Se protéger en matière de cybersécurité: oui, mais comment?

Le Forum économique mondial a récemment ajouté la cybersécurité à la liste des risques pour l'économie, aux côtés du changement climatique et de la pandémie de coronavirus. Selon son rapport, face à la numérisation croissante, les cyberattaques seront toujours plus nombreuses et agressives. Cela concerne différents domaines et notamment celui du droit. Comment les avocats peuvent-ils se protéger et protéger leurs clients? Nous l'avons demandé à trois experts:

Steven Meyer

Steven Meyer, ingénieur EPFL en cybersécurité et directeur de Zendata, entreprise de cybersécurité qui évalue les risques d'une organisation, fournit les services de protection adaptés et intervient sur des incidents de cyberattaques avec des investigations scientifiques digitales.

Jacques de Werra

Jacques de Werra, professeur ordinaire de droit des obligations et de droit de la propriété intellectuelle à la Faculté de Droit de l'Université de Genève, directeur du Digital Law Center, qui développe des activités de formation, de recherche et de services en droit du numérique en faveur de la communauté universitaire et de la société.

Yaniv Benhamou

Yaniv Benhamou, professeur associé de droit numérique à la Faculté de droit, spécialisé en protection et gouvernance des données, droit de la création et des technologies, membre du Digital Law Center.

Où en est la Suisse en matière de cybersécurité?

S.M. Tous les pays et les industries sont en retard. La menace a progressé ces dernières années, rendant les défenses des compagnies, des organisations et des gouvernements inadéquates. La Suisse ne fait pas partie des bons élèves. Les régulations locales ont historiquement été moins rigides que dans d'autres pays, ainsi que la sensibilisation faite par les autorités ou d'autres organismes.

J.d.W. et Y.B. Les autorités suisses sont conscientes des enjeux. Preuve en est par exemple la création d'une équipe cyber au sein de l'armée suisse. Le Centre national pour la cybersécurité (NCSC) présente régulièrement les principaux cyberincidents qui se sont produits en Suisse. Il a récemment publié son rapport sur les cyberincidents survenus au cours du deuxième semestre 2021 en Suisse et sur le plan international. Cela étant dit, la Suisse a encore beaucoup à faire, si l'on en croit le classement mondial actuel de l'Union internationale des télécommunications sur la cybersécurité où la Suisse occupe la 42ème place.

Quels types d'attaques sont les plus courantes en Suisse?

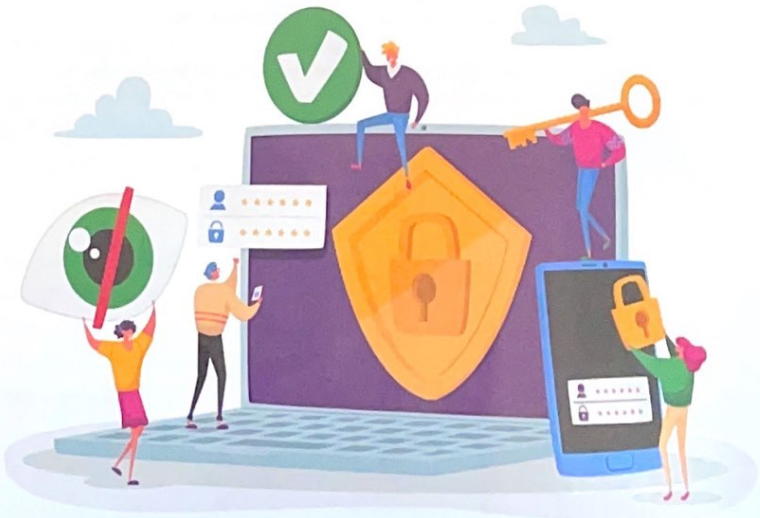
J.d.W. et Y.B. Les attaques peuvent provenir de cyberattaquants différents, comme des individus, des professionnels, des activistes, le crime organisé ou des acteurs gouvernementaux, et être de natures différentes. Selon l'OFC et le NCSC, en 2021 on recensait 30 351 infractions numériques, une augmentation de 24% par rapport à 2020. La plupart des cyberincidents étaient des cas de fraudes, rançongiciels ransomware et hameçonnage phishing.

Qu'en est-il du domaine du droit?

S.M. Les études d'avocats remplissent des critères qui motiveraient des groupes de criminels à les cibler. La sensibilité des données qu'elles détiennent les rend une proie idéale pour les ransomware. Le pouvoir de procuration de nombreuses études est intéressant à exploiter lors de BEC (Business Email Compromise). L'accès à des informations privilégiées, telles que des plaidoiries en cas de divorce ou des données sur une fusion-acquisition, sont intéressantes dans le cas de cyberespionnage industriel. Par ailleurs, les études d'avocats ne sont souvent pas bien protégées: la digitalisation du métier du droit a été assez lente et de nombreux professionnels ne comprennent pas très bien le fonctionnement de leurs systèmes digitaux.

Lorsqu'une attaque a déjà eu lieu, comment limiter les dommages?

S.M. Il ne faut surtout pas improviser, car des petites erreurs peuvent avoir de lourdes conséquences. Visiter le site de la rançon peut lancer le compte à rebours, nettoyer une infection peut déclencher un système d'autodestruction de l'appareil et manipuler l'ordinateur peut mener à la suppression d'informations utiles pour l'investigation. Idéalement, l'étude victime établit au préalable un plan d'urgence/



de continuité et se fie à une compagnie experte afin d'assurer une intervention rapide. De façon générale, chaque type d'incident requiert une réponse différente afin de minimiser les dégâts, permettre l'investigation et arrêter l'attaque.

J.d.W. et Y.B. En fonction des normes applicables, et particulièrement lorsque le Règlement européen sur la protection des données (RGPD) s'applique (également bientôt la nouvelle loi fédérale sur la protection des données LPD), des notifications doivent être faites aux autorités et parfois au régulateur de l'industrie concernée (p.ex. FINMA dans le domaine bancaire et financier) et aux personnes dont les données ont été touchées.

Comment faut-il réagir lorsqu'une rançon est demandée?

S.M. Les cyberrançons suivent le principe de la double extorsion: le cryptage des données (afin qu'elles ne soient plus utilisables par la victime) et l'exfiltration de la donnée (pour qu'elle soit rendue publique). Il faut donc avant tout savoir si les données sont récupérables (backup fonctionnel) et quelles données ont été volées. La décision de payer ou non la rançon est très personnelle. Le plus important est de faire un choix avisé en comprenant bien les conséquences du paiement et du refus d'obtempérer.

Comment les études peuvent-elles se protéger efficacement?

S.M. Un outil de sécurité à lui seul ne peut pas protéger contre des cyberattaques. En plus de produits adaptés au type de hackeurs qui vise l'étude, il faