113

CIO.FOCUS

Mars 2016

Cybersécurité : faire face aux nouvelles menaces contre le système d'information

En bref

Les systèmes d'information n'ont jamais été autant menacés. Et pourtant, les isoler dans des forteresses est toujours moins envisageable. Comment malgré tout assurer leur sécurité ? Le sujet a été largement débattu au cours de la Matinée stratégique CIO du 16 février 2016 sur le thème "Cybersécurité : Les nouvelles menaces contre le système d'information". Les différentes interventions sont ici synthétisées.

Sommaire

Stratégie
La cybercriminalité est passée en phase industrielle

Stratégie
Contrer les cybermenaces actuelles sur les systèmes traditionnels comme sur les objets connectés

Stratégie
La cybersécurité vue par le duo DSI / RSSI

Projets
Le RSSI du PMU ne vit pas en chambre close

Projets
Comment recruter, retenir et manager des équipes sécurité ?

Stratégie

La cybercriminalité est passée en phase industrielle

François Beauvois, Commissaire de police, Chef de la Division Anticipation, Sous-Direction de la lutte contre la cybercriminalité, Direction centrale de la police judiciaire, est intervenu sur la Matinée Stratégique « Cybersécurité » du 16 février 2016.

François Beauvois, commissaire de police spécialiste en cybercriminalité, a apporté son expertise lors de la Matinée Stratégique CIO « Cybersécurité : les nouvelles menaces contre le système d'information » à Paris le 16 février 2016.

La cybercriminalité est l'un des freins majeurs à l'adoption et au développement de services en lignes, notamment dans le cloud, tant par les particuliers que par les entreprises. Comment parler de cette menace sans tomber dans le strictement anxiogène ?

Peut-être en décrivant la réalité tout en expliquant ce que fait la police. C'était le défi relevé par François Beauvois, Commissaire de police, Chef de la Division Anticipation à la Sous-Direction de la lutte contre la cybercriminalité de la Direction centrale de la police judiciaire, lors de la Matinée Stratégique CIO « Cybersécurité : les nouvelles menaces contre le système d'information » à Paris le 16 février 2016. Il est ainsi revenu sur l'industrialisation de la cybercriminalité.

La Direction centrale de la police judiciaire (DCPJ), créée par Georges Clémenceau, a eu, dès l'origine, la mission de rendre plus sures les routes à l'orée du vingtième siècle. Une centaine d'années plus tard, sa mission comprend également la sécurité des autoroutes de l'information. Le rôle particulier de la Sous-Direction de la lutte contre la cybercriminalité (SDLC-DCPJ) a été expliqué en juillet dernier par Catherine Chambon, sa sous-directrice. En particulier, la BEFTI dépend de la Préfecture de Police de Paris et n'est pas rattachée à la DCPJ. La SDLC-DCPJ s'occupe uniquement des formes organisées et transnationales de cybercriminalité, en plus d'être un service support spécialisé pour les autres divisions de la police. « Les groupes organisés de cybercriminels peuvent dériver jusqu'à de véritables mafias » a relevé François Beauvois.

Un manque de prise de conscience

Le 8 février, nos confrères *Les Echos* titraient : « La France dans le top cinq des pays où Internet est le moins sûr ». Projetant l'article, François Beauvois a ironiquement posé la question : « et que fait la police ? » Mais, avant que la police puisse intervenir, il faut que les victimes potentielles se rendent compte que leurs biens ont de la valeur et adoptent un minimum de bonnes pratiques.
Or une étude, citée par le commissaire et réalisée par l'éditeur Trend Micro, a établi que les citoyens attribuent des prix extrêmement bas pour leurs données, surtout en France, d'où un certain je-m'en-foutisme. Les informations de santé sont celles qui sont les plus valorisées, surtout pour les Américains. « On commence à voir quelques affaires dans ce domaine » a relevé François Beauvois. Il est vrai que la réglementation française protège fortement les particuliers en cas de piratage, par exemple du numéro de carte bancaire. Pour les entreprises, les premiers risques sont classiques : mauvaise réputation, perte de confiance de consommateurs, etc.

Mais certains risques sont négligés par les entreprises. Ainsi, si un serveur web est piraté, il peut héberger des contenus illicites. « Certaines entreprises se retrouvent à héberger des contenus pédo-pornographiques tous les mois » a pointé François Beauvois. Dans ce genre de cas, les services de sécurité s'aperçoivent du problème en général assez vite. Plus subtil peut être l'hébergement de codes malicieux injectés sur un site web légitime, transformant le site web de l'entreprise en site de rebond pour la diffusion de malwares.

Quand le cauchemar devient réalité

Très souvent, on parle de risques, y compris des risques qui viennent d'être mentionnés. Mais François Beauvois a préféré raconter de véritables cas concrets, « quand les risques se réalisent ».

