Julie Gommes → https://www.linkedin.com/in/juliegommes
Sécurité des systèmes informatiques chez DevoTeam

Voici la liste de questions que nous avions préparé avant l'entretien. Au cours de ce dernier, de nouvelles questions sont apparues, elles figurent toutes en gras dans la retranscription.

**Grille de questions**

- Quelle est votre définition de la cybersécurité ? / En quoi consiste la cybersécurité ?

- Dans quelle mesure la cybersécurité est-elle devenue incontournable aujourd'hui ?

- Comment peut-on qualifier l'année 2017 en ce qui concerne la cybersécurité ?

- Que pensez-vous de l'ampleur d'une cyberattaque sur le plan politique ?
- Les pirates informatiques d'aujourd'hui ont-ils les moyens techniques d'influencer le résultat d'une élection présidentielle ?
- Quelles sont les techniques de piratage les plus utilisées dans le monde aujourd'hui ? Comment s'y préparer ?

- Devons-nous faire plus de sensibilisation ?

- Quels sont les groupes de hackers russes connus ? pouvant avoir exécuté la cyberattaque contre les U.S ?

- Quel intérêt pour les Russes vis à vis de l'élection présidentielle américaine ?

- Dans certains cas de cyberattaques, le gouvernement peut décider de censurer des informations sensibles. Qu'en pensez-vous ?

- Comment peut-on vérifier l'exactitude des faits dévoilés par les pirates informatiques ? Que pensez-vous de la position de WikiLeaks dans cette affaire ?

- Quelles sont les failles du système informatique de vote aux U.S ?

- Quels cyber-risques doit-on craindre pour 2018 ?

**Retranscription Entretien avec Julie GOMMES le Samedi 20 Mai 2017**

Lors de l'introduction, elle nous donne les coordonnées d'un contact à l'IFRI (Institut Français des Relations Internationales) qui est spécialiste de politique russe.

**En guise d'introduction, pouvez-vous vous présenter et nous dire ce que vous faites au quotidien ?**

Bien sûr, alors je suis Julie GOMMES, je suis auditrice senior en sécurité. Alors un auditeur c'est quoi ? C'est quelqu'un qui est dans la peau d'un hacker, aussi bien au niveau technique qu'au niveau de la gouvernance de la sécurité ou de la sécurité physique. L'idée est de retourner l'entreprise dans tous les sens pour voir comment un attaquant pourrait s'y prendre et ainsi aider l'entreprise à corriger ses failles. Je fais également un peu de recherche. J'ai travaillé sur les outils de cryptographie utilisés par les djihadistes. Aujourd'hui je travaille plutôt sur les méthodologies de gestion justement de la gouvernance de la sécurité. Il y a constamment des standards qui sortent dans le secteur bancaire, dans les transports, dans l'énergie, etc. On s'aperçoit qu'on finit plutôt par cocher des cases en disant « c'est bon » que faire vraiment de la sécurité. Je suis en train de développer une nouvelle méthodologie de gestion et de présentation de la sécurité vis-à-vis de ces standards-là. Je travaille dans la sécurité depuis 5 ans maintenant. J'ai fait un passage par l'IFRI, institut qui traite de géopolitique donc j'ai aussi quelques notions de géopolitique en matière de sécurité de l'information.

**Quelle est votre définition de la cybersécurité ? / En quoi consiste la cybersécurité ?**

Je préfère employer le terme sécurité des systèmes d'information plutôt que cybersécurité. On a le mot « cyber » qui part dans tous les sens : les cyberguerres, les cyber-armées, etc. C'est devenu ce qu'on appelle un « buzzword », on devrait parler de sécurité des systèmes d'information. La sécurité de l'information aujourd'hui couvre un champ beaucoup plus large que seulement l'informatique, la technique. Cela passe par les métiers de l'entreprise, ça peut passer par l'intendance, ça peut passer par l'accueil. Aujourd'hui on peut porter atteinte à la sécurité du système d'information en exploitant une vulnérabilité qui n'est pas du tout informatique. Par exemple, en sécurité physique, on peut aller piquer des données dans un data center s'il n'y a pas un processus de gestion des accès. Par exemple, on y entre comme dans un moulin, en se faisant passer pour un livreur. C'est déjà arrivé sur des audits en sécurité physique. On se fait passer pour le livreur, on entre dans le data center et on peut voler des informations comme on veut en se

connectant à des serveurs. Donc cela arrive malheureusement encore aujourd'hui. Pour moi, la sécurité, c'est vraiment assez global, ce n'est pas seulement technique. Je préfère parler de sécurité de l'information en elle-même et du fait qu'elle reste confidentielle, qu'elle soit disponible à l'instant t quand on en a besoin et qu'elle soit intégrée, c'est-à-dire qu'on ne puisse pas la modifier ou y toucher.

