

**Entretien avec Nicolas ARPAGIAN: LES ENTREPRISES FACE À LA "CYBERINSÉCURITÉ"**

*Julien MARCEL : Lorsque l'on parle de cyberguerre ou de cybersécurité de quoi parle-t-on ? Derrière ces termes quels sont les enjeux ?*

Nicolas ARPAGIAN : Le choix du terme *cyberguerre* est intéressant. C'est un mot médiatiquement efficace. Car lorsqu'il est employé il évoque chez votre interlocuteur tout un imaginaire. Cependant, son emploi peut être problématique, car il peut inciter nombre de particuliers ou d'entreprise à croire que les attaques cybernétiques ne concernent que les seuls militaires et autres membres des services de renseignement. C'est à dire les professionnels de la guerre conventionnelle. Aussi, pour que les citoyens et les acteurs économiques prennent pleinement la mesure de ce qui se joue lorsqu'ils se connectent à Internet, il nous faut préférer le terme de *cybersécurité*.

Qu'il s'agisse d'établir et de protéger votre identité numérique, et de connaître les menaces techniques qui existent sur la Toile. Chaque utilisateur du Net, dans sa vie personnelle ou professionnelle est un maillon de la *cybersécurité* ou de la *cyberinsécurité*. En divulguant nombre d'informations personnelles sur le Net, on favorise les opérations d'usurpation d'identité. En multipliant les téléchargements à partir de sites à la fiabilité incertaine ou par le biais de clés USB qui passent d'ordinateurs en ordinateurs on peut participer à la circulation de logiciels malicieux. Enfin, il faut être conscient que l'informatique d'une entreprise ou d'un individu peut être victime d'une attaque ciblée, mais, comme sur un champ de bataille, on peut également être la victime collatérale d'une attaque massive\*. Par exemple lorsque vos données présentes chez un tiers sont piratées ou lorsqu'un ver informatique, par exemple *Conficker* en 2009, a atteint des dizaines de milliers d'ordinateurs parmi lesquels ceux du ministère français de la Défense. Ce dernier n'était pas la cible visée spécialement mais il a fait partie des victimes.

*JM : Quelles sont les attaques dont peuvent être victimes les entreprises ? Vous distinguez notamment dans vos ouvrages les attaques sur le réseau informatique et les attaques informationnelles.*

NA : Il y a en effet deux grands piliers en termes d'attaques. Il y a d'abord les attaques visant le réseau informatique, avec différentes options possibles. La première est l'espionnage. Celle-ci consiste à pénétrer dans votre réseau le plus discrètement possible pour en sortir des informations que l'attaquant considère comme essentielles. L'idée étant que l'outil utilisé soit le plus indolore possible du point de vue informatique afin que la cible ne change rien à ses habitudes et continue à exploiter ses systèmes sans se méfier. Dans le champ de ces attaques, on peut également citer l'interception de données, ou encore l'attaque qui consiste à pénétrer dans votre réseau informatique pour l'altérer et créer ainsi des dysfonctionnements ponctuels. On peut imaginer ainsi que des données soient modifiées ou que l'outil de production d'une entreprise puisse être stoppé au moment opportun.

Le second pilier est composé des attaques informationnelles. On y retrouve l'usurpation d'identité, mais également le *cybersquatting*. Sans oublier les attaques qui consistent à propager sur le Net des rumeurs ou des informations que vous souhaitiez occulter. On utilise, en l'espèce, l'information comme une arme. Ces attaques coûtent très peu cher, ne nécessitent pas un savoir informatique important et peuvent être mises en place avec peu de moyens techniques. À cela s'ajoute une relative impunité judiciaire de l'attaquant. En un simple clic, les données circulent d'un pays à un autre. Le magistrat, qui lui est soumis à un respect scrupuleux des règles de procédure fruit des accords internationaux et de la diplomatie judiciaire, aura grand peine à instruire ce type d'affaire dans des délais courts. Tandis que le déplacement des données illicites d'un pays à l'autre pour se jouer des réglementations s'effectue en quelques minutes.

