des marchés financiers en Pologne (la Polish Financial Supervision Authority), ceux qui insistent beaucoup sur les règles de cybersécurité. Ce site web finalement distribuait des malwares spécifiques pour les banques de Pologne qui téléchargeaient un document infecté, ils ont réussi à piéger 50 banques dans le pays à partir du site du régulateur.

L'observation de ces différents cas amène à se reposer la question des piliers de la cybersécurité : protéger, détecter, réagir. « *Ces 3 piliers d'une stratégie de sécurité sont toujours là, on voit bien qu'il faut continuer à investir sur les basiques, mais ne pas hésiter à investir sur l'innovation, marcher sur ses deux jambes et ce n'est pas toujours, toujours, évident*. »

Sur la détection, il y a eu de vrais progrès, en 2011 c'était 500 jours en moyenne, si on regarde en 2016, c'était 100 jours, on a divisé par 5 la durée, c'est encore très long, on voit qu'il y a eu des investissements et des progrès. Dans les SOC des entreprises, on voit du petit ransomware, du petit incident, et finalement ça endort les équipes, dépassées quand vient un incident grave, parce que les équipes ne sont pas assez préparées.

Plus de PC, plus d'annuaire, plus de mail

« *Sur la partie réponse, la capacité à réagir, on voit clairement des choses à repenser ». C'est : je prends mon PC, j'alerte les collègues, j'envoie des emails. Pour gérer la crise, on a vu que les dernières grandes attaques comme Wanacry ou Not Petia ont amené la destruction des systèmes d'information, incapables de gérer la crise. A un moment, vous vous retrouvez avec plus rien, vous n'avez plus de PC, plus d'annuaire téléphonique, plus de possibilités d'envoyer des mails. Vous n'avez plus rien, donc, la première réaction de la cellule de crise c'est de se dire comment on fait ? C'est de basculer sur les adresses mails des collaborateurs, de créer des groupes sur WhatsApp, créer des sites gratuits rapidement pour communiquer et donc ça fait perdre du temps et fait prendre d'autres risques. Je pense qu'en 2018, il faut prendre d'autres mesures, en fonction de ce qui a été observé en 2017* ».

« *Quatrième pilier à ajouter à notre sens, celui de la reconstruction. Les entreprises se retrouvent avec des dizaines des milliers de PC à réinstaller, donc on a développé des*

stratégies de cyber-résilience, pour décider comment se remettre en route rapidement. Est-ce que je peux demander à mes collaborateurs de le faire ? Faut-il du matériel en stock et mettre en place des services de découplage des activités internes et des activités cloud ? Faut-il autoriser le télétravail pour le byod, ne serait-ce que pendant une semaine pour continuer à travailler ? On avait eu des alertes, avec les attaques sur Sony ou Saudia Aramco, on a eu plusieurs attaques majeures en 2017, on ne peut pas passer à côté du sujet de la destruction massive. Voilà sur la stratégie ».

Un autre sujet est une vraie révélation en 2017, selon Gérôme Billois c'est devenu un sujet de direction générale. « Jamais on a été autant mobilisés par les directions générales, jamais on a reçu autant de questions directes ». Il y a le cas Not Petya, l'affaire Yahoo avec une perte de 350 millions d'euros lors de la revente, ces cas parlent aux directions générales, l'affaire Vinci n'a pas eu d'incident, mais a marqué et ouvert l'attention des dg.

Mesurer l'impact de ses projets de cybersécurité

Il existe deux grandes situations sur le marché. La grande majorité des entreprises qu'il faut convaincre d'investir. C'est par le levier des incidents, le levier du benchmark, c'est assez efficace. La capacité d'écoute des dg est bien meilleure. Certaines entreprises ont déjà franchi le cap et savent mesurer l'impact de leur projet de cybersécurité. Elles ont passé les étapes, de spécifications et d'appels d'offres. Même si elles ont leur utilité, il faut déployer sur le terrain les outils et les processus et former les gens.

