Veillée d'arme numérique

Cyberattaques: préparer la guerre pour avoir la paix

Les entreprises doivent s'astreindre à un entraînement quasi-militaire face aux criminels du net

Les faits — Une cyberattaque mondiale d'une ampleur jamais vue a fait ce week-end, selon le directeur d'Europol Robert Wainwright, près de 200 000 victimes, essentiellement des entreprises, dans 150 pays. Pour ce que l'on en sait pour le moment, elle n'a touché qu'une entreprise importante en France : le constructeur automobile Renault, qui a dû arrêter plusieurs sites de production. Est-ce à dire que les autres entreprises françaises sont bien préparées ? Il est trop tôt pour le dire, l'évaluation étant en cours. Ce qui est certain, c'est que prévoir la prochaine attaque est le meilleur moyen d'y survivre.

« Personne, absolument personne, n'est à l'abri. Cette cyberattaque doit servir d'alerte pour les entreprises. Pour l'heure, ses conséquences sont limitées, mais elle n'est peut-être qu'une forme d'essai. Les attaques de ce genre, dont on peine à identifier motivations et auteurs, vont se multiplier. » Ce constat, c'est celui que dresse Olivier Hassid, directeur conseil sur les questions de sécurité chez PWC, qui dirigea de 2007 à 2016 le CDSE, un organisme professionnel fédérant les directions sécurité et sûreté des grandes entreprises européennes.

Pour lui, si les entreprises françaises ont globalement compris la nécessité de s'organiser, elles doivent se résoudre à une préparation sans fin. 20 % d'entre elles sont aguerries, les 80 % restantes restent vulnérables. Il leur faut un entraînement de fond, permanent, en trois étapes : prévention, protection, gestion de crise. « Les entreprises doivent évidemment faire de la veille, préparer leurs équipes à débusquer les attaques. Elles doivent aussi s'assurer que les systèmes et les sauvegardes sont à jour. Mais, sans fatalisme, elles doivent aussi garantir qu'elles peuvent reprendre leur activité après une attaque. Cela se prépare », détaille Olivier Hassid.

Parce que les cyberattaques, désormais, ce ne sont plus simplement un fichier clients volé comme chez Orange, un faux communiqué envoyé pour nuire à Vinci ou un système de facturation au tapis. C'est un harcèlement permanent, une guerre larvée et sans fin au cours de laquelle l'entreprise peut tomber : « Ce qui a changé, c'est la digitalisation globale des sociétés. Il y a de plus en plus de perméabilité entre le système d'exploitation — c'est-à-dire l'ossature informatique des entreprises — et les systèmes industriels », ajoute Olivier Hassid.

Un sujet transversal. Les grandes entreprises doivent donc désormais considérer le cyber-risque comme un sujet vital et le faire remonter dans l'échelle d'importance. « Les cyberattaques ne relèvent plus seulement de la direction informatique, explique Philippe Cotelle, directeur du risque et des assurances chez Airbus et vice president de la commission systèmes d'information de l'Amrae (l'Association pour le management des risques et des assurances de l'entreprise). Le risque doit être géré de façon transversale par le comex, parce qu'il recouvre des domaines très vastes. Chez Airbus, par exemple, outre les bonnes pratiques informatiques, nous devons être attentifs aux aspects réglementaires qui nous sont imposés par la loi de programmation militaire, car Airbus est considéré comme un organisme d'intérêt vital, mais aussi par les directives européennes et le règlement GDPR sur les données personnelles. »

La plupart des grands groupes se sont dotés de directeurs des risques, ou de CISO (chief information security officer) pour cartographier les zones dangereuses et établir des plans de survie. Mais ils doivent aussi sortir du tabou. « La cyberattaque est un sujet sensible, qui affecte la réputation, la confiance des clients et des fournisseurs, note Philippe Cotelle. C'est aussi pour cela qu'il faut avoir un plan prêt pour réagir vite. »

Pour François Beaume, administrateur de l'Amrae et par ailleurs directeur des risques et des assurances de Bureau Veritas, « faire tout ce qu'il fallait » implique de considérer aussi l'écosystème autour des entreprises. « Si Renault, coté, a l'obligation de notifier au marché des incidents de sécurité affectant sa production, des quantités d'ETI et de PME, moins bien outillées, peuvent avoir été affectées sans qu'on le sache. Or, les grands groupes sont en interaction avec des sous-traitants qui peuvent constituer des points d'entrée dans leur système de sécurité ». Les grandes entreprises doivent donc diffuser les exigences à tout le tissu économique. Elles commencent à le faire via l'Amrae, . De son côté, l'Agence nationale de sécurité des services d'information a publié avec la CPME un guide des bonnes pratiques à l'usage de l'entreprise.

Mais il faut sans doute aller au-delà. « Même la NSA, l'agence de sécurité numérique américaine, a été hackée. Même à moi, qui suis un spécialiste, cela peut m'arriver. Nous sommes tous saturés d'informations. La digitalisation de la société nous impose désormais de développer une culture de la sécurité qui passe par absolument tous les citoyens », conclut Olivier Hassid.

PLUS DE CONTENUS SUR CES SUJETS

L'AUTEUR VOUS RECOMMANDE

Par Emmanuelle Ducros
Cybersécurité
Esthi Peshin (Israeli Aerospace) : «Il faut que les États mettent en place leur protection numérique»

Par Emmanuelle Ducros
Fric-frac numérique
Cyberfraude : alerte sur les PME

Par Cyrille Lachèvre
Far West
Trois enseignements d'une cyberattaque sans précédent

VIDÉO RECOMMANDÉE

Guillaume Poupard : Pour éviter d'être touché par la cyberattaque, "il faut être pr

Video Smart Player invented by Digiteka