*JM : Comment les entreprises peuvent-elles aujourd'hui se protéger ?*

NA : La sécurité informatique coûte certes de l'argent dans sa mise en place, avec des logiciels adaptés et des processus ad hoc. Mais tout cela restera vain si le comportement des usagers (salariés ou particuliers) ne suit pas des règles essentielles de sécurité. Ce qui exige une collaboration étroite entre la Direction sûreté, celles des ressources humaines et les équipes chargées de la sécurité informatique. Il faut par exemple rappeler aux personnes qui composent les entreprises qu'il faut changer régulièrement de code d'accès, qu'il ne faut pas utiliser sa messagerie personnelle depuis son lieu de travail, qu'il faut éviter de connecter son ordinateur à des outils de stockage externe comme une clef USB, ou qu'il ne faut pas télécharger des documents sur internet qui n'ont pas été vérifiés... Ce sont de simples mesures d'hygiène numérique qui sont, en effet, contraignantes, chronophages et ingrates, mais qui sont indispensables. Encore plus que dans la sûreté physique, une porte laissée entrouverte dans le cyberspace à des conséquences désastreuses, puisque cette ouverture est permanente et celui qui l'a laissée ouverte n'en a probablement pas conscience. Rappelons qu'une *cyberattaque* réussie est bien souvent un piratage dont la victime ne sera jamais informée.

L'objectif n'est pas de transformer l'ensemble des salariés en techniciens, mais de mettre en place des procédures, des bonnes pratiques, qui vont parfois ralentir les processus, mais qui éviteront à l'entreprise bien des déconvenues. Par exemple, il me semble plutôt aisé et peu onéreux de déconseiller aux salariés en déplacement de se connecter à un ordinateur accessible à tous... Le risque, en la matière, c'est bien souvent la facilité. Or, il suffit de voir que des petits équipements, baptisés *Key Loggers* et qui coûtent quelques dizaines d'euros permettent en toute simplicité de récupérer en temps réel les données frappées avec le clavier d'un ordinateur de bureau collectif. Comme ceux mis obligamment à la disposition des clients dans les halls des grands hôtels...

*JM : Aujourd'hui, régulièrement, les attaques informatiques que subissent les entreprises font les titres des journaux... Doit-on en déduire que les entreprises sont de plus en plus menacées sur le cyberspace ?*

C'est une illustration du phénomène. Mais je le rappelle il ne faut pas négliger les attaques se déroulant à l'insu de leurs cibles. Le problème c'est qu'aujourd'hui il est bien difficile de dresser un diagnostic en matière de *cyberattaque* contre les entreprises, car nous n'avons pas de chiffres clairs. Il faut absolument que l'État se dote d'un organe capable de chiffrer ces actes de malveillances. Aujourd'hui, les principales statistiques disponibles émanent des vendeurs de solutions de sécurité ou d'assureurs... C'est un peu comme si les vendeurs de portes blindées étaient les seuls à nous fournir des statistiques sur les cambriolages ! Cela n'est pas sérieux. Dans le rapport 2011 de l'Observatoire Nationale de la Délinquance et des Réponses Pénales (ONDRP), j'ai donc appelé à la création d'un dispositif public de collecte des données en la matière. Nous ne pourrions envisager un arsenal de lutte contre ces *cyberattaques* acceptable aux yeux de l'opinion que si nous arrivons à en avoir une photo instantanée qui soit la plus réaliste et neutre possible. Il sera également bien difficile de faire accepter aux citoyens des règles parfois très restrictives sur le plan des libertés individuelles, si nous ne les argumentons pas avec des chiffres vérifiés et vérifiables. Il faut que les dispositifs de sécurité soient justement adaptés à la réalité de la menace.

Dans le cas où un observatoire de ses attaques était mis en place, il faut bien garder à l'esprit que les chiffres qu'il produirait seraient nécessairement imparfaits, puisqu'il ne pourrait pas prendre en compte les attaques qui ont atteint leurs objectifs et qui n'ont pu être détectées.

Cependant, aujourd'hui, la tendance en termes d'attaque ne peut être qu'à la hausse. À ce jour, nous sommes à environ 40 millions de Français connectés à l'internet haut débit, toutes les entreprises sont connectées sur le Net, les documents administratifs se remplissent dorénavant sur le web et les relevés bancaires sont de plus en plus envoyés par *email* ... Il y a de plus en plus d'informations ou de données qui ont de la valeur qui sont en circulation sur la toile, cela crée des convoitises.