« *Notre sentiment est que le CISO doit changer de casquette et devenir un chief investment security officer, se mettre dans cette logique de démontrer à sa dg qu'il y a eu des investissements et qu'ils vont avoir des effets. Je ne parlerai pas du ROI de la cybersécurité, j'ouvrirai une boîte de pandore, c'est un sujet serpent de mer. Il faut démontrer que, quand on investit, le risque diminue et derrière pour avoir cet accord de la dg il faut structurer le budget. Souvent c'était des petits budgets, des centaines de milliers d'euros à gauche ou à droite, des projets d'une DSI ou d'une entreprise. A partir du moment où on va être dans un programme cohérent et une masse critique, la dg va s'y intéresser. On parle de programmes de cybersécurité quand on est sur des programmes cohérents avec des KPI claires. Les chiffres dépendent de la structure de l'entreprise, de sa taille et du secteur d'activité. On parle de programmes à partir du moment où on est sur plusieurs millions d'euros de budget, aujourd'hui ce qu'on voit c'est 15/20 millions d'euros et ça monte jusqu'à des 150 millions d'euros investis sur 3 ans. Quand on est sur cette tendance-là, on est capable de faire venir dans l'équipe sécurité un directeur de programmes, qui va être capable de faire aboutir les projets, on va voir l'ampleur que ça prend, le « board » va appuyer*".

Les grandes entreprises s'y mettent

« *Vous allez dire c'est une vision théorique, pas tant que ça, on voit comment ça a démarré, 25 % des groupes du CAC 40 ont fait ce choix avec un reporting au niveau du board. C'est clairement un progrès, si je regarde dans le rétroviseur. Depuis toutes ces années où on accompagne les entreprises, il y a un vrai changement, 75 % n'en ont pas, mais la tendance va dans la bonne direction* ».

Pour conclure, Gérôme Billois insiste sur deux points. Ceux qui sont les plus avancés ont des problèmes pour faire bouger les équipes opérationnelles, en particulier les

équipes opérationnelles de la DSI. « On a l'accord de la DG, on pense que tout va avancer tout seul, malheureusement on a des structures ancrées dans leurs habitudes, difficiles à bouger ». Wavestone a fait une étude sur les sites Web. « *40% de ceux qu'on a audités, à l'audit suivant, avaient des failles graves. Ce qu'on voit, c'est souvent que ces audits ont lieu, mais les actions à la base ne sont pas réalisées. Pour moi, un des challenges dans les années à venir, sera quand une dg agit, d'avoir un suivi sur le terrain, c'est aussi une conduite du changement. Je dirai que les équipes cyber n'en ont pas forcément l'habitude* ».

Second point, enfin, il faut être capable de prouver l'efficacité de la cybersécurité. « *C'est un sujet de réflexion, je ne vous dirai pas aujourd'hui que j'ai la solution, c'est quelque chose sur lequel on réfléchit beaucoup en interne, parce que les dg une fois qu'elles ont donné de l'argent, ont finalement vu l'avancement des projets. Mais comment faire avec une menace qui évolue en temps réel pour être efficace ? Il y a une attente de la DG, pour qu'on lui prouve que la sécurité augmente* ».

En savoir plus

- Télécharger l'étude *Quelle gestion des risques face aux défis de la cybersécurité ?*
- Contenus associés à la conférence *Cybersécurité : nouvelles menaces, nouvelles solutions* (Mises à jour régulières)

Didier Barathon
Journaliste

Les ministères sociaux et la Société Générale IBFS face aux cybermenaces

Philippe Loudenot des ministères sociaux, à gauche, et Stéphane Nappo, Société Générale IBFS, à droite, débattent des nouvelles menaces et de leur impact.

CIO a organisé une matinée stratégique, «Cybersécurité : nouvelles menaces, nouvelles solutions », le 21 novembre 2017 avec, sur la première table-ronde, les témoignages des Ministères sociaux et de la Société Générale IBFS.

La première table-ronde de la matinée «Cybersécurité : nouvelles menaces, nouvelles solutions » organisée par CIO le 21 novembre 2017 réunissait deux responsables cybersécurité de haut niveau, appartenant à deux univers différents, l'un dans le public, l'autre dans le privé et à l'international. Le premier, Philippe Loudenot, est précisément Fonctionnaire de Sécurité des Systèmes d'Information, aux Ministères Sociaux, donc FSSI. Les Ministères Sociaux comprennent : l'éducation nationale, le travail, la santé, la jeunesse et les sports. Philippe Loudenot a également sous sa responsabilité, un ensemble d'organismes qui dépendent de ces ministères : Pôle Emploi, CNAM, ACCOS, Epad, hôpitaux et CHU. L'étendue du poste est impressionnante. Son titulaire a occupé les mêmes fonctions à Matignon, dans son poste actuel, il dépend lui-même du Haut Fonctionnaire de Défense du Ministère, c'est à dire du Secrétaire Général de ces ministères, pas de la DSI.

