

La cybersécurité doit être améliorée

Selon une étude, neuf entreprises sur dix ont été victimes de cyberattaques en 2016. Malgré cela, seule une minorité d'entre elles disposent de plans d'urgence pour répondre à de telles situations. Pour maîtriser les défis de la transformation numérique, l'État et les entreprises doivent prendre les mesures qui s'imposent sans perdre un instant. *Matthias Bossard*

Abrégé Le monde numérique offre des possibilités quasi illimitées d'interactions économiques et sociales. Or, à possibilités nouvelles, risques nouveaux. Une étude de la société de consultants KPMG montre que 88 % des entreprises interrogées ont été victimes d'une cyberattaque ces douze derniers mois, avec, entre autres conséquences, des interruptions d'exploitation et des pertes financières. Pour les firmes, la cybersécurité est un impératif absolu, puisqu'elle peut décider de leur réussite ou de leur échec. Étant donné que ces attaques sont très souvent liées à un facteur humain, les systèmes de défense purement techniques ne suffisent pas. Il convient également de prendre en considération des éléments moins quantifiables, comme la culture d'entreprise, la vulnérabilité des processus opérationnels et la facilité des mesures de sécurité. Pour que la place économique suisse reste sûre, la Confédération et les entreprises se doivent d'agir.

La numérisation, l'industrie 4.0, l'Internet des objets et d'autres technologies de pointe font aujourd'hui irruption sur la scène économique. Que ce soit dans le sillage de l'économie du partage ou avec la restructuration des chaînes de valeur mondiales, les derniers développements du monde virtuel et numérique ont profondément transformé les représentations traditionnelles de l'économie suisse et l'organisation des entreprises. La collecte, l'évaluation et l'exploitation de grandes masses de données (méga-données ou « big data ») deviennent un nouveau critère de capacité distinguant les bonnes firmes des autres. Dans le même temps, les nouvelles interfaces électroniques offrent des champs nouveaux aux activités criminelles, qui ne se limitent pas toujours au monde virtuel. Grâce à l'Internet des objets, par exemple, des cyberattaques peuvent aussi causer des dégâts tangibles dans le monde déconnecté, par exemple sur des véhicules, des stimulateurs cardiaques (« pacemakers »), des commandes de machines ou encore des infrastructures critiques, comme celles de centrales électriques ou d'hôpitaux.

Pour la plupart des entreprises suisses, les cyberattaques sont devenues un réel danger. Selon la dernière étude de la société de consultants KPMG¹, 88 % des sociétés interrogées en ont été victimes ces douze

derniers mois, soit une progression de 34 points par rapport à l'année précédente. Pour plus de la moitié d'entre elles, les attaques ont provoqué une interruption d'activité et, pour plus d'un tiers, un préjudice financier (voir *illustration 1*). Malgré cela, elles sont peu nombreuses à avoir mis sur pied des programmes d'urgence pour y faire face. Il est essentiel que les entreprises comprennent que la cybersécurité est stratégiquement

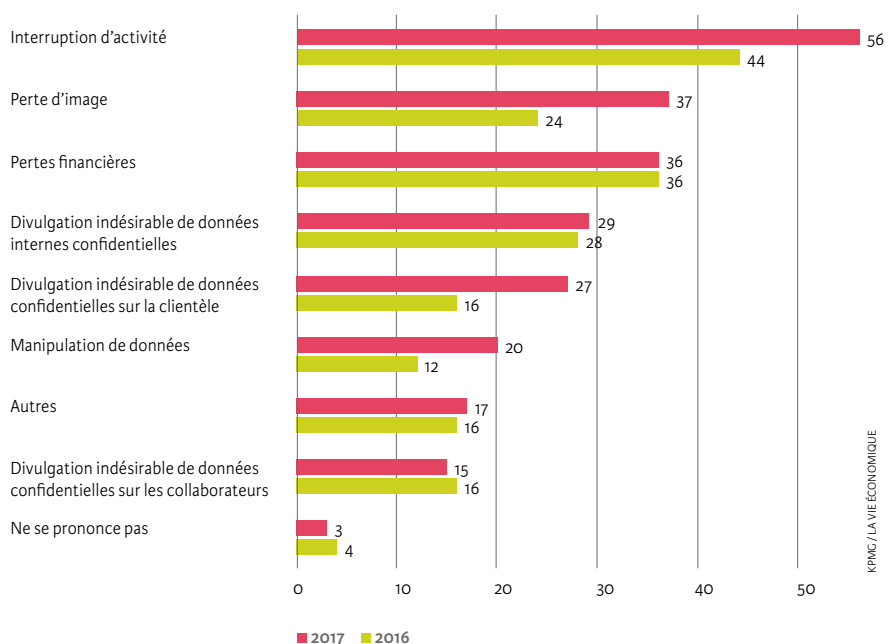
incontournable. Se mettre la tête dans le sable n'est pas une solution.

Les dangers de l'« ingénierie sociale »

Selon l'enquête, les cybercriminels cherchant à accéder aux données ultraconfidentielles d'entreprises ont, le plus souvent, eu recours aux logiciels malveillants, aux courriels d'hameçonnage ou encore au « social engineering ». Cette dernière astuce consiste à manipuler les victimes en se dissimulant sous de fausses identités ou en se faisant passer pour des autorités, par exemple.