Un hacker avait piraté le compte d'un informaticien en 2010. Mais, en 2014, cet informaticien est devenu administrateur réseau d'une société. « Et les codes sont toujours bons » a soupiré le commissaire. Résultat : le pirate n'a plus seulement accès à l'ordinateur personnel de l'informaticien mais au réseau complet de son employeur. Dans ce cas, le hacker a voulu faire chanter l'administrateur. François Beauvois s'est réjoui : « pour le coup, l'administrateur a eu le bon réflexe et nous a aussitôt appelés car dès que l'on met les doigt dans le chantage, c'est fini. » En remontant les pistes, la police trouve des traces en Allemagne et en Roumanie. « Heureusement, les victimes ne sont pas les seules à être naïves, les auteurs aussi » a persiflé le commissaire. En l'occurrence, l'auteur a pris rendez-vous avec la victime et l'interpellation a ainsi pu être menée sans difficulté. La perquisition réalisée par la police allemande a permis de retrouver la base de données volée à la victime (ce qui évite les doutes sur la culpabilité personnelle) et 1,7 million de numéros de cartes bancaires.

Autre affaire : le piratage d'IPBX. « Avec IP, on peut facilement se faire pirater son téléphone, ce qui n'était pas simple avant » a remarqué François Beauvois. Le principe est ici de souscrire un numéro surtaxé (« Premium Rate Service ») dans un pays off-shore à la réglementation quasi-inexistante puis de pirater un IPBX pour lui faire appeler le dit numéro du vendredi 19h au dimanche 23h. Puis l'entreprise reçoit la facture de son opérateur favori. Le commissaire a soupiré : « pour un tel piratage, il n'est souvent pas nécessaire d'avoir réussi une thèse en informatique puisqu'il suffit de

taper admin/admin comme identifiant/mot de passe dans trois cas sur quatre. » En général, l'IPBX a été installé à la va-vite plusieurs années auparavant et plus personne ne s'en est occupé. Bilan selon le commissaire : « 11 individus, 4 mois, 3 millions d'euros ». La piste partait de Londres, revenait à Paris puis à Amsterdam et, à la chaîne, dans d'autres pays. L'affaire est actuellement en cours d'instruction.

Des modes de transferts de fonds avec des méthodes sophistiquées

Troisième affaire : les malwares. « Les bons vieux virus du temps jadis, dès la fin des années 70, qui se contentaient de détruire sont devenus des engins très complets qui font tout, de la backdoor au keylogger, se déployant furtivement dans un système » a décrit François Beauvois. Ces malwares évoluent régulièrement et frappent massivement, les maillons faibles cédant en premier. Le temps n'est plus au duel ciblé mais à la mitrailleuse qui arrose indistinctement.
Pour le commissaire, « le pire est le cryptolocker qui chiffre vos données et, là, vous avez beau être assuré, les documents de travail sont perdus. » Les mails pour inciter à cliquer sur des liens infectés sont aujourd'hui plus propres et convaincants que ceux d'hier en provenance d'un directeur de banque centrale africaine avec une faute d'orthographe par mot. Le risque est donc élevé. Et, pour déchiffrer les données (documents bureautiques en premier lieu), il faut payer une rançon avec des « méthodes de trafiquants de drogue » pour dissimuler les vrais destinataires. La meilleure protection contre ce genre d'attaque est une sauvegarde... un cryptage professionnel étant quasi-impossible à casser.
Des documents bureautiques envoyés peuvent obliger à activer les macros pour être lus. Or une macro peut télécharger ensuite le code malicieux. Certains malwares sont très vicieux comme Dridex qui se dissimule dans la RAM et pas sur le disque dur. A l'extinction, il se sauvegarde dans une clé de registre. « La meilleure désinfection passe alors par une coupure brutale d'alimentation électrique, même si c'est un peu léger comme politique de sécurité informatique » a remarqué . Dridex vole les codes d'accès à des services en ligne. Les attaques se font par vagues, la France et la Grande Bretagne étant actuellement visées.

Une collaboration public-privé

L'argent passe soit par des règlements en bitcoins (qui peuvent alors être tracés), soit par des « mules ». Les « mules » sont des gens qui acceptent l'offre alléchante de « travailler sur Internet de chez eux quelques heures par mois pour 4000 euros », c'est à dire d'ouvrir un compte bancaire à leur nom, d'y recevoir l'argent des victimes puis de le reverser en liquide à des commanditaires. Jusqu'au jour où ils se font interpeller pour escroquerie en bande organisée.
Actuellement, pour faire face à ces formes de plus en plus sophistiquées de cybercriminalité, la DCPJ monte une nouvelle division sous la direction de François Beauvois. Celle-ci aura comme particularité de fonctionner avec des partenaires privés dépositaires d'une expertise.
Interrogés via Evals.fr, seuls les deux-tiers des participants de la conférence ont admis prendre en compte actuellement la cybercriminalité dans leur entreprise. Il y a donc encore bien du travail à faire en la matière.

En savoir plus

- Télécharger les contenus associés à la Matinée Stratégique *Cybersécurité : les nouvelles menaces contre le système d'information* organisée par CIO le 16 février 2016.