**Selon vous, dans la société actuelle au XXIe siècle qui est numérique et de plus en plus digitalisée, dans quelle mesure la sécurité de l'information est-elle devenue incontournable et presque indispensable ?**

Ah ben bien sûr ! Aujourd'hui si on prend à la taille d'une ville toutes les installations techniques, les feux de signalisation, l'approvisionnement en électricité, en eau, etc. Tout cela passe par des systèmes d'information. Les usines de production, on l'a vu avec Renault la semaine dernière, ça passe par les systèmes d'information. Tout dépend de systèmes d'information aujourd'hui, y compris le fait qu'on téléphone. En fait, on passe par des smartphones qui sont des ordinateurs avec lesquels on téléphone. L'idée c'est aussi de protéger toutes ces installations dans les villes, pas seulement techniquement. Techniquement aujourd'hui on sait le faire, il y a des schémas d'architecture, il y a des « pen-tests » réguliers (tests de pénétration au sein d'un système d'information). Il y a de plus en plus de normes et de standards, même au niveau français avec l'ANSII par exemple, qui va obliger les entreprises à se conformer à certaines démarches de sécurité : en faisant des audits réguliers, en appliquant un certain nombre de mesures de sécurité, en faisant des analyses du risque, en les tenant à jour, etc. Un des enjeux majeurs aujourd'hui, c'est vraiment d'assurer la continuité d'activités à travers quelques grands principes qui vont plutôt être liés aux gouvernances et à la gestion de la sécurité. Vos feux tricolores, ils peuvent être hyper bien réglés au niveau des configurations, si le serveur est en open-bar sur internet, sans mot de passe, en anonyme, etc., alors n'importe qui pourra s'y connecter et jouer avec les feux de signalisation. Regardez ce qu'il s'était passé en Ukraine il y a quelques années, quand la Russie aurait attaqué, on n'est pas sûr que ce soit la Russie, tous les deux tricolores. Ils s'étaient attaqué aux deux de signalisation, à plusieurs ministères, en s'attaquant systématiquement à quelques systèmes d'information qui étaient bien ouverts.

**La sécurité de l'information est omniprésente et elle peut donc avoir une grande ampleur**

Ah oui ! Imaginez quand c'est de la signalisation des voies ferrées par exemple. Là il y a un gros problème. Si vous voulez il y a une époque où on se disait que la sécurité c'est avant tout technique, aujourd'hui la technique on maitrise, ce qu'il faut faire aujourd'hui c'est assurer une continuité d'activités

dans le temps. Ce n'est pas tout d'avoir le dernier Windows qui va bien avec tout un tas d'outils autour, si on n'applique pas les patchs, alors on est fichu. C'est tout bête mais cela passe par des processus de sécurité.

**Comment peut-on qualifier l'année 2017 en matière de sécurité de l'information ?**

C'est totalement fou, et ce n'est que le début ! L'année n'est pas finie. On en parle à chaque élection à juste titre et puis vous avez vu la publication des Shadow Brokers il y a quelques semaines. Ils ont sorti des outils utilisés par la NSA. On a récemment là dans la semaine WikiLeaks qui a sorti d'autres outils utilisés par la CIA, la NSA, etc. Tout cela est un début d'apocalypse pour nos entreprises parce que finalement, si on a eu WanaCry il y a quelques jours, c'est en fait à cause d'un outil qu'avait publié Shadow Brokers. Il a été modifié pour pouvoir exploiter la vulnérabilité. La modification consistait en une injection d'un crypto-locker. Ce qui est fou aujourd'hui c'est que ces publications d'outils ne font pas réagir les entreprises. Il faut savoir que dès que ces outils sont publiés, on a des attaquants, ça va du gamin de quinze ans aux Polonais ou au Roumain, qui récupèrent ces outils et qui s'en servent, on l'a vu avec WanaCry, pour mener des attaques. Ce qui est embêtant c'est qu'aujourd'hui les entreprises, dès la sortie de ces outils, ne se mettent pas en mode cellule de crise ou bien es ce qu'on est vulnérable à cet outil. Les entreprises attendent finalement, en se disant que ça ne sera peut-être pas exploité et on verra bien ce que ça va donner. Alors que ce sera forcément exploité donc je pense que 2017 est loin d'être terminée en termes de sécurité. On aura d'autres attaques.

**On réagit souvent trop tard**

On réagit après ! Il y a de plus en plus d'entreprises aujourd'hui qui ont une démarche en amont, mais maintenant on agit encore trop tard. J'étais à une conférence hier, on a un chercheur en sécurité qui nous a montré comment on peut attaquer un système en 12h et il a fallu à l'entreprise plus de 200 jours pour pouvoir s'apercevoir que quelqu'un s'était introduit dans le système. Déjà il faut être attaqué pour réagir et il faut aussi l'avoir vu et ça c'est encore un problème. On a encore beaucoup de problèmes dans la détection des incidents.