Stéphane Nappo, lui, est Global Chief Information Security Officer & Board Advisor, à la Société Générale IBFS. C'est-à-dire la banque de détail à l'international et les services financiers, soit une quarantaine de banques, réparties sur 3 zones géographiques : europe, russie, afrique, avec de la location de flottes, des prêts aux entreprises et de l'assurance. Donc, protéger la confiance des clients et les opérations.

Quelles sont les grandes menaces en 2017 ? Philippe Loudenot estime qu'au lieu de nents, il retient que nous restons fragiles dans le domaine de la santé, sur

les crypto virus. Aujourd'hui, un manque de prise en compte par les directions constitue la plus grande menace, c'est le manque de crise en compte par les directions, un sujet que Gérôme Billois a soulevé par ailleurs. Stéphane Nappo dresse le même constat, la menace est transverse, surtout elle ne se caractérise pas forcément par sa nouveauté, plutôt par sa fréquence et son impact, elle est plus visible et plus dévastatrice.

« *Le meilleur anti-virus c'est quand même le cerveau humain* »

L'IA dont on parle tant est-elle utilisée ? Pour Philippe Loudenot, « *ce n'est pas l'IA qui est utilisée mais la bêtise naturelle de l'humain. Le meilleur anti-virus c'est quand même le cerveau ce qui suppose, d'une, d'en avoir un, et deux, de savoir s'en servir. De temps en temps, nous avons par exemple un cadre qui vous dit : « j'ai cliqué sur un mail en italien mais ne je ne comprends pas cette langue ». Il pense qu'en cliquant, il va mieux parler italien, en fait, en cliquant il a pourri tout un système, toute son organisation* » !

Pour Stéphane Nappo, les cyber-technologies ont trois visages. C'est d'abord le visage du progrès, c'est formidable pour développer les nouveaux services, pour que vous ayez une banque dans la poche et qu'on la sécurise. « *C'est aussi le visage de la weaponization, l'armement, ces technologies servant à nous attaquer et comme elles rapportent beaucoup d'argent aux pirates, on se bat dans une lutte asymétrique, pour les pirates c'est un moyen de gagner des millions d'euros, pour nous c'est un moyen d'économiser de l'argent. Et de protéger la confiance de nos clients. Fort heureusement le troisième visage dans ce triptyque c'est la défense, il faut lutter à armes égales et l'IA est le moyen de ne plus courir et donc d'avancer à la même vitesse que le pirate et d'agir clairement avec des robots face à des gens qui utilisent des robots* ».

Les cybercriminels achètent-ils sur Internet ? Sur son secteur, Philippe Loudenot ne l'a pas constaté aujourd'hui. « *Je vais citer ce qui se fait aux ministères sociaux, la mise en place non pas d'un SOC mais d'un SOA, à quelques personnes nous récupérions les informations pour appuyer les petites structures. On a trop tendance à confier la sécurité aux DSI, je ne vais pas me faire des amis dans la salle, mais cela peut s'avérer aussi dangereux que de confier un rasoir à un singe. Dans le domaine de la santé, les infractions entrent pour la plupart par le matériel bio médical, par les matériels d'infrastructures, par la gestion énergétique ou de fluide. Or la DSI ne voit que le matériel IT ou l'informatique de gestion. Quand on ne prend pas la sécurité numérique dans son ensemble, on se prépare à des jours qui seront grinçants* ».

« *Il faut surveiller le clean business* »

Stéphane Nappo explique que parmi les tentatives qu'on peut observer à l'international, pour les services financiers, on voit que les hackers ont achevé avec succès leur transformation digitale. « *Ils font du cloud, on peut acheter un DDOS pour 30 dollars, on voit également des crypto virus qui se revendent à l'unité ou par licence et je voudrais attirer l'attention de tous ici, les security manager doivent partager plus d'informations, dans le respect de notre devoir de réserve, les pirates s'orientent vers un clean busines. Ils souhaitent comme l'a dit Gérôme Billois, prendre notre information pour la revendre ensuite, à vos enfants ou à des gens qui ne sont pas forcément des criminels, mais vont acheter une licence Adobe un jeu ou autre, donc il faut surveiller ce clean business, ce ne sont pas seulement des gens qui manipulent de l'argent. On fait très attention à la Société Générale, mais aujourd'hui tous les acteurs qui*

manipulent de l'information ou de l'argent vont être concernés par des attaques, vous serez attaqués si vous possédez de l'information, tout ce là coûte de l'argent ».