- 10 juillet 2015 : Catherine Chambon (SDLC-DCPJ) : « gardez sur Internet le même bon sens que dans la vie physique ! »

Bertrand Lemaire
Rédacteur en chef de CIO

Stratégie

Contrer les cybermenaces actuelles sur les systèmes traditionnels comme sur les objets connectés

Frédéric Carricaburu (SFA) et Benoit Guennec (Eedomus) ont témoigné lors de la conférence CIO « Cybersécurité » à Paris le 16 février 2016 (de gauche à droite sur la photo).

Frédéric Carricaburu (SFA) et Benoit Guennec (Eedomus) ont témoigné lors de la Matinée Stratégique CIO « Cybersécurité : les nouvelles menaces contre le système d'information » à Paris le 16 février 2016. Ces deux témoins ont expliqué comment les systèmes d'information classiques et les objets connectés devaient être protégés contre les nouvelles cybermenaces.

Sur la Matinée Stratégique organisée par CIO le 16 février 2016 et consacrée au thème « Cybersécurité : les nouvelles menaces contre le système d'information », deux témoins sont intervenus sur une table ronde pour expliciter les bonnes pratiques pour protéger les systèmes d'information contre les cybermenaces actuelles. Même si, bien entendu, aucune protection n'est absolument inviolable, il faut se préoccuper de minimiser les risques autant pour les systèmes d'information au sens traditionnel que pour les évolutions récentes telles que les objets connectés.

Le premier de ces deux témoins a été Frédéric Carricaburu, DSI et RSSI du groupe SFA, un groupe disposant de 23 implantations internationales et trois sites différents de production en France. Connu grâce à son sanibroyeur grand public, SFA est une société aux activités bien plus larges. On y côtoie aussi bien la fabrication de produits pour le bâtiment (pompes, broyeurs sanitaires, tuyauterie...) que la presse avec le groupe Challenge (Challenge, Sciences et Avenir, Historia...). Les défis de ce premier témoin sont classiques. C'est nettement moins le cas du second : Benoit Guennec, président fondateur de Connected Object qui commercialise la box Eedomus. Cette box vise à piloter un grand nombre d'appareils électroménagers ou électriques au domicile

des clients, notamment via des prises électriques commandées. Ces derniers utilisent leurs smartphones, tablettes ou PC et le SaaS du fabriquant. Objets connectés et cloud sont deux défis particuliers à relever dans cette structure légère. Chacun a donc pu témoigner que les cyberattaques ne sont pas que pour les autres.

Un catalogue complet de cyberattaques

« Ransomwares, fraudes au président, cyberattaques issues de divers pays... nous avons eu droit à tout, aussi bien sur notre activité industrielle que presse » a confirmé Frédéric Carricaburu. Le seul point rassurant pour SFA est l'absence, pour l'instant, d'un site e-commerce grand public mais Frédéric Carricaburu ne s'est guère fait d'illusion : « lorsque nous en aurons un, il sera évidemment attaqué. »
La principale leçon qu'il veut retenir de son expérience, c'est la nécessité de tout remettre à plat tous les six mois. « Comme tout le monde, nous sommes partis d'un petit firewall mais nous nous sommes aperçus qu'il était contourné, certains allant même jusqu'à connecter une Freebox sur une prise téléphonique pour se monter une petite salle de marché » a déploré Frédéric Carricaburu. Les smartphones et les objets connectés sont devenus autant de point de fragilité dans la sécurité des systèmes. Pour le DSI et RSSI, « l'enjeu aujourd'hui n'est plus de savoir qui va rentrer mais plutôt ce qui va concrètement sortir, et pas seulement au travers du firewall. Nous avons donc des sondes réseau, une surveillance des surveillants au travers d'un reporting de qui se connecte à quoi, quand, comment... »

Eloge de la simplicité

Par contre, il faut rester raisonnable pour que les systèmes d'alertes soient pertinents. « Par exemple, pour les accès aux mails des VIP, nous n'avons que deux alertes : sur une connexion à partir d'un terminal non-identifié et sur un accès simultané à partir de deux zones géographiques distinctes, sinon c'est ingérable » a expliqué Frédéric Carricaburu.
Les technologies mises en oeuvre sont très variées. Certaines reposent sur des appliances, d'autres non. Cette variété est en soi une nécessité. Le Web Application Firewall, bien que gourmand en ressources, permet ainsi de sécuriser davantage les accès à des applications. « On ne peut pas se reposer sur le seul VPN car, si on a accès à une application via le VPN, on peut tenter d'avoir accès à d'autres » a averti Frédéric Carricaburu. Si un terminal accédant de manière légitime au VPN est corrompu, les conséquences peuvent donc être dramatiques et des protections complémentaires s'imposent.