**Une précision concernant ce que vous avez dit, vous mentionnez « Shadow Broker », quel est ce groupe ?**

Oui alors en fait c'est un groupe de hackers/pirates, qui ont récupéré des outils utilisés la NSA. Alors je crois qu'ils ont attaqué une entreprise qui travaillait avec la NSA pour leur vendre les outils. C'est la NSA qui se serait fait hackée. C'est un groupe de hackers qui a publié pas mal d'outils utilisés par

la NSA pour mettre en place des programmes de surveillance, pour pirater des cibles bien déterminées.

**Pour rebondir sur ce que vous avez dit, vous parlez de hacker/pirate, est-ce qu'il y a une différence entre hacker et pirate ?**

Ah c'est un gros débat. En anglais, il n'y a pas de différence. Maintenant, en français il y a une différence de termes sur le fait que le pirate est celui qui va faire un acte malveillant. Le hacker c'est plutôt le petit malin, par exemple c'est celui qui va utiliser l'eau de la cafetière pour faire cuire ses saucisses. Le hacker est celui qui va détourner un objet de son usage. C'est très français comme distinction. D'un point de vue international on parle de hackers partout.

**Que pensez-vous de l'ampleur d'une attaque contre les systèmes d'information sur le plan politique**, **dans le cadre d'une élection présidentielle ?**

Alors pour perpétrer ces attaques, on va utiliser les systèmes d'information, encore une fois le terme « cybersécurité » me gêne. Alors il y a plusieurs choses. Déjà il faut bien qualifier le terme « attaque ». Une attaque c'est l'exploitation d'une vulnérabilité à des fins préjudiciables. C'est-à-dire je veux vous attaquer, je veux vous faire du mal, je vous attaque. Ce qui s'est passé avec WanaCry par exemple la semaine dernière, ce n'était pas ciblé, c'était dans le but de toucher très large. StuxNet, il y a plus de dix ans maintenant, c'était une attaque ciblée pour toucher le système nucléaire iranien. Le virus s'est propagé et s'est baladé partout jusqu'au jour où cela a fonctionné. Avec WanaCry c'était visiblement plus large. On voulait toucher de tous les côtés pour récolter des sous donc on n'était pas sur une attaque ciblée. Au niveau du plan politique, oui, oui c'est possible, il y a eu des précédents. En France, attention il y a eu beaucoup de bruit concernant la campagne de Macron avant le premier tour. C'est assez facile de se faire passer pour un russe sur internet. Pour tout vous dire, moi je m'étais amusée avec mon VPN à aller me balader sur le site de Macron avec une adresse IP russe juste pour faire du bruit, voilà c'était assez rigolo. Le problème aussi est que le site de Macron était vulnérable, il n'était pas mis à jour, il était facilement attaquable. Aujourd'hui cela peut être dévastateur, ça peut modifier les résultats. Quand on prend les machines à voter par exemple, c'est assez costaud aux Etats-Unis. Vous voyez ces machines à voter sont stockées dans des caves, des écoles, des musées, dans des salles, des mairies, etc., par spécialement surveillées, donc concernant ces machines, quasiment n'importe qui pourrait y avoir accès. Il est très facile de les modifier. Il est très facile de brancher une clé USB. Tout cela pourquoi ? Et

bien parce qu'il n'y a pas une réelle démarche de sécurité autour de ces machines à voter pour les protéger, pour faire des audits réguliers, pour les mettre à jour. Par ailleurs, le code à l'intérieur de ces machines, on ne sait pas ce qu'il fait car cela est une propriété des constructeurs. Si demain j'appuie sur Hillary Clinton et la machine me renvoie +1 pour Donald Trump, il y a aucun recours là-dessus, on ne peut pas faire de constatations habituelles même avec les outils adéquats. Il y a un gros problème à ce niveau-là avec les machines à voter. Le deuxième problème c'est au niveau des sites internet qui sont souvent mal mis à jour voire pas du tout. C'est très facile d'accéder à des bases de données, avoir des accès administrateur pour pouvoir faire via ces accès là des publications de tout et n'importe quoi sur le site. Cela va plutôt être un enjeu de communication. Cela peut remettre en cause toute une campagne, il y a un vrai risque, un vrai risque qui est multiforme.