*JM : Pensez-vous que les entreprises sont désormais bien préparées contre ces attaques ?*

NA : Ce qui est sûr, c'est que les entreprises les mieux préparées et les mieux protégées sont celles qui ont subi des attaques. Comme dans beaucoup d'autres domaines relatifs à la sécurité, se protéger contre les attaques informatiques peut coûter cher et peut encore une fois paraître contraignant... C'est encore hélas lorsque l'on a été confronté à une attaque informatique que l'on comprend l'intérêt de se protéger. A l'instar de *Sony*, qui a recruté un responsable de la sécurité des systèmes d'informations APRÈS avoir été piraté à très grande échelle.

Par contre, il n'y a pas de protection de l'information s'il n'y a pas une prise de conscience de la direction générale. Il est impensable de demander à des salariés d'appliquer des procédures si les personnes les plus importantes dans la hiérarchie de l'entreprise ne les appliquent pas. D'autant plus que cette population peut constituer la cible privilégiée des attaquants du fait de leur vulnérabilité : ils sont souvent extrêmement mobiles et sont d'importants consommateurs de produits high-tech.

*JM : Comment l'État peut-il améliorer l'aide qu'il fournit aux entreprises ?*

NA : Dans chaque entreprise, il est important d'identifier en amont les procédures à suivre place en cas d'attaque informatique constatée. Il faut par exemple mettre en place des procédures d'investigation légale et identifier les organismes de l'État qui peuvent soutenir l'entreprise. Le rôle de l'État c'est de rendre clairs ces modes opératoires. Pour ce faire il doit continuer à sensibiliser les entreprises et les informer. C'est dans cet esprit que j'ai conçu le cycle annuel dédié à la Sécurité Numérique à l'Institut National des Hautes Etudes de la Sécurité et de la Justice (INHESJ). Où des responsable de la sécurité informatique d'entreprises rencontrent les différents services de l'Etat : police judiciaire, Gendarmerie, DCRI, Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI), DPSD... pour échanger et par la suite travailler plus efficacement ensemble. Comme en épidémiologie, plus nous amasserons de connaissance contre ces attaques, mieux nous préparerons nos défenses et mieux nous saurons à quel moment il convient de contre-attaquer.

*JM : Ces dernières semaines, c'est le groupe Anonymous qui fait la une des journaux. L'OTAN, Sony ou encore EDF ont été victimes de ce réseau. Qu'est-ce que le groupe « Anonymous » ? Faut-il en avoir peur ?*

Les *Anonymous* sont un collectif informel. *Anonymous* est une marque ombrelle, qui à mon sens peut risquer de s'esouffler si elle continue à être utilisée à tort et à travers. En effet, il est très difficile d'exister sur la durée d'un point de vue marketing lorsque l'on n'est pas incarné par un leader ou une figure. On peut déjà observer une certaine cacophonie : actions de piratage revendiquées par les uns, dénoncées par les autres. Tandis que certaines sont annoncées sans qu'elles n'aient jamais lieu. En outre, certaines attaques sont associées un peu rapidement aux *Anonymous* sans que l'on ait vraiment vérifié la source des revendications. Ce qui évidemment difficile dès lors qu'il n'y a pas de siège social auprès desquels les autorités et les médias peuvent obtenir confirmation. Faut-il avoir peur d'*Anonymous* en tant que structure ? Je ne pense pas. Il faut plutôt y voir une nouvelle forme de contestation. Ce qui est déstabilisant pour le moment c'est que la cause et cette manière de protester ne sont apparues que très récemment sur les écrans radars des entreprises et des organes étatiques qui ont mis du temps à les prendre au sérieux. Or, elle peut surgir à tout moment à l'encontre d'une institution et repartir aussi vite qu'elle est venue. Contrairement aux militants comme par exemple *GreenPeace* qui s'oppose sur la durée, frontalement et à visage découvert aux acteurs de la filière nucléaire. Il est certain que cette forme d'action offensive n'ira qu'en se développant, associant ponctuellement des individus qui ne se connaissent pas forcément dans la vie réelle. Mais que la réussite d'une cause suffit à coaliser le temps d'une action commando. Cela complique d'autant la tâche des professionnels de la sécurité puisque la mission de veille et d'anticipation porte sur des champs extrêmement vastes. Faute de pouvoir l'empêcher, il faut s'y préparer.