Les objets connectés sous la menace

La corruption d'un système informatique peut avoir des conséquences, aujourd'hui, jusqu'au domicile de particuliers via des objets connectés domestiques. La box Eedomus, par exemple, se connecte d'un côté à Internet et au service web du fabriquant, de l'autre à des objets connectés domestiques, le plus simple étant de simples prises électriques connectées. « Je peux désactiver mon alarme, ouvrir mon portail... avec mon smartphone » a décrit Benoit Guennec, qui revendique 10 000 clients équipés en France. Pour lui, « notre enjeu principal est de concilier les enjeux considérables -l'accès et la sécurité des domiciles- et les moyens d'une toute petite structure comme la nôtre. »
Pour limiter les risques, la box ne peut pas être reliée à une serrure connectée. Cependant, même désactiver une alarme peut mettre en danger un domicile. Bien

entendu, le risque est connu et Connected Object protège ses propres systèmes avec les technologies classiques comme celles évoquées par Frédéric Carricaburu. Mais les risques doivent être remis en perspective : un risque de piratage n'est pas le pire. « Il y a environ 300 000 cambriolages par an en France, ce risque est bien supérieur au risque de se faire pirater son système de surveillance » a observé Benoit Guennec.

Eviter le risque du rapprochement d'informations sensibles

Pour éviter qu'un piratage n'ait trop de conséquence, Connected Object applique une règle qui a fait ses preuves dans les réseaux clandestins de résistance politique : ne pas trop en savoir. Benoit Guennec revendique, sur ce plan, une stratégie inverse de celle d'une banque : « nous ignorons tout de nos clients et nous refusons de savoir qui ils sont, où ils habitent, etc. » En savoir le moins possible est la meilleure protection : ne rien avoir à voler permet de ne pas subir de vol. L'infrastructure qui héberge la boutique en ligne est ainsi totalement séparée et cloisonnée de celle gérant le service de gestion des objets connectés, empêchant de fait un vol de numéros de cartes de crédit en attaquant l'infrastructure du service.
Par ailleurs, si un client se fait voler son smartphone doté de l'application Eedomus pour piloter sa box et, par exemple, éteindre une alarme, il faut encore que le voleur connaisse l'adresse physique concernée. Le lien entre identifiant Eedomus et adresse physique n'apparaît pas dans l'application. Malgré tout, si le cambrioleur est bien informé, le client peut être averti que son alarme a été désactivée à partir de son ordinateur. Il peut alors anticiper le cambriolage en prévenant les forces de l'ordre.

Une bonne pratique : la simplicité

Connected Object est une petite structure et s'assume comme telle. Mais Benoit Guennec a attesté : « nous mettons en place des mesures simples mais nous les mettons réellement en place, comme par exemple le chiffrage des données ou la géolocalisation des utilisateurs qui se connectent. » Si un utilisateur se connecte à partir de Chine, alors qu'il devrait travailler en banlieue parisienne, il est probable qu'il y ait un incident à traiter.
« La simplicité est toujours une bonne chose » a confirmé Frédéric Carricaburu. Pour lui, « plus vous introduisez de la complexité, plus vous introduisez des risques potentiels. La complexité de mène à rien. »

En savoir plus

- Télécharger les contenus associés à la Matinée Stratégique *Cybersécurité : les nouvelles menaces contre le système d'information* organisée par CIO le 16 février 2016.
- Le 7 Octobre 2015 : SFA gère ses VPN et optimise son WAN grâce à son pare-feu

Bertrand Lemaire
Rédacteur en chef de CIO

Stratégie

La cybersécurité vue par le duo DSI / RSSI

De gauche à droite : Martine Guignard du Clusif, Jean-François Louâpre, Cesin, Jean-Paul Mazoyer, Cigref

La cybersécurité n'est pas qu'une affaire de technologies mais aussi de faiblesses humaines et de contraintes financières et juridiques, comme en témoignent les responsables du Clusif, du Cesin et du Cigref. Ils s'exprimaient sur une table ronde durant la Matinée Stratégique CIO du 16 février 2016 consacrée à la cybersécurité.

Pour aborder le sujet des contraintes, la Matinée Stratégique CIO consacrée à la cybersécurité, le 16 février 2016, avait sollicité trois intervenants reflétant le secteur : Martine Guignard, secrétaire général du Clusif (et RSSI de l'Imprimerie Nationale), Jean-François Louâpre co-fondateur et vice-président du Cesin (et Ciso de CNP Assurances), Jean-Paul Mazoyer, Président du cercle cybersécurité du Cigref (et directeur général de la Caisse de Crédit Agricole Pyrénées Gascogne et auparavant directeur informatique et industriel groupe). Trois organismes différents pour une vision globale de la problématique.

Le Clusif compte deux collèges, un de RSSI, l'autre de fournisseurs, avec des axes de travail comme les SOCs, la cyberassurance, les Scada... et même un groupe de travail composé uniquement des RSSI pour parler de leurs problèmes propres de RSSI, « c'est libérateur » note avec humour Martine Guignard. Le Cesin, créé il y a un peu plus de trois ans, fonctionne comme un club de RSSI uniquement. Ses 230 membres, tous RSSI ou directeurs des risques, viennent parler entre eux de problèmes de cybersécurité et aucun livrable n'est publié, seul compte le partage d'expérience, avec des adhérents venus de toutes les tailles d'entreprises et de tous les secteurs d'activité.