**Justement, par rapport à cela, si j'ai bien compris, les pirates informatiques disposent des moyens techniques pour influencer l'issue du résultat d'une élection ?**

Alors cela pourrait ne pas être possible s'il y avait une réelle démarche de sécurité derrière : si ces machines étaient bien stockées, si on était sûr que n'importe qui n'y accède pas, que le code à l'intérieur de la machine fait bien son boulot, si on était sûr que les ports USB étaient bloqués, si on était sûr que ces machines n'étaient jamais connectées à internet. Pour faire une mise à jour il faut bien se connecter à un moment ou un autre. Encore une fois c'est une histoire de gouvernance de la sécurité. Comme elle est mal gérée aujourd'hui, il est possible que des attaquants aient les moyens de le faire. Alors ce serait très simple de mettre en place un système de stockage sécurisé sur ces machines-là, des audits réguliers une fois par an, des mises à jour régulières sous contrôle. Le problème est que ces machines ne sont pas auditables parce que le constructeur ne veut pas alors que finalement le réflexe à avoir serait de voir comment un attaquant pourrait exploiter les failles. Cela encore une fois n'est pas possible aujourd'hui.

**Quelles sont les techniques de piratage les plus utilisées ? Comment peut-on s'y préparer ?**

Alors cela va dépendre du public d'attaquants. Vous pouvez avoir des techniques assez différentes suivant leur niveau, j'ai envie de vous dire de l'attaque web ciblée, typiquement alors pirater les sites web de site pour aller récupérer des bases de données derrière et faire un phishing ou bien publier sur le site « je suis le meilleur » pour impressionner ses petits copains, ça c'est l'attaque classique du gamin. Après vous avez aussi des groupes de pirates organisés qui vont parfois embrigader ces gamins pour aller justement faire des effacements ou récupérer des données. Cela constitue un premier

niveau d'attaques informatiques. Si on veut rentrer un peu plus dans la technique, il y a tout ce qui relève de l'insertion, par exemple le KeyLogger. Alors un KeyLogger est-ce que vous savez ce que c'est ? [Nous hochons négativement la tête] C'est un outil qui va enregistrer ce que l'on tape sur le clavier d'un ordinateur. On peut l'attraper soit via une clé USB qu'on aurait branché stupidement sur sa machine soit en téléchargeant un logiciel contrefait par exemple. Cet enregistreur de frappe conserve tout ce que vous tapez. Tout est ensuite envoyé à l'attaquant. S'il récupère les informations d'un compte Yahoo d'il y a quinze ans ce n'est pas trop grave. Par contre quand il s'agit d'informations bancaires que vous tapez sur le clavier ou bien votre e-mail actuel et que vous vous connectez, là c'est plus intéressant car il y a beaucoup d'informations utiles pour le pirate. Il y a peut-être votre RIB que vous avez envoyez par mail à un copain pour le rembourser ou bien votre numéro de sécurité sociale. Si vous êtes américain, ce numéro est assez important. L'usurpation de droits est également beaucoup utilisée. Cela concerne toutes les attaques par « man in the middle ». Est-ce que vous voulez des éclairages là-dessus ? [Nous hochons positivement la tête] Imaginez une connexion du type StarBucks, MacDonald's, qui sont assez ouvertes, ou sur un réseau même chez vous lorsque vous êtes connectés en Wi-Fi, cet personne va se mettre entre votre machine et votre point d'accès internet. Il va récupérer le trafic, dans un sens et dans l'autre. Qu'est-ce qu'il va récupérer ? Et bien pour se connecter par exemple à certains sites qui sont peu protégés. Aujourd'hui la plupart des sites, que ce soit Facebook ou Google, c'est écrit en « https » donc le trafic va être crypté mais il y a encore des sites qui ne sont pas en « https » et ces attaquants vont pouvoir récupérer les informations que vous transmettez, par exemple votre identifiant et votre mot de passe, soit encore les cookies de session qui peuvent leur permettre aussi de se connecter sur différentes applications. Cela constitue un des gros points d'attaques, plutôt liées au fait qu'aujourd'hui il y a beaucoup de réseaux qui sont assez peu protégés. Cela permet certes d'avoir un côté pratique et confortable pour avoir de l'internet gratuit partout par exemple pour les Hotspots, sauf qu'en général les données ne sont pas bien sécurisées. La technique du phishing, qui a été utilisée pour les attaques contre Hillary Clinton, reste encore beaucoup utilisée. Il existe des techniques de phishing en deux temps. Vous avez de la récupération de données personnelles puis l'attaquant va se servir de son mail professionnel pour envoyer des mails de phishing à l'intérieur de l'entreprise. Je ne sais pas si vous connaissez le concept de RedTeam. Il s'agit d'un nouveau type d'audit qui est pas mal car au lieu de simuler un seul attaquant, il y a toute une équipe multi-tâches. Il va y en avoir un qui craque le Wi-Fi de la boite, vous en avez un autre qui récupère les badges d'accès,