De nombreux cybercriminels ne mettent pas seulement à profit des systèmes techniques, mais aussi le comportement humain, pour éluder des obstacles technologiques. Le circuit suivi par les données et les applications électroniques offre certes de nouveaux angles d'attaque, mais au final, même dans un monde hautement technologique, l'énergie criminelle reste toujours un élément humain.

III. 1. Formes de dommages dues aux cyberattaques (2016 et 2017, en %)



¹ Voir KPMG (2017), *Clarity on Cyber Security. Ahead of the next curve*, étude intégrale en ligne sur Kpmg.com.

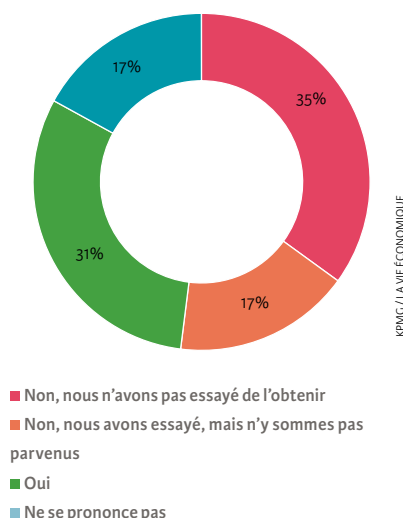
On constate aussi que, régulièrement, les dangers viennent de l'intérieur: des collaborateurs, des partenaires commerciaux, des fournisseurs ou d'autres prestataires de services. Pour cette raison, les entreprises doivent centrer leurs réflexions non pas exclusivement sur la technologie, mais davantage sur les facteurs «mous», peu mesurables, comme la culture d'entreprise, la vulnérabilité des processus opérationnels et, surtout, la simplicité avec laquelle s'applique la cybersécurité. Trop souvent, cette facilité d'utilisation ne joue qu'un rôle subalterne. C'est ce qui ressort de l'enquête de KPMG mentionnée plus haut: 65% des personnes interrogées reconnaissent que leur entreprise ne se préoccupe pas systématiquement de ce point et 11% d'entre elles seulement consultent des spécialistes sur le sujet.

L'Internet des objets recèle également des risques nouveaux. Or, l'enquête a montré que beaucoup d'entreprises suisses s'intéressent bien trop peu aux aspects sécuritaires liés à cet aspect. Plus de la moitié des sondés ont admis n'avoir aucune vue d'ensemble des appareils liés à l'Internet des objets dans leur entreprise. Près d'un tiers d'entre eux n'ont même pas essayé de l'obtenir et 17% ont essayé, mais n'y sont pas parvenus (voir *illustration 2*). Dans ces conditions, rien d'étonnant à ce que la moitié des personnes interrogées indiquent que leur stratégie de cybersécurité et les directives afférentes ne s'étendent pas à l'Internet des objets.

Les facteurs de succès: innovation et gestion des risques

La réalisation de bénéfices est indissociable du risque entrepreneurial. Le but consiste à contrôler ce dernier à tous les niveaux opérationnels ainsi qu'au sein de la direction au fur et à mesure de l'évolution technologique.

III. 2. Avez-vous une vue d'ensemble de tous les appareils liés à l'Internet des objets dans votre entreprise ?



Il faut, toutefois, conserver un espace pour l'innovation, les visions d'avenir et les technologies disruptives. Dans une économie basée sur des données et des technologies, les directions d'entreprises doivent placer la gestion des cyberrisques en haut de leur agenda. Peut-être faut-il voir comme un élément consubstantiel à la fulgurante mutation numérique la nécessité pour tous les intéressés d'apprendre à contrer les risques nouveaux. Qu'est-ce que cela signifie pour les managers? L'aptitude à tirer aussitôt le meilleur parti des très rapides développements technologiques et à exploiter les ressources des données devient un facteur de succès toujours plus déterminant pour les entreprises. Pour une entreprise désireuse d'assurer durablement sa réussite, il est essentiel de savoir quelle stratégie mettre en œuvre contre des cyberrisques spécifiques. Dans un monde de plus en plus interconnecté et comple-

xe, vouloir combattre la cybercriminalité de façon isolée n'a aucun sens. Il faut mettre partout sur pied des coopérations intelligentes, afin de mutualiser les expériences et le savoir-faire acquis. Par exemple, des synergies peuvent être organisées sur la base d'un partage d'informations concernant l'état des menaces. Elles peuvent aussi prendre la forme d'un échange d'expériences ou d'efforts de prévention conjoints. Ce qui manque à l'économie suisse, c'est une plateforme où elle puisse suivre cette menace systématiquement et efficacement.

À cet égard, la Suisse est un endroit optimal qui allie une forte capacité d'innovation à un cadre d'investissement solide. C'est une raison de plus pour ne pas perdre de temps et s'attaquer résolument à la question du cyberisque au niveau de chaque firme comme à l'échelle de la place économique toute entière. Sur le plan international, la Suisse ne s'est guère illustrée jusqu'ici comme un pays d'avant-garde en matière de cyberdéfense. Si la Confédération et les entreprises se saisissent plus résolument du problème en vue d'installer solidement dans l'économie numérisée les piliers de la réussite helvétique que sont la sécurité juridique, la sphère privée et la qualité des infrastructures, la Suisse a de bonnes chances de sortir gagnante de la révolution numérique.



Matthias Bossardt
Chef de la Cybersécurité, KPMG Suisse,
Zurich