Plus connu, le Cigref, créé il y a 47 ans, compte 150 adhérents, grandes entreprises ou associations d'entreprises. Jean-Paul Mazoyer a mis sur pied il y a deux ans le cercle de la sécurité, et il révèle : « pour que la cubersécurité soit un thème mis au-dessus de la pile, les DSI devant se saisir du sujet pour aider les RSSI et convaincre leurs

directions générales ». Au-delà de ce double objectif, le Cigref a engagé une grande campagne de sensibilisation. Elle a pu surprendre, le Cigref s'adressant directement au grand public par des spots télévisés, la « hack academy ». Pourquoi diable, le Cigref, qui est plutôt CAC 40 et zoome très peu aux alentours, s'adresse-t-il au grand public sur ce sujet de la cybersécurité ?

Passer par le grand public

La réponse de Jean-Paul Mazoyer est limpide. Pour lui, le grand sujet est de faire remonter les questions de cybersécurité au ComEx et auprès du PDG ou du DG. Compliqué. Mais à titre personnel, souvent par leurs enfants ou leurs amis ils sont sensibilisés, de même que les collaborateurs de l'entreprise. Conclusion : autant passer par le grand public, en le sensibilisant on alerte la sphère privée des dirigeants d'entreprise. Plus efficace qu'un savant programme interne.
C'est la première fois qu'une campagne nationale d'intérêt public est ainsi financée sur fonds privés. « C'était le meilleur moyen de toucher l'ensemble des salariés et des dirigeants en s'adressant à leur entourage en même temps qu'à eux-mêmes », précise Jean-Paul Mazoyer. Il ajoute : « On s'est mis autour de la table, on a demandé le soutien de l'ANSSI et du cyber préfet, Jean-Yves Latournerie au ministère de l'Intérieur, 25 grandes entreprises ont financé, ensuite on est allé voir les médias. Nous avons déjà fait des serious games, là avec la hack academy, nous jouons un rôle sociétal pour les grandes entreprises, comme, réalité, nous le faisons depuis longtemps. L'essentiel est de créer un mouvement avec les DSI et au-delà pour porter le sujet. »
Le DSI étant porteur des sujets de cybersécurité, comment le Cesin et le Clusif, représentant les RSSI, jugent-ils leurs relations avec eux ? Aujourd'hui, la cybersécurité est une cause nationale qui intéresse tous les niveaux de l'entreprise et tous les citoyens. Ce qui nécessite déjà, aux yeux du Cesin une forte collaboration au sein de l'entreprise. Les deux premiers rôles sont joués par le RSSI et le DSI.
Le Cesin publie en fait un livrable, le baromètre de la cybersécurité, vue par ses membres. « Il y a des années, rappelle Jean-François Louâpre, on parlait de sortir la RSSI de la DSI, aujourd'hui 73% de nos membres sont à l'intérieur de la DSI ». Problème réglé donc.

Pas compris par le DAF

Côté Clusif, le ton se veut plus vif. « On a beaucoup parlé de sensibilisation au Clusif, note Martine Guignard, elle pose un problème, on peut faire des sessions, mais nous n'avons pas que ça à faire, nous avons donc besoin d'outils, or nous ne sommes pas très bien compris niveau budgétaire ! Le RSSI va finalement trouver ses outils, pour cela, il faut embrigader la RH et la Com. Pour avoir des résultats, il faut aussi s'adresser aux utilisateurs à titre personnel, leur parler de ce qui se passe chez eux en matière de sécurité, là ils commencent à comprendre, et vont être sensibilisés.».
La sensibilisation est un grand thème, mais comment se fait-il, demande l'animateur, malgré tous les outils en place, que l'hameçonnage puisse encore passer ? Aujourd'hui note Jean-François Louâpre, on a des équipes qui réussissent dans 85 à 90% des cas, mais les cyberciminels s'en sont aperçus et ne s'intéressent donc qu'aux autres, les 5 à 10%. « Je vous fais la même réponse qu'aux utilisateurs qui expliquent qu'ils subissent encore des spams, aujourd'hui, la cybercriminalité est active et organisée, la police judiciaire parlait de vagues d'attaques Dridex, quand la France a été attaquée c'était sept attaques nouvelles par jour. Avec sept variantes on est à la limite de la technologie, on ne peut pas opposer la technologie et l'utilisateur, il faut effectivement des dispositifs techniques, mais complétés par des dispositifs utilisateurs. Un dispositif

technique mal compris et mal expliqué sera inutile ».
Serait-ce suffisant pour éviter divers contournements, en particulier avec le cloud ? « Aujourd'hui, note Jean-Paul Mazoyer, il est impossible de faire le tri entre les faux mails et les vrais, on trouve de vraies factures et de vrais CV, avec à l'intérieur des spams. J'en ai souvent discuté en interne. Mais allez expliquer au responsable RH ou financier qu'il ne devrait pas ouvrir, c'est impossible. On a des logs malveillants, même quand on les ouvre dans un bac à sable. Ils savent très bien où ils se trouvent et ne s'exécutent pas dans le bac à sable. C'est le jeu du gendarme et du voleur, et c'est une course permanente. Je reprendrai les propos de Alexandre Huard (HP), il n'est pas question de surveiller une forteresse, il y aura toujours quelqu'un pour franchir.

