La menace cyber-terroriste n’a jamais été aussi vaste

La menace cyber-terroriste n’a jamais été aussi vaste

Général d'Armée, Marc Watin-Augouard a cofondé en 2007 le Forum international de la cyber-sécurité. À l'heure des attentats, il revient sur les menaces de cyber-terrorisme qui pèsent sur les entreprises.

Le cyber-terrorisme est-il une réalité aujourd'hui ?

On le voit apparaître aujourd'hui autour de quatre phénomènes. Le premier, c'est l'atteinte aux contenus, comme l'effacement de sites. Suite aux attentats de janvier, 19.000 sites ont été effacés en France suite à des intrusions sur les serveurs, avec parfois la modification de données pour diffuser de la propagande ou de l'incitation au terrorisme. Le second phénomène, c'est l'utilisation du web par les terroristes à des fins d'organisation. Daesh n'aurait pas son visage actuel s'il n'existait pas un réseau mondial lui permettant de diffuser de l'information et des ordres. Le troisième aspect, c'est le recours des terroristes à la criminalité du cyber-espace pour se financer : vols de données bancaires, escroquerie, etc. Enfin, même si c'est une menace encore rare, il existe un danger d'attaque visant à bloquer ou saboter du matériel : en 2012, 30.000 ordinateurs de l'entreprise saoudienne Saudi Aramco ont été détruits à distance par des activistes. La menace cyber-terroriste n'a donc jamais été aussi vaste.

Toutes les entreprises peuvent-elles être concernées par ces menaces ?

Il ne faut jamais oublier que si une entreprise peut être une cible potentielle, elle peut être aussi un vecteur qu'on utilise pour mener une attaque en rebond. Regardez la chaîne américaine de magasins Target, qui a été victime en 2014 d'une cyber-attaque massive : elle a été touchée parce qu'on s'est d'abord infiltré chez un prestataire qui s'occupait de la climatisation des points de vente. Une entreprise peut donc être visée simplement parce qu'elle est sous-traitante de la « vraie » cible.

Quel est aujourd'hui le niveau de préparation des entreprises françaises face à ces cyber-menaces ?

Il y a une prise de conscience : nos entreprises sont en train de prendre très au sérieux ces dangers. C'est le cas tout d'abord des opérateurs d'importance vitale, qui travaillent dans les secteurs critiques, et qui doivent mettre en place des règles dans le cas de la loi de programmation militaire. Ces règles doivent d'ailleurs être aussi respectées par leurs sous-traitants, ce qui créé un effet de diffusion de l'hygiène informatique. Les entreprises ont également en face d'elles des assureurs qui s'intéressent de plus en plus à ces risques. Aujourd'hui, beaucoup d'entreprises s'organisent donc en commençant à faire remonter à l'échelon stratégique ce qui était considéré parfois comme un simple rouage technique. C'est positif.

Le problème, c'est que la cyber-sécurité coûte cher…

Oui, elle a un prix, mais les résultats d'une cyber-attaque aussi. Il y a des arbitrages à opérer. Mais si l'on se plonge dans le guide de l'hygiène informatique publié par l'Agence nationale de la sécurité des systèmes informatiques, on voit que nombre de ces prescriptions ne coûtent rien. Et qu'elles permettent d'annihiler 85 % des risques. Cela débute souvent avec la sensibilisation des personnels : une grande partie des cyberattaques est le fait de collaborateurs malveillants ou d'erreurs humaines dont les personnels sont les porteurs. L'arnaque de l'escroquerie au président commence par exemple par une interaction humaine. Le bon sens, l'organisation, la réflexion, cela n'a pas de coût.

Née dans la foulée des attentats de janvier, la loi sur le renseignement a brusqué les entreprises du numérique, notamment avec ces « mouchards » que sont les boîtes noires susceptibles d'aspirer des données. Comment réagissez-vous ?

Je comprends qu'on puisse dire que c'est une mauvaise loi, mais c'est de loin la meilleure. Et face aux problèmes qui sont aujourd'hui les nôtres, la question d'une éventuelle évasion à l'étranger de clients qui craindraient pour la confidentialité de leurs données me semble dépassée depuis quelques jours. On a trop souvent compris que cette loi reposait sur l'aspiration massive de données, ce n'est pas le cas : les boites noires ne transmettent pas de données nominatives et n'agissent que lorsque des algorithmes signalent des signaux faibles de comportement terroriste. Le point positif, c'est que cette loi amène opérateurs et hébergeurs à dialoguer avec l'État et que cela crée une co-responsabilité qui aidera à lutter contre les cyber-menaces.

Justement, n'y a t'il pas un problème de culture du web : né du militaire, il a aussi pris un virage libertaire. Comment concilier ces deux visages ?

Dans une pile électrique, il y'a deux pôles opposés, mais leur interaction crée la lumière. C'est la même chose dans le cyber-espace : il y a deux pôles, un sécuritaire et un libertaire. La peur est la fille de la sécurité, l'audace est la fille de la liberté. Il nous faut trouver la sagesse, l'équilibre. Aujourd'hui, nous avons besoin d'entendre les deux voix, et notamment celle des libertaires qui disent qu'il ne faut pas faire n'importe quoi au nom de la sécurité absolue. Le trop sécuritaire tuerait en effet le potentiel de croissance du web. Mais un cyber espace sans règles serait dominé par la loi du plus fort, avec des conceptions de la justice parfois très différentes. Dans le contexte actuel, il ne faut pas laisser les choses partir dans tous les sens : les actions contre Daesh menées par les Anonymous nous « arrangent » aujourd'hui, mais elles peuvent nous porter préjudice demain. Un des enjeux majeurs, c'est d'harmoniser la régulation mondiale du web. C'est une urgence. Il faut mettre fin au Far-West.

Réagissez à cet article

Source : http://www.lejournaldesentreprises.com/editions/44/chutier/la-menace-cyber-terroriste-n-a-jamais-ete-aussi-vaste-04-12-2015-275472.php