Si on interroge les deux intervenants sur la question des budgets, les réponses sont également très voisines, malgré des contextes différents. Pour Philippe Loudenot ce n'est pas qu'une histoire d'argent, si on commence à penser uniquement d'argent ça veut dire qu'on met des briques et des boîtes, il faut savoir ce que l'on veut faire. Faire une analyse de risque, quelques simples mesures d'organisation permettent d'assurer la sécurité. Mais, à un moment donné il faut savoir ce que l'on veut protéger, avec quels risques. « *Et arrêter d'agiter le chiffon rouge, ça tout le monde sait faire. Les questions techniques évidemment la direction s'en fiche, en revanche si on arrive à lui sortir les impacts métiers, c'est nettement mieux. Je pense que la transformation numérique c'est remettre l'humain et les métiers au centre des débats. Je vois trop de RSSI dans mon périmètre qui réagissent instinctivement en disant on va mettre des boîtes* ».

« *Il y a peu de temps, j'ai eu une réunion avec un de mes opérateurs, pas de problème de sécurité dit-il tout est dans le datacenter, c'est nickel. Mais c'est comme si vous mettiez un bifteck périmé depuis trois mois dans un réfrigérateur neuf, c'est pas ça qui va le protéger de l'intoxication alimentaire* ».

« *Traiter la menace comme quelque chose de volatile* »

Selon Stéphane Nappo, l'argent n'est pas directement un moyen de protection, ce qui est important c'est l'adéquation entre ce que vous faites, la menace, et votre appétit aux risques. Si dans telle ou telle région vous avez une menace de type chinoise, russe ou autre ou des contestataires, il va falloir se protéger. Il y a une menace facile à traiter, mais la menace c'est souvent le reflet de nos vulnérabilités, on voit souvent plus dans les dernières attaques que les opportunités d'attaques sont créées ou engendrées par nos vulnérabilités ou notre retard sur les mises à jour. « *Donc, il ne faut pas traiter la menace avec de la peur mais la traiter comme quelque chose de volatile. L'armée américaine a une approche pour les processus volatiles, parce que la guerre n'est plus quelque chose où on se donne rendez-vous à tel endroit et à telle heure, ça peut arriver de n'importe où. La cybersécurité c'est pareil, c'est une approche de la vulnérabilité, la crainte ne suffit pas, il faut s'orienter vers des basiques* ».

La prévention c'est capital, vos mots de passe, installer les mises à jour coûte moins que de ne pas les installer, et derrière il faut vérifier votre appétit aux risques. Qu'est-ce que vous voulez manger qu'est-ce que vous pouvez digérer comme risques, je vous rappelle qu'un banquier c'est un professionnel, du risque, le profit de nos opérations financières aux travers des vôtres c'est une prise de risque. Je veux qu'on parle de l'argent comme d'un moyen, et donc qu'on en parle peut être moins souvent, qu'on parle avant tout du rôle du RSSI pas un policemen mais un diététicien du risque, ça c'est un risque qu'on ne peut plus prendre pour nos fonds propres ou notre réputation, là c'est un risque qu'on peut digérer, faire accepter au board, ça ce sont des mitigations on doit se protéger prendre aux médicaments, ce rôle est vital, c'est le digital qui est notre levier de développement et où le risque est le plus important, le RSSI est le RSSI du oui pas celui du non.

Le RSSI est-il celui qu'on contourne ? Pour Philippe Loudenot : « *je vais avoir du mal à vous répondre ça fait des années que je me bats pour que le RSSI soit celui qui dit « oui », ou « oui mais », oui je vous accompagne si on ne prend pas les nouveautés et les enjeux métier d'entrée de jeu, je pense que on s'est trompé de métier et d'objectif,*

j'aime beaucoup l'image du RSSI diététicien, car c'est accompagner ».

Primo vaccination et piqures de rattrapage

Quels sont leurs chantiers prioritaires, ceux de 2017 ou ceux de 2018 ? Philippe Loudenot estime que c'est d'abord la primo vaccination, pour la plupart des dirigeants d'organismes et des piqures de rattrapage régulières pour la prise en compte du risque numérique, cette prise en compte doit faire comprendre que la sécurité est affaire de tous. « *Je ne fais pas de pub mais il y a un très bon film de HP, The Wolf sur ces sujets* ». Ne plus avoir de RSSI permet de se poser les bonnes questions, l'homme central c'est le RSSI ce n'est plus le pirate.
« A la Société Générale, à l'international comme partout, on va continuer à travailler sur la conscience du risque, les nouvelle menaces et leur impact. On a commencé et on continue à travailler sur la conscience du risque, il y avait il y a quelques années le risque de conformité, ou de contre-partie aujourd'hui le risque arrive aussi sur la régulation avec par exemple GDPR, un bon exemple voilà nous allons aussi travailler à ne pas lutter aujourd'hui avec les armes d'hier, on a eu une vision rétrospective du risque, en calculant les pertes, en regardant de manière factuelle, il faut maintenant regarder les nouvelles menaces, le pirate se bat avec un arsenal couteux et perfectionné ».