vous en avez un autre qui est connecté aux systèmes d'information et qui va monter les privilèges du badge pour pouvoir permettre d'accéder aux bureaux de la direction. Cela va ensuite vous permettre de récupérer des documents, informations et de passer des coups de fil pour faire du social-phishing. L'idée est vraiment de se monter une équipe d'attaquant avec cinq ou six personnes et voir quelle est la vulnérabilité. Ce type d'audit est de plus en plus répandu et demandé par les entreprises parce qu'il y a toujours ce qu'on appelle des « fraudes au président », c'est-à-dire des gens qui vont vous faire transférer des milliers d'euros sur un compte pour le fermer quelques jours après, tout cela en faisant croire que c'est le comptable qui appelle depuis la salle de réunion. Il y a toujours ce type d'attaques aujourd'hui. Le phishing est un moyen pour collecter les informations dans ce genre d'attaque.

**Est-ce que cela signifie qu'on doit faire plus de sensibilisation sur le plan humain ?**

Alors cela se fait déjà mais c'est clair qu'il faut continuer, continuer, continuer. Il y a de plus en plus de gens qui adoptent la bonne démarche. Il y a une meilleure formation de certains pôles au sein de l'entreprise, notamment le service communication qui peut se faire toucher par Facebook ou Tweeter. Mais tout cela ne suffit pas. C'est bien, il faut faire de la sensibilisation mais surtout ce qu'il faut faire c'est une vraie démarche de sécurité. Si on dit aux gens de ne pas télécharger tout et n'importe quoi mais qu'en parallèle les ports USB de leurs machines sont ouverts et que par la suite ils installent des logiciels contrefaits sur leurs ordinateurs de bureau, c'est qu'il y a un problème. Là il y a un problème, un trou dans la raquette parce que le virus on ne l'attrape pas de nulle part, on l'apporte sur sa clé USB. L'idée c'est de passer plus de temps sur l'analyse des risques sur le plan technique. Comme on le disait tout à l'heure, il y a beaucoup de choses qui sont réalisées après une attaque et finalement la prise en compte en amont pourrait vraiment réduire la surface d'attaque. Cela peut se faire en passant par des choses très très simples et faciles à mettre en place.

**Concernant les grands pirates informatiques, quelles sont leurs techniques ? Utilisent-ils les techniques que vous venez de citer ?**

Ah ben bien sûr ! Il y a une variante du phishing qui s'appelle le water-holing. C'est l'image du point d'eau dans la savane. Tous les animaux vont boire à ce point d'eau. Il y a des techniques assez répandues : on crée un nouveau dossier partagé que les gens de l'entreprise vont recevoir sur leurs adresses mail. Ils se disent que tout va bien, ils cliquent sur le dossier et en fait cela donne des droits d'accès à l'attaquant. C'est toujours comme ça que les attaquants vont jouer, parce que c'est facile et que ça marche encore. De plus, ce n'est pas très compliqué à mettre en place.

**A présent, revenons un peu sur la Russie et les Etats-Unis. Quels sont les grands groupes de hackers russes ? Quels sont ceux soupçonnés d'avoir pirater l'élection américaine ?**

Alors vous devriez allez voir Bogachev, celui-là a sa tête mise à prix par le FBI. C'est assez rigolo, il a l'air bien costaud. Je ne sais pas si vous avez suivi mais c'est vrai que concernant les hackers russes il y a toujours eu une ambigüité avec McAfee. Vous connaissez McAfee, l'antivirus ? Le leader est John McAfee qui a donné son nom au produit. Le bonhomme en lui-même est déjà très louche, il y a plusieurs articles sur lui, ce serait un agent secret des renseignements et on le soupçonne même d'avoir une armée de hackers russes qui créent des virus et des malwares pour faire vendre son anti-virus. Il a un discours très étrange disant qu'au final il ne faut pas faire de sécurité, pas de besoin de former les gens. Il y a aussi le revers de la médaille qui est que si on ne fait pas de pédagogie alors les gens vont se faire infecter. Parce que pour que l'anti-virus détecte une attaque, il faut que l'attaque soit connue. C'est ce qu'il s'est passé avec WanaCry. Au début les anti-virus de ne le reconnaissaient pas car il n'était pas dans leurs bases virales. Une fois que le virus est sorti, ils ont pu l'ajouter à la base virale et ensuite prendre des mesures pour le bloquer. Mais il y a eu tout un temps où ces virus-là étaient en place et sont passés à travers les mailles du filet. Il faut savoir que les russes sont spécialistes dans le vol et la revente d'à peu près tout et n'importe quoi sur le black market. En fait, si vous allez chercher dans les services cachés de TOR, vous avez de la carte bleue, vous avez des plaques d'immatriculation, des armes. Ce qu'il passe là-bas c'est que vous avez des gens qui sont ingénieurs de très haut niveau mais avec des niveaux de salaires assez ridicules. Et ces gens-là, par rapport à l'Europe, par rapport aux Etats-Unis, précisent que faire ces activités criminelles va leur rapporter beaucoup plus au final qu'un boulot d'ingénieur dans leur pays. C'est un peu l'attrait de l'argent facile. Dans un contexte politique en lui-même, vous verrez que McAfee est suspecté d'avoir une implication dans ce milieu-là, enfin c'est ce qui se dit de toute façon. Il a une grosse implication dans tout le Dark Web. Après il faut faire attention à une chose, c'est qu'avec un proxy ou même en utilisant un VPN, moi demain je suis russe. Il n'y a rien de plus facile que de se faire passer pour un russe sur internet et il devient impossible de vous tracer. Dès lors que vous effectuez plusieurs sauts, entre différents serveurs de plusieurs pays, on ne peut pas remonter jusqu'à vous. Pour retracer une adresse IP cela prendrait des mois pour retrouver l'attaquant qui est derrière. Dans cette affaire on soupçonne les russes mais encore une fois il y a un gros point d'interrogation là-dessus. C'est pour l'instant impossible à prouver.