Un risque vital

Reste le sujet de départ, celui posé par Skyhigh en début de séminaire, la sécurité du cloud et l'attitude des directions métiers qui vont dans le cloud, souvent à l'insu de l'informatique. « Le sujet, souligne Jean-Paul Mazoyer, c'est le PDG ou le DG car à quelle vitesse, ce dirigeant se rendra-t-il compte que l'entreprise est bien sur en situation de risque vital ? Je me souviendrai longtemps du témoignage d'Yves Bigot, PDG de TV5 Monde, six mois après l'évènement [un piratage de tous les sites web, NDLR], il avait encore des trémolos dans la voix pour aborder le sujet, dans une conférence où le Premier Ministre avait choisi de la faire intervenir en premier. Le sujet, c'est bien la sensibilisation des ComEx et des dirigeants d'entreprise ». Répondant à une question Evals, il note qu'une entreprise sur six n'a jamais fait d'exercice de cybercrise en présence du dg ou du Pdg.
Le Clusif répond sous un autre angle. Pour Martine Guignard il y a différentes formes de cloud, différentes spécialités. « Je demande régulièrement à faire des tests d'intrusion et je tombe sur des applis poreuses. Exemple, une appli RH pour la formation, peut rendre accessibles les évaluations de tous les salariés ». Les exemples ne manquent pas. Et selon Martine Guignard, « tout le monde n'est pas en mesure de faire des tests d'intrusion, et beaucoup d'offres sur le marché sont lamentables en termes de sécurité ».
Jean-François Louâpre prend le contrepied de ses collègues, « on a trop tendance à opposer cloud et sécurité, le cloud est inéluctable, la sécurité doit s'adapter ». On a tendance aussi à opposer les métiers et la DSI, mais ils ne sont pas seuls en scène. « J'ai tendance à dire, que je passe plus de temps avec la direction juridique qu'avec la DSI, moi RSSI ! »
« En fait, conclut Jean-Paul Mazoyer, nous estimons au Cigref qu'il existe trois types d'attaques : celles liées à l'intelligence économique, tout ce qui relève de l'activisme, c'était le cas avec TV5 Monde, enfin, les malversations financières, c'est là qu'il faut réagir. Mais il ne sert à rien de courir plus vite que le tigre, il suffit de courir plus vite que son voisin, et parier sur la fainéantise du hacker qui s'attaque à ceux qui sont le moins bien préparés » !

Didier Barathon
Rédacteur en chef de Réseaux & Télécoms

Projets

Le RSSI du PMU ne vit pas en chambre close

Farid Illikoud est à la fois RSSI et chargé de la compliance au sein du PMU

Le PMU, c'est non seulement des systèmes centraux mais aussi plus de 12 000 points de vente à surveiller et administrer comme l'explique Farid Illikoud, son RSSI. Il s'est exprimé sur la Matinée Stratégique CIO du 16 février 2016 consacrée à la cybersécurité.

Invité de la Matinée Stratégique CIO du 16 février 2016 consacrée à la cybersécurité comme grand témoin, le RSSI du PMU, Farid Illikoud, a donné un aperçu non seulement des risques affrontés par son entreprise, mais aussi de son propre rôle en interne, Farid Illikoud étant parallèlement responsable de la conformité. Son entreprise elle-même est un sujet évident en termes de sécurité, étant le premier acteur européen du pari et le deuxième au monde.
Le PMU a trois activités : paris hippiques, paris sportifs et poker. 80% des enjeux sont réalisés dans ses 12 200 points de vente, en 2013 c'était 10,4 milliards d'euros d'enjeux, avec 6 millions de clients. PMU.fr est un des premiers sites de e-commerce en France avec 1,7 milliard d'enjeux. La société est n°2 sur les paris sportifs, n°1 sur les sites généralistes proposant une offre poker.

L'activité est génératrice de contacts et de paiements à un rythme très soutenu avec une multitude de points de vente, sans parler des accès Web. Tout le monde connaît le PMU, mais n'a pas forcément une idée de son infrastructure et des risques en matière de sécurité. Le PMU est bien une cible idéale avec une activité particulière, encadrée et règlementée par l'Argel (Autorité de régulation des jeux en ligne) et le Ministère de l'intérieur. « Nous sommes le deuxième réseau de vente en France, derrière La Poste » souligne le RSSI.

La question de la sécurité se pose évidemment. Que ce soit du fait du petit hacker qui souhaite se faire plaisir, ou des attaques DDoS, l'activisme de type Daesh ne peut

épargner des sites de paris. Mais le PMU doit protéger aussi bien ses systèmes centraux que les points de ventes, où se font les paris. Est-ce partout pareil ? « Tout DSI et tout RSSI, répond Farid Illikoud, ne peut se passer des éléments de base : définir une politique, des directives, des chartes. Le RSSI ne vit pas en chambre close, mais avec toutes les directions de l'entreprise. Coté métier aussi, on entend beaucoup parler du numérique, il fait peur avec l'ubérisation telle qu'elle est traitée dans les journaux et ailleurs, mais le résultat c'est l'abolition des frontières entre DSI et métiers, et le fait que tout acteur du numérique, en particulier les nouveaux venus, Chief digital officer ou Chief data officer, tous se rencontrent autour de cette thématique : la gouvernance de la donnée ».