« *Quand on est attaqué par un robot informatique qui commet des centaines d'intrusions à la minute, poursuit Stéphane Nappo, c'est compliqué d'agir, le modèle on cherche à le simplifier, le pirate il a un coup d'avance sur tout le marché des solutions de sécurité. Pour la Société Générale c'est une source d'inspiration pour avoir un temps d'avance, voilà nos chantiers pour 2018* ».

Partager les signaux faibles

Dans le monde de la santé, rappelle Philippe Loudenot, depuis le 1er octobre il y a obligation dans la loi de déclarer tous les incidents permettant de capter un ensemble de signaux faibles, manière de réagir aux nouvelles menaces. « *C'est aussi être capable de partager dans un espace de confiance les différentes menaces et je suis ravi du fait que les ministères sociaux soient le 1er secteur à avoir annoncé les impacts des crypto virus en 2014 tout ça parce qu'il y avait différents signaux faibles, on retrouve la même ambiance au Cesin où on peut échanger entre pairs et voir un ensemble de signaux faibles les partager et savoir ce qui va nous tomber sur le coin de la figure* ».

« *Il est possible de travailler avec des start-ups, analyse Philippe Loudenot, en France nous avons des pépites magnifiques, mais confrontées au code des marchés publics c'est un peu gênant, car à partir du moment où elles n'ont pas un chiffre d'affaires suffisant, une ancienneté suffisante, elles sont difficilement éligibles. Pour montrer patte blanche c'est encore un peu compliqué* ».

En savoir plus

- Télécharger l'étude *Quelle gestion des risques face aux défis de la cybersécurité ?*
- Contenus associés à la conférence *Cybersécurité : nouvelles menaces, nouvelles solutions* (Mises à jour régulières)

Alain Bouillé (CESIN) : « la sécurité n'est pas nécessairement au rendez-vous dans le cloud »

Lors de la conférence « Cybersécurité : nouvelles menaces, nouvelles solutions » organisée par CIO le 21 novembre 2017 à Paris, Alain Bouillé, président du CESIN a été le Grand Témoin.

Alain Bouillé, président du CESIN (Club des Experts de la Sécurité de l'Information et du Numérique), a été le Grand Témoin de la conférence « Cybersécurité : nouvelles menaces, nouvelles solutions » organisée par CIO le 21 novembre 2017 à Paris.

Né il y a cinq ans avec une soixantaine de membres, le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) a récemment fêté son 350ème membre. Ce club fédère des RSSI (et fonctions similaires) dans les entreprises. Son président, Alain Bouillé, par ailleurs Directeur Sécurité des SI Groupe du Groupe Caisse des Dépôts, a été le Grand Témoin de la conférence « Cybersécurité : nouvelles menaces, nouvelles solutions » organisée par CIO le 21 novembre 2017 à Paris.
Le CESIN organise de nombreux travaux entre pairs. Mettre des pairs d'accord entre eux sur les sujets de cybersécurité, c'est bien. Mais qu'en est-il des directions générales, des directeurs financiers ou même des DSI ? « Cela fait beaucoup de gens avec qui il faudrait être d'accord » a reconnu Alain Bouillé. Mais l'intensité des menaces est un bon facteur de mobilisation de toute l'entreprise. Et le bruit fait par les cyber-attaques remonte bien jusque dans les Comités Exécutifs.

Faites du bruit !

Avec son enquête annuelle le « Baromètre des Menaces », le CESIN a pu montrer que 85 % des entreprises ont déclaré avoir subi au moins une cyber-attaque conséquente,

30 % en ayant subi plus de 15. Alain Bouillé a précisé : « la menace se rapproche et il est clair que, ici, nous ne parlons pas d'un anti-virus qui aurait détecté quelque chose dans un mail, bien d'une pénétration réelle ayant entraîné des dégâts et du bruit. » Ce bruit remonte parfois d'ailleurs jusqu'en Conseil d'Administration.
Ce niveau, dans les entreprises, n'entendaient parler d'informatique, jadis, que lorsque le DSI venait faire sa présentation annuelle ou semestrielle sur les projets Legacy, surtout ceux dépassant les budgets et les délais. Aujourd'hui, le Digital a rendu l'informatique « un peu plus sexy » et, du coup, pour Alain Bouillé, « on peut aussi parler de sécurité. Comme on le martèle, le Digital ne se fera pas sans sécurité. Mais il vaudrait mieux que le sujet n'arrive pas au Comité Exécutif via une attaque mais plutôt par des bonnes nouvelles. » Les entreprises conscientes d'avoir été attaquées sont évidemment plus sensibles. Le DSI parle plutôt budget et impact sur les plannings avec le RSSI. Le CDO a au moins l'avantage de parler d'impact sur les usages.