**Donc lorsque la CIA et le FBI ont publié des rapports en affirmant que les attaques venaient de la Russie, peut-on leur faire confiance ?**

Peut-être qu'ils disposent d'informations que nous n'avons pas. Après il y a aussi les informations qu'ont les services de renseignement : les gens qui sont sur le terrain en Russie, les gens qui sont sur le terrain aux Etats-Unis, les gens qui ont infiltré des groupes de hackers, etc. Techniquement, ça reste hyper difficile de savoir qui est à l'origine de l'attaque. En général ce qu'il faut faire après une attaque c'est ne rien toucher. Ne rien toucher pour ne pas effacer les traces de l'attaquant, ou rajouter du bruit par-dessus. L'idée c'est de faire appel à des spécialistes de sécurité et des experts. Ils vont essayer de tracer l'attaquant, de détecter des pièges encore actifs laissés par l'attaquant pour revenir plus tard attaquer le système d'information. Ils vont également essayer de corriger les vulnérabilités du système que l'attaquant a exploitées. Il se peut que dans cette analyse post-incident, on s'aperçoive que les adresses sont effectivement localisées dans tel ou tel pays, pareil pour les serveurs. Mais encore une fois, avec de l'analyse technique pure, ce n'est pas possible de dire que c'est tel ou tel groupe si l'attaque n'est pas signée.

**Aujourd'hui cela signifie qu'il s'agit uniquement de soupçons concernant les groupes FonzyBear et CozyBear ?**

Au niveau technique, on ne peut avoir que des soupçons. Mais peut-être que les renseignements disposent d'autres informations. Il y a quand même Bogachev qui semble impliqué, le grand ami du FBI. La personne avec qui je vais vous mettre en relation pourra vous en dire plus quant aux groupes de hackers soupçonnés d'avoir exécuté l'attaque.

**D'un point de vue politique, quel est l'intérêt pour la Russie d'avoir, ou pas, effectué ces attaques ?**

Alors ça c'est de la géopolitique. Pour moi, c'est dur de vous dire. Mais je pense qu'il y a une certaine idée de softpower, une volonté d'assoir sa puissance. Le fait même de dire qu'ils l'ont peut-être fait, même si ce n'est pas avéré, ça leur prête un pouvoir, une assise au niveau international. Aujourd'hui, tous les états vont avoir peur de ces attaquants russes. Ils communiquent bien là-dessus et ça leur donne une nouvelle position sur l'échiquier international.

**Concernant la censure des attaques à présent. On voit parfois que le gouvernement intervient pour censurer le fait que des attaques aient eu lieu. Cela est ensuite dévoilé par WikiLeaks ou bien sur internet. Que pensez-vous du rôle de l'état à ce niveau ?**

En Europe la réglementation est en train de changer. Si vous regardez aux Etats-Unis, les grandes entreprises qui se font voler par exemple les données de cartes bancaires, les données de sécurité sociale, ces données

sont automatiquement publiées parce qu'on va avoir l'obligation de dire à l'état qu'on a subi une attaque. Ensuite on va avoir l'obligation de se mettre à jour, de faire une réponse sur incident, de corriger les failles. En Europe aujourd'hui, ce n'est pas encore le cas, mais la réglementation européenne va de plus en plus de ce sens et les entreprises pourraient être amenées, d'ici cinq ans, à avoir le même système en déclarant qu'elles ont été attaquées. Cela se fera soit en le déclarant à un institut comme l'ANSII soit au niveau européen, je ne sais pas exactement, mais on s'oriente vers cela et c'est bien. C'est bien de communiquer là-dessus. On ne peut pas communiquer sur le détail de l'attaque car il y a une vulnérabilité tant que le problème n'est pas résolu. Si on sort l'information immédiatement sur comment l'attaque a été faite alors l'entreprise pourrait être réattaquée tout de suite.

