CARTE BLANCHE

La quête de sécurité numérique impose une alliance public-privé

L'omniprésence des systèmes d'information dans nos organisations constitue un élément considérable de fragilisation potentielle. En effet, les réseaux sont autant de vecteurs possibles de déstabilisation pour l'ensemble des activités économiques. Les cyberattaques peuvent par exemple affecter les « tuyaux » – avec des immixtions visant à espionner, altérer, suspendre, voire interrompre les systèmes d'information et de communication. Quelles que soient la taille, la localisation géographique ou la nature de l'activité de la cible visée, les agresseurs ne manquent pas. Ancien salarié mécontent, concurrent hostile, militants politiques… Sans oublier les assauts fortuits, comme lorsque votre entité fait partie des millions d'ordinateurs contaminés par un virus informatique.

Des rançons pour récupérer ses données

La cybersécurité passe aussi par les contenus. La nature même de l'information véhiculée ou stockée sur ces réseaux représente un actif capable de porter des préjudices conséquents. Cela va des campagnes de dénigrement menées sur la Toile, à la prise de contrôle à distance – sous forme, par exemple, de cryptage – de données vous appartenant. Une rançon vous est alors réclamée, afin de vous laisser avoir à nouveau libre accès auxdites données.

Le vol d'informations ou la modification de celles-ci à l'insu de leur légitime propriétaire font également partie des périls qui guettent les utilisateurs des technologies numériques. Très souvent encore, les victimes ignorent qu'elles ont été attaquées, ne savent pas forcément évaluer les dégâts ainsi causés et n'ont pas le réflexe de s'adresser aux autorités compétentes. Une certaine méconnaissance des enjeux de sécurisation des systèmes d'information, la peur de voir sa réputation et son crédit professionnels entachés et l'absence fréquente de contacts au sein de l'appareil d'Etat expliquent largement la relative passivité

DR

Nicolas Arpagian,
coordonnateur d'enseignements à l'INHESJ et responsable du cycle Sécurité numérique au sein de cet établissement

des entreprises qui ont pourtant fait l'objet de ces opérations ciblées. Pour pallier cette situation, l'Institut national des hautes études de la sécurité et de la justice (INHESJ), l'établissement public chargé notamment des questions de sécurité intérieure, s'est associé au Cigref, l'association regroupant les patrons informatiques des grandes entreprises et des administrations françaises, afin de proposer une réponse commune à ces cybermenaces. Ils réunissent deux jours par mois, d'octobre à mai, des cadres d'entreprises concernés par cette thématique de la sécurité numérique. Ce cursus a été réalisé en partenariat avec l'ensemble des administrations qui interviennent dans la protection de la sphère numérique.

« La fragilisation, voire la mise en grave difficulté d'une entreprise à l'occasion d'une cyberattaque, est désormais un enjeu de sécurité nationale »

La gendarmerie nationale forme les DSI

A commencer par la police judiciaire, avec l'Office central chargé de la lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), la gendarmerie nationale avec ses experts de l'Institut de recherche criminelle (IRCGN), qui savent faire parler les disques durs ou les cartes SIM les plus retors, les gendarmes qui effectuent la surveillance sur le réseau des réseaux des contenus illicites (STRJD), ou enfin les équipes de l'Agence nationale pour la sécurité des systèmes d'information (Anssi) qui assurent la sécurisation du maillage informatique des ministères et des infrastructures critiques du pays.

La fragilisation, voire la mise en grave difficulté d'une entreprise à l'occasion d'une cyberattaque est désormais un enjeu de sécurité nationale : en effet, un savoir-faire et certainement des emplois sont in fine menacés. Dans ce contexte de mondialisation accélérée, de compétition internationale où tous les coups semblent permis, il convient de ne pas courir ce risque.

Au contraire, face à un tel climat de concurrence exacerbée, les entreprises françaises doivent se rapprocher des équipes gouvernementales dédiées à la sécurité de cette société de l'information qui se généralise. Rien de tel, pour ce faire, que d'entreprendre un « entraînement » en faisant plancher les collaborateurs concernés par les enjeux de sécurité numérique avec des homologues du secteur privé et des représentants des administrations spécialisées. C'est ainsi que s'établira la société en réseau, façonnée par une exploitation grandissante des technologies numériques. ■

NICOLAS ARPAGIAN