Pour une conception orientée sécurité dès l'origine

Mais le message du RSSI au CDO est clair pour Alain Bouillé : « ou bien le développement des démonstrateurs est fait proprement dès le départ, avec prise en compte de la sécurité *by design*, ou bien la mise en production supposera un redéveloppement complet. » Le coût est alors évidemment différent. Mais le second choix reste possible, avec des avantages évidents de timing et d'agilité, pourvu qu'il soit assumé ! Le digital a, de toutes façons, l'avantage d'être généralement une surcouche au SI. Une bêtise est donc aisée à isoler le cas échéant.
Il en est tout autrement avec des outils ayant accès au coeur du SI, notamment les terminaux mobiles. Les outils collaboratifs ou autres en SaaS, le cloud d'une manière générale, posent aussi des soucis de base : les données sont par définition en dehors de l'entreprise. Il ne peut plus être question de sécurité périmétrique pour ces parties du SI. « Les frontières de l'entreprise ont totalement explosé et bien malin serait aujourd'hui celui qui serait capable de dire où sont exactement ses données et comment précisément elles sont traitées » a soupiré Alain Bouillé. Mais il a voulu tordre le cou à une idée reçue : « la sécurité n'est pas nécessairement au rendez-vous dans le cloud. Il est faux de dire, si vous êtes une grosse entreprise (pas si vous être une petite PME), que chez Monsieur Microsoft, Monsieur Salesforce ou Monsieur Google, la sécurité serait meilleure que chez vous. » D'autant que les mails contenant des données sensibles sortent désormais de l'entreprise avant d'éventuellement y retourner pour un échange entre bureaux.

Le cloud n'est pas la panacée de la sécurité

Ces outils mutualisent en effet la sécurité entre ses clients avec un effet d'alignement, peut-être pas sur le bas, mais au mieux sur un niveau médian. Quand on a des exigences très fortes de sécurité, soit il faudra renoncer à recourir au cloud, soit il faudra acheter des solutions de sécurité à rajouter, avec un coût associé. « Par exemple, si vous voulez un anti-spam sur Office 365, vous n'aurez jamais l'efficacité de l'outil que vous pouviez personnaliser en interne et vous devrez en ajouter un à celui fourni en standard... garanti contractuellement (en petites lignes) uniquement pour la langue anglaise ! » a cité Alain Bouillé. Le CESIN a donc réalisé un vademecum de recommandations et de précautions à prendre pour le cloud. Alain Bouillé a plaisanté : « le cloud, c'est comme le mariage. Le mariage, c'est résoudre à deux des problèmes que l'on n'avait pas seul. Le cloud implique lui aussi de résoudre des problèmes que l'on n'avait pas avant. »
Mais insister ainsi sur tous les problèmes du digital, du cloud, bref de tout ce qui est à

la mode n'est-il pas transformer le RSSI en « Monsieur Non » ? « On n'est plus dans cette position » a voulu rassurer Alain Bouillé. Mais le shadow-IT, qui entraîne par définition des fuites de données, est de fait davantage une préoccupation du RSSI que du DSI. Ce qui est dommage. Car aujourd'hui le SI Legacy reste le socle, le digital-cloud officiel vient par-dessus et il faut ajouter le shadow cloud. Quand on mène un recensement des services cloud inconnus utilisés via des solutions dédiées, on arrive souvent à près d'un millier dans une entreprise d'une certaine taille, parfois plus de 1500. Le patrimoine immatériel de l'entreprise se retrouve ainsi dispersé aux quatre vents.

Et le GDPR...