**Globalement, vous pensez que c'est une bonne chose ?**

Moi je pense que c'est une très bonne chose de communiquer sur les attaques, de dire que telle ou telle entreprise a été victime d'une attaque. Pour les entreprises cela leur permet aussi d'avoir peur de ces publications donc elles vont augmenter leur niveau de sécurité, elles vont améliorer leurs démarches et leurs processus donc c'est une très bonne chose. Maintenant, je suis contre le fait de publier les détails techniques d'une attaque immédiatement après son apparition.

**Quels sont les moyens aujourd'hui pour attester l'exactitude des faits révélés sur internet par des attaques informatiques ?**

Ah ça c'est dur, c'est dur comme question. Non aujourd'hui il n'y a pas de moyens de vérifier la véracité des informations et documents mis en ligne si ce n'est par le sérieux du travail effectué. Quand les premières informations ont été dévoilées par WikiLeaks et que plusieurs médias dans le monde y jettent un œil pour vérifier les informations, là on peut y croire. Mais si c'est quelque chose qui sort comme ça de nulle part sans réelle source alors c'est plus difficile de faire confiance. Je ne dis pas que ces informations seront nécessairement fausses mais ce sera plus difficile d'y croire. Il faut toujours se méfier.

**Oui parce qu'il y a même souvent des théories du complot car concernant les rapports publiés par le FBI et la CIA, beaucoup de passages sont surlignés en noir donc certaines personnes vont jusqu'à dire que tout cela a été orchestré par les Etats-Unis eux-mêmes.**

Oui voilà, il faut que chacun se fasse sa propre opinion et puis aussi prendre un peu plus le temps. Aujourd'hui on est dans une société de l'information où il faut que ça aille vite, on veut être les premiers à sortir tel ou tel scoop et on ne prend plus le temps de vérifier. Aussi parce que le spectateur, le lecteur, le consommateur de l'information veut tout savoir tout de suite. Sauf que si on veut que MediaPart vérifie les données alors ça prend

du temps. Et ce temps-là, le consommateur actuel de l'information ne veut pas le donner. On est dans un vrai problème où on se plaint parfois d'avoir des fake news et des informations non vérifiées mais on veut être les premiers à être informés de tout et n'importe quoi donc c'est assez contradictoire.

**Concernant WikiLeaks, qui a la réputation de tout dévoiler le plus rapidement possible, ne pensez-vous pas que parfois un recoupement des différentes sources serait plus approprié ?**

Sur la question des informations qui avaient été relayées par Bradley Manning, cela a fait bouger des choses au niveau politique, on a vu qu'il y avait une utilité. Je pense que WikiLeaks a une vraie responsabilité géopolitique qui est de vérifier ce qui est publié. Est-ce qu'ils le font ? Je ne sais pas, je ne suis pas dans leur cuisine interne.

**Quelles sont les failles des systèmes d'information aux Etats-Unis concernant l'affaire de l'élection présidentielle américaine ?**

La faille principale que je vois concerne les machines de vote. Je n'en vois pas d'autres.

**Est-ce que l'affaire des mails d'Hillary Clinton est également une autre faille ?**

Ah ben cela a de l'influence c'est clair ! Il y a une redistribution des cartes qui peut se faire. C'est un peu l'idée du softpower que j'évoquais tout à l'heure. Avoir accès à ces mails et les publier, c'est avoir un certain pouvoir sur la diffusion de ces informations. Effectivement, c'est vrai que je n'avais pas pensé à cela, la publication de tous ces courriers a beaucoup joué dans l'élection présidentielle américaine.

**N'y a-t-il pas un problème au niveau du gouvernement sachant que les personnes visées sont hautement placées et il apparaît surprenant qu'elles se soient faites avoir aussi facilement ?**

Ah ben vous savez je vais vous en raconter une belle sur l'Elysée et un ministère il y a quelques années. Ils étaient une équipe de trois ou quatre gars qui travaillaient dans un cabinet, trois d'entre eux avec un compte Facebook et le dernier n'en avait pas. Qu'a fait l'attaquant ? Il a créé un faux compte Facebook à l'image du quatrième gars, il a ajouté plusieurs amis et puis il a ajouté les fameux gars avec le collègue travaillait. Il a discuté avec eux, bon, et puis un jour il leur envoie un lien avec écrit « T'as vu la nouvelle messagerie web qui nous ont mis, elle est bizarre tu trouves pas ? », et sauf que c'était pas du tout la nouvelle messagerie de l'entreprise mais bien un lien de phishing tout bête dans lequel un de ses collègue a rentré son login et son mot de passe. Cela a permis ensuite à l'attaquant d'avoir un accès total aux mails de ce gars-là qui travaillait dans un cabinet du ministère. Si vous regardez il y a quelques années quand il y avait eu le G8, enfin le G7 ou G8 en France là, c'était à l'époque sous Sarkozy, il avait invité

