CYBERSÉCURITÉ

SOLANGE GHERNAOUTI
Professeure, directrice du Swiss Cybersecurity Advisory & Research Group, HEC – Unil (www.scarg.org)

La manipulation pire que le vol des données

Cette nouvelle forme de cyberattaque ne vise pas à la prise de contrôle de systèmes informatiques mais à celle du cerveau humain.

Jusqu'à présent, la majorité des problématiques de cybersécurité était centrée autour des questions de disponibilité et de confidentialité des données et des moyens à mettre en œuvre pour lutter contre des attaques en déni de service, contre l'espionnage ou encore le vol ou la destruction de données. Désormais, c'est la manipulation de l'information visant son intégrité, sa fiabilité et sa véracité qui semble devenir une préoccupation majeure des experts sécurité, comme le souligne en particulier l'article paru le 10 septembre dernier sur le site américain Defense One «La nouvelle vague de cyberattaque ne volera pas des données mais les modifiera».

En ébranlant la confiance dans l'information accédée, en affectant ainsi la perception de la réalité et son analyse, «l'ennemi» est paralysé et n'est plus en mesure de décider correctement.

Ce brouillage de l'information, le fait de ne jamais savoir avec certitude si elle est juste ou non, relève des mêmes mécanismes que ceux utilisés par des personnalités perverses pour rendre l'autre fou et le manipuler à son avantage. Il s'agit d'une véritable guerre psychologique et sémantique, une guerre d'influence où les manipulations à des fins tactiques et stratégiques peuvent être d'envergure et concerner la population comme également des décideurs civils et militaires. Ce type de cyberattaque ne vise pas à la prise de contrôle de systèmes informatiques mais à celle du cerveau humain.

C'est le pouvoir de l'information comme le soulignait, il y a plusieurs décennies déjà, le slogan du magazine *Paris Match* «Le poids des mots, le choc des photos», plus que jamais d'actualité, Internet offrant une caisse de résonnance sans précèdent à ce phénomène préexistant à l'ère digitale. Il suffit pour s'en convaincre de se rappeler la manière dont les photos de personnes décapitées ou d'un enfant mort sur une plage impactent le comportement des individus et influencent les décisions politiques qui affectent la vie de chacun.

Selon une des dernières études du groupe Allianz concernant les cyberrisques, l'augmentation de la connectivité et de la commercialisation des outils de la cybercriminalité accroissent le nombre, la gravité et le coût des incidents, constitue une des menaces les plus importantes auxquelles nous sommes confrontés. En outre, la performance économique de nos organisations est de plus en plus dépendante de l'impact des contraintes réglementaires liées au monde numérique et aux conséquences financières relatives à leur non respect ou consécutives à des vols de données. A cela s'ajoute, toujours selon Allianz, les coûts liés aux interruptions des affaires, aux vols de propriétés intellectuelles ainsi qu'aux chantages rendus possibles par des cyberattaques.

Bien que les cyberrisques soient complexes et multiformes, nous disposons pour les maîtriser de quelques fondamentaux qui doivent être pris en considération au niveau stratégique et instanciés en mesures opérationnelles efficaces. Cela passe entre autres par:

- une gestion continue des risques pour les éviter, les accepter, les contrôler ou éventuellement les transférer;
- l'identification des valeurs critiques de l'entreprise et des risques associés (cela ne concerne pas uniquement les risques d'origine technologique mais aussi ceux liés à l'humain, ou à une trop forte dépendance à des entités tierces, ou encore à des situations conjoncturelles de fusion, acquisition par exemple);
- une culture de la cybersécurité et une hygiène informatique appropriées;
- des plans de gestion de crise et de continuité des affaires.

Ainsi, pour une organisation, quels que soient sa taille et son secteur d'activité, toute infrastructure connectée est attaquable, augmentant notamment son risque de réputation et d'image. Dès lors, comprendre son exposition aux cyberattaques et ses nouvelles vulnérabilités afin d'être prêts à gérer les cyberincidents est devenu primordial.

Cette inévitable phase de sensibilisation aux cyberrisques est fondamentale, car elle permet de définir sa posture vis-à-vis des risques et d'agir en toute connaissance de cause mais aussi de renforcer le pouvoir de chacun à produire de la sécurité en adoptant des comportements cohérents, en réduisant sa fenêtre d'exposition et devenant un vecteur privilégié de la détection des risques et non de leur propagation.

Se connaître soi, avoir les pieds sur terre, rechercher l'authenticité ne constituent pas une autre idée du bonheur mais est devenu un invariant du développement personnel et économique et nous renvoie à la nécessité de pouvoir disposer des bonnes informations, aux bons moments, aux bons endroits, et donc à l'urgence de pouvoir contrer ou pallier les dispositifs visant à en modifier le sens et à les manipuler. ■