De plus, actuellement, le RSSI se voit confronté au GDPR. « Même si je frôle l'overdose » a soupiré Alain Bouillé, se plaignant de recevoir quotidiennement quantité de messages sur le sujet, surtout des propositions commerciales de solutions techniques (aucune solution technique n'étant une solution magique à la question de la conformité GDPR) ou de cabinets de conseil inconnus. Mais le rôle exact du RSSI au sujet du GDPR est variable et dépend notamment de la répartition des tâches et de l'entente entre RSSI et CIL/DPO. Mais il reste exact que la difficulté principale du GDPR relève de la sécurité. Alain Bouillé a confirmé que « il faut que le RSSI et le CIL/DPO se parlent, et se parlent intelligemment, même si ce n'est pas le cas dans toutes les entreprises. Le RSSI doit en effet assurer la sécurité de toutes les données, même celles qui ne sont pas personnelles. Or, si on écoute certains CIL, il ne faudrait s'occuper que des données personnelles... »
La démarche doit donc être équilibrée. Alain Bouillé a surtout regretté qu'une telle réglementation ait été nécessaire : « quand une réglementation de ce genre arrive, c'est que quelque chose a été raté avant, dans nos approches et systèmes de protection. » En mai 2018, il faudra donc être conforme... même si rien ne se passera dans les jours qui suivront l'échéance. Pour Alain Bouillé, le chantier GDPR est une évidence. Mais il ne doit pas tout monopoliser.

En savoir plus

- Télécharger l'étude *Quelle gestion des risques face aux défis de la cybersécurité ?*
- Contenus associés à la conférence *Cybersécurité : nouvelles menaces, nouvelles solutions* (Mises à jour régulières)

Bertrand Lemaire
Rédacteur en chef de CIO

Cybersécurité et RGPD : le rôle du RSSI/CISO remis en question

Lors de la conférence « Cybersécurité : nouvelles menaces, nouvelles solutions » organisée par CIO le 21 novembre 2017 à Paris, Mahmoud Denfer (Vallourec), José Perez (Allianz France) et Henri d'Agrain (Cigref) ont témoigné sur la deuxième table ronde (d

Henri d'Agrain (Cigref), Mahmoud Denfer (Vallourec) et José Perez (Allianz) ont témoigné sur la conférence « Cybersécurité : nouvelles menaces, nouvelles solutions » organisée par CIO le 21 novembre 2017 à Paris.

Face aux nouvelles cyber-menaces, il faut apporter de nouvelles solutions. A cela s'ajoute la difficulté d'une mise en conformité avec la nouvelle réglementation européenne sur les données personnelles, le GDPR. Au coeur de ces problématiques, il y a un poste : celui de RSSI (Responsable de la Sécurité du Système d'Information) ou de CISO (Chief Information Security Officer). L'évolution du rôle et du profil de ce poste a été le sujet de la deuxième table ronde de al conférence « Cybersécurité : nouvelles menaces, nouvelles solutions » organisée par CIO le 21 novembre 2017 à Paris.
Ont témoigné sur cette table ronde trois spécialistes. Le premier était Henri d'Agrain, Délégué Général du CIGREF, association regroupant 145 très grands comptes français mais aussi ancien dirigeant-fondateur du CHECy (centre des hautes études du cyberespace), ex-président de Small Business France et, auparavant, officier de marine responsable de sujets SI/Télécom. José Perez, RSSI de l'assureur Allianz France, et Mahmoud Denfer, Global CISO du producteur de tubes pour environnements contraints Vallourec, présent dans 23 pays avec 24 000 utilisateurs et 80 sites.

RSSI ou CISO, une fausse différence ?

Tout d'abord, de qui parle-t-on ? RSSI et CISO sont-ils bien la même personne, avec un acronyme français ou anglais ? « Mis à part la différence de langue, le terme CISO [illegible] problématique plus ouverte que ce que couvrait au départ celui de RSSI, le

CISO étant davantage tourné vers une problématique métier et le RSSI plus vers de l'opérationnel » a estimé Mahmoud Denfer. Mais il a aussitôt nuancé : « cette différence n'existe plus aujourd'hui ».
Dans une entreprise industrielle présente dans des pays comme la Chine ou la Russie, telle que Vallourec, la sécurité informatique représente des défis particuliers. La conformité réglementaire et la culture de la protection de l'information varient beaucoup d'un pays à l'autre, sans négliger, parfois, l'impact d'influenceurs officiels ou militants, de secteurs d'activité, etc. « Il y a parfois des trains de mesures que nous sommes amenés à prendre mais qui peuvent être en contradiction les uns avec les autres » a relevé Mahmoud Denfer.