« Je passe du temps avec la direction juridique »

Une fois la politique de sécurité bien définie, le cadre rédigé, il faut le porter auprès de certains métiers. « Aucun projet ne se fait sans analyse de risque au PMU, je passe du temps avec la direction juridique, le contrat est le seul moyen de se retourner. Autre pont essentiel, faire intervenir la direction achat, aucun achat ne peut se faire sans politique de risque ». Mais attention, prévient Farid Illikoud, on est à l'écoute, la sécurité ne saurait être un bloqueur, « je souhaite être un facilitateur de business, comme m'a demandé celui qui m'a recruté, on est là pour apporter des solutions, et aboutir à un meilleur compromis dans une logique de surveillance des coûts et du business ».

Dans la réalité du PMU, cette politique de sécurité doit englober le réseau physique, les cafés et bureaux de tabac dispersés, avec des PC, des terminaux de paiement, des liaisons, à sécuriser. « Le basique c'est effectivement la sécurité des terminaux au PMU, avec, depuis six mois, un projet de big data en sécurité. L'entreprise collecte un maximum d'informations et de logs, et doit les corréler et les croiser, donc intégrer le facteur sécurité, sans oublier l'ensemble des utilisateurs et des points de vente ».

Mais, selon Farid Illikoud, « un outil ne fait pas tout, on sait que si on a pas le triptyque people / process / technologies, on ne fait pas grand-chose. On a des outils, mais on s'aperçoit qu'il fallait de vrais analystes. En France difficile de recruter des sachants sur ce type de poste, on a la culture d'ingénieurs, on a par exemple d'excellents développeurs, ensuite on le passe chef de projet puis directeur, très vite, parce qu'on a peu de profils. On a un outil, ça fait un peu sapin de Noël, ça clignote de partout, mais le meilleur outil ne sert à rien si personne n'est derrière ! »

« Il n'y a pas de risque zéro »

De plus, le secteur est très règlementé, par l'Argel, la Cnil, sous la surveillance des Commissaires aux comptes. Farid Illikoud est d'ailleurs responsable de la conformité, en plus de sa responsabilité en matière de sécurité. « L'Argel voit en temps réel que ça clignote chez nous ». Mais il faut distinguer les évènements des incidents de sécurité, tout ce qui clignote des vrais alertes. Et, dans ce cas, il faut des plans de continuité.
« On a eu de bons plan de lutte, mais pas toujours en intégrant les cybermenaces, donc on a évalué notre CA versus une crise cyber, avec une démarche classique de PCA pour traiter correctement une crise de cyberattaques. De toute façon, il n'y a pas de risque zéro. Ce matin, on avait quelques « visiteurs » chez nous. La question n'est pas si nous allons être attaqués mais comment nous allons faire face à ce qui va se produire. Une attaque ce n'est pas grave, toute entreprise est attaquée à tout moment, il y a ceux qui le savent et ceux qui l'ignorent, il faut toujours procéder en trois étapes :

détecter, remédier, éventuellement et anticiper ».

A une question posée via Evals.Fr sur le nombre d'attaques qu'il subit, Farid Illikoud répond que c'est très variable. Des attaques graves ne surviennent cependant qu'une à deux fois par an, une attaque peut être mineure pour une entreprise et majeure pour une autre. « Ce qu'on redoute le plus, c'est le déni de service, toute notre activité passant sur le réseau. Après, ce que l'on craint le plus, c'est la fuite de données clients, protéger le patrimoine informationnel est donc une priorité ». Dernier point sur lequel Farid Illikoud a tenu à alerter l'auditoire c'est la nouvelle règlementation européenne qui va obliger à notifier toute perte de données, sous peine d'amende.

Mais son action n'est rien sans un environnement. Le ComEx d'abord et le rôle du Pdg « on a fait une campagne de faux pishing, envoyés aux salariés, la réaction de notre Pdg a été géniale, il voulait que le défilement soit plus lent afin que le collaborateur ait encore plus peur en voyant l'avertissement s'afficher sur son écran ». Le RSSI doit également disposer d'un réseau de correspondants sécurité, il ne peut pas être partout, et le numérique est une vraie chance. aujourd'hui la DSI du PMU peut compter sur la direction juridique, la DRH se sent mobilisée par le Byod et la direction du digital veut faire un maximum en matière de sécurité pour consolider ses projets ».

Didier Barathon
Rédacteur en chef de Réseaux & Télécoms

Projets

Comment recruter, retenir et manager des équipes sécurité ?

Patricia Cabot, à droite, Fondatrice du cabinet SPsearch et Caroline Tampigny, à gauche, Consultante associée.

Patricia Cabot, Fondatrice, et Caroline Tanguy, Consultante associée, du cabinet SPsearch expliquent comment recruter, retenir et manager des spécialistes en cybersécurité malgré la pénurie de profils disponibles. Elles s'exprimaient sur la Matinée Stratégique CIO du 16 avril 2016 sur le thème Cybersécurité : Les nouvelles menaces contre le système d'information. Partout dans le monde, le constat est le même : les entreprises n'arrivent pas à recruter suffisamment de spécialistes en cybersécurité.