Mark Zuckerberg d'ailleurs à venir , c'était en Normandie, on a une partie non négligeable des chefs d'Etat et dirigeants qui était présent et ces derniers ont cliqué sur le lien vers un mail dont l'objet était « Carla Bruni nue » [rires], et ce truc là leur a filé des malwares, en sachant que ce sont des gens qui ont des documents ultra stratégiques sur ordinateur. C'est encore difficile aujourd'hui et c'est encore une question de gouvernance. C'est vraiment une question de gouvernance d'apprendre les bonnes pratiques à ces gens-là, de ne pas cliquer n'importe où, de ne pas télécharger n'importe quoi, c'est vraiment la base de la base. En fait aujourd'hui, les employés, les secrétaires, tous les gens qui sont au plus bas de l'organigramme de l'entreprise savent très bien tout ça. Par contre quand on est tout en haut chez les VIP, on a encore certains problèmes pour faire passer des messages en termes de sécurité alors que ce sont eux qui possèdent les informations les plus stratégiques. Concernant l'affaire d'Hillary Clinton, il y a une histoire selon laquelle elle a utilisé un serveur mail qui n'était pas contrôlé par l'Etat. Alors ce n'était pas Yahoo, ce n'était pas Google, je ne connais pas le nom de l'hébergeur chez qui elle était, mais ce qui est sûr c'est qu'elle a utilisé un mail perso pour faire circuler des infos d'Etat. C'est encore un problème de gouvernance car ces informations là où elles parlent de données stratégiques pour l'Etat, tout cela était stocké dans un serveur potentiellement accessible par des boites privées. Je ne sais pas si vous êtes au courant mais quand vous envoyez un mail, il y a en réalité quatre copies du mail. Vous avez-vous le mail dans votre boîte de messages envoyés, vous avez le destinataire qui a le mail dans sa boîte de réception, mais vous avez aussi une copie, par exemple chez Google si vous êtes chez Gmail et une copie si vous êtes chez Yahoo enfin si l'autre est hébergé chez Yahoo. Donc même si vous supprimez le mail de votre boîte de réception ou de votre boîte d'envoi, il est toujours stocké chez votre hébergeur. Le problème il est là. Quand Hillary Clinton utilise une boîte mail privée pour parler de questions d'Etat, ce sont des informations qui forcément fuitent.

**Vous n'êtes pas obligée de répondre, mais quel est votre avis sur la controverse de l'élection présidentielle américaine ?**

Je vais vous dire, en tant qu'auditeur j'en sais rien moi. Je me fonde vraiment sur des faits, sur des preuves que je vais trouver. J'ai aucun avis sur la question.

**Quels sont les risques à craindre pour l'année à venir en termes de sécurité des systèmes d'informations et d'attaques ?**

Alors c'est peut-être un peu tôt pour parler de 2018 mais déjà pour 2017, fin 2017 on risque d'avoir une belle apocalypse et on va bien s'amuser. Il est sûr qu'on va avoir d'autres problèmes. Comme je vous le disais, cela se fera par les outils qui sont révélés au grand public. On a eu le cas WanaCry,

je pense qu'on va avoir l'équivalent avec d'autres outils que la NSA a utilisé et qui ont dévoilés aujourd'hui. Et cela parce que les entreprises n'ont toujours pas jugé bon de mettre en place des mises à jour de sécurité. On a récemment eu une attaque sur des millions d'objets connectés dont les mots de passe par défaut n'avaient pas été changé, parce que typiquement la petite caméra qu'on place chez soi ou bien le téléphone pour bébé, on ne change pas le mot de passe par défaut. Cela est possible par d'autres outils. Ah tiens d'ailleurs, cette semaine WikiLeaks a révélé d'autres outils pour mener des attaques contre les systèmes d'information, vous pourrez regarder l'article sur VAULT7. Il faut bien prendre conscience que dès qu'une vulnérabilité est publiée, il y a automatiquement des gens qui vont s'en servir à des fins malveillantes. Cela s'annonce plutôt chaud pour la fin de l'année. J'espère qu'il va y avoir une prise de conscience. Même au niveau mondial, on risque de voir de nouvelles attaques contre les systèmes d'information.