Gérer les risques avec le DSI

« Trop longtemps, le RSSI a été vu comme Dr No, c'est à dire celui qui dit non, mais plus vous bloquez quelque chose plus on voudra contourner l'interdiction et passer par ailleurs » a observé quant à lui José Perez. Le métier trouve toujours une réponse à son besoin. Et, le cas échéant, cela signifiera une situation totalement hors de contrôle avec du shadow IT. José Perez en a déduit : « il vaut donc mieux accompagner qu'interdire. » Les contraintes réglementaires interpellent cependant tous les métiers : dans une entreprise de plus de 110 milliards d'euros de chiffre d'affaires, une amende de 4 % pour non-conformité RGPD fait rapidement une jolie somme (4,5 milliards d'euros). Du coup, les RSSI sont sollicités par tous. Traiter les données client de manière un peu cavalière n'est plus acceptable et les métiers en sont bien conscients.
Les entreprises membres du Cigref, très grands comptes, ont toutes les mêmes préoccupations. Au sein de l'association, DSI et RSSI sont amenés à travailler ensemble sur cette problématique de sécurité. « Evidemment, les DSI sont directement concernés par la sécurité du SI ; la plupart sont membres du ComEx et sont challengés par le Conseil d'Administration » a insisté Henri d'Agrain. Les DSI doivent rendre des comptes sur cette question alors même que la transformation numérique est au coeur de la stratégie des grandes entreprises. La préoccupation de conformité réglementaire est aussi un sujet pour le Conseil d'Administration et le RGPD est évidemment dans le viseur actuellement. Le Cigref, l'AFAI et Tech'In France ont d'ailleurs récemment publié un vademecum sur le GDPR.

La sécurité à l'ère du Digital

Au sein du CESIN (Club des Experts de la Sécurité de l'Information et du Numérique), un club de RSSI, les travaux autour de ces sujets sont encore plus centraux. « Et on peut y confronter les approches de différentes entreprises ou de différents secteurs » s'est réjoui Mahmoud Denfer. Parmi les thèmes très actuels, il y a bien sûr le « digital ». Celui-ci vient s'ajouter, avec sa dimension nécessairement agile, à un système Legacy plus lourd. Protection des données, protection du patrimoine, mais aussi élimination des silos : le digital doit atteindre tous ces objectifs.
« Aujourd'hui on ne sécurise plus un logiciel unitairement mais un produit final délivré » a jugé Mahmoud Denfer. Toutes les équipes liés à un projet sont désormais en charge de la sécurité. Et le RSSI/CISO se retrouve davantage comme un expert et un conseil que comme une autorité. Il est là pour amener un partage des leçons dans des contextes variés (par exemple, les quantités de données et les traitements ne seront pas les mêmes entre B2B et B2C) pour les appliquer de manière pertinente dans chaque cas. Mahmoud Denfer a observé : « si une donnée n'est pas sécurisée, cela peut prendre des proportions importantes... »

Les postures, ennemies des RSSI

« Malheureusement, malgré les postures prises sur la nécessité de détecter les risques dès le départ des projets, on continue de saisir le RSSI à la fin... » a soupiré José Perez. Grand optimiste, il continue de croire que les bonnes pratiques seront un jour adoptées. Cela dit, les projets amenés en fin de course au RSSI prennent tout de même en compte, aujourd'hui, la préoccupation de sécurité. José Perez a soupiré : « on peut alors en général redresser l'arbre qui partait du mauvais côté. » Et de plus en plus de projets sont menés en intégrant la préoccupation de sécurité dès l'origine. « Ce n'est plus le RSSI qui amène la contrainte mais les porteurs du projet qui la font leur » s'est-il réjoui. Pour José Perez, il faut savoir expliquer aux métiers que tout ce qu'ils veulent faire est parfaitement possible tout en étant totalement sécurisé pourvu que l'on prenne les précautions nécessaires.

Alain Bouillé, président du CESIN et Grand Témoin de la Matinée, a conclu la table ronde et la conférence. Il s'est notamment réjoui de l'entrée du sujet de la cybersécurité au Comité Exécutif mais cela suppose pour le RSSI d'un côté d'adopter un discours orienté business mais, de l'autre, de rester profondément un technicien, un expert de la sécurité. Cette expertise est particulièrement nécessaire pour bien décrypter les contrats avec les prestataires cloud sur le plan de la sécurité.

En savoir plus

- Télécharger l'étude *Quelle gestion des risques face aux défis de la cybersécurité ?*
- Contenus associés à la conférence *Cybersécurité : nouvelles menaces, nouvelles solutions* (Mises à jour régulières)

Bertrand Lemaire
Rédacteur en chef de CIO

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 : Bertrand Gros
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