La cybersécurité est devenue un cauchemar pour les recruteurs. Non seulement en termes de recrutement purs, mais aussi pour retenir et faire évoluer ces talents très particuliers. C'est la thématique choisie pour le quart d'heure du coach DSI qui se tenait en clôture de la matinée-stratégique CIO dédiée à la cybersécurité, le 16 février 2016. Trois questions étaient mises en débat pour cette dernière intervention : quels profils pour quels postes pour gérer la sécurité ? Comment retenir les profils demandés ? Comment manager les ultra-spécialistes de la sécurité ? Trois questions traitées par le cabinet SPsearch, sa fondatrice Patricia Cabot et Caroline Tanguy, consultante associée.

Premier élément de réponse, celui de Patricia Cabot, sous forme d'affirmation forte, « nous évoluons sur un métier vraiment en tension ». Son cabinet SPSearch a l'expérience du sujet, il est spécialisé depuis 2003 sur les métiers de l'IT, mais avant tout comme recruteur par approche directe, sur des métiers souvent en tension, digital, big data, IT en général et donc cybersécurité. Sur l'année 2015, 50% des recrutements du cabinet étaient d'ailleurs effectués sur le sujet cybersécurité.

Pénurie partout dans le monde

Cette tension n'est pas propre à la France, rappelle Patricia Cabot, les marchés en pénurie sont un vrai problème pour les industriels en France, aux Etats-Unis ou partout dans le monde, « on estime qu'il faudrait deux à trois fois plus de spécialistes pour répondre aux violations de la sécurité des systèmes d'information des entreprises ». Les professionnels en sont conscients, ces cinq dernières année le chiffre des demandes pour cette spécialité a progressé de 74% dans le monde et de 37% d'ici 2022. Des chiffres prometteurs, mais il est difficile de se réjouir, en 2015 209 000 offres restaient non pourvues aux Etats-Unis, pour la cybersécurité, un million dans le monde, en France un millier. Ce dernier chiffre parait dérisoire, mais en face on ne forme que 2 à 300 jeunes diplômés sur ce marché hexagonal.

Problème évident de recrutement, mais problème tout aussi flagrant pour retenir ces profils indispensables, comme devait le souligner Caroline Tampigny, consultante associée au cabinet SPsearch. « Oui, ils sont très sollicités, même une fois chez vous, heureux et épanouis, il faut donc comprendre comment les retenir, les évaluer, les motiver ». Ils veulent être challengés, alimentés en termes de projets avec un niveau de complexité suffisante. Leur n+1 doit être d'un niveau technique suffisant et le contenu des projets également de très bon niveau et évolutif en termes de technologies. L'autre grand levier, c'est le travail en équipe, « une vraie demande des candidats qu'on reçoit, ils sont dans une logique d'amélioration mais en équipe, ils veulent apprendre avec leur voisin. »

En recherche passive

Le dernier levier qu'on peut activer, peut-être moins important en apparence, c'est celui des salaires. Il faut toujours être au courant des salaires du marché, recommande Caroline Tampigny et essayer d'être à niveau. « Beaucoup de candidats sont en recherche passive, ils ont juste un problème de reconnaissance lié au salaire, par rapport au copain d'école qui, lui, a changé souvent d 'entreprise et a vu sa rémunération évoluer plus vite». La course aux salaires est un problème et provoque l'augmentation du turn-over.

Il n'existe malheureusement pas de chiffres de référence sur l'évolution des salaires en France dans le monde de la cybersécurité. On sait que, pour un profil pointu comme le big data, elle est de 4,5 à 4,7%, et pour l'IT en général, sur 2015, l'augmentation s'élevait à 7,7% sur l'année. On n'avait pas vu d'augmentation aussi importante depuis dix ans. Ajoutons que sur cette spécialité justement, on ne recrute pas que sur des critères techniques, mais des compétences plus larges, donnant des positions d'influenceur, de communiquant, avec un plus grand besoin d'autonomie, avec l'adhésion de la direction générale à la stratégie du RSSI et du DSI.
Des équipes visiblement délicates à gérer, compte tenu de l'évolution des postes et des besoins en sécurité. Chacun essaye de « piquer » les meilleurs profils. Mais ils ne sont pas simples à intégrer et faire évoluer. Leurs compétences fortes ne leur paraissent pas toujours reconnues par leur n+1. Ils souhaitent pourtant un management plus transparent. Il faut s'entretenir régulièrement avec lui, recommande Caroline Tampigny, vérifier s'il est heureux, comment il peut favoriser tout ce qui est lié à l'innovation et à la R&D dans l'équipe. C'est un rapport gagnant/gagnant, qui aboutira à un investissement plus fort du collaborateur.

En savoir plus

Retrouver les contenus associés à la Matinée Stratégique CIO du 16 février 2016 : *Cybersécurité : Les nouvelles menaces contre le système d'information*.

Didier Barathon
Rédacteur en chef de Réseaux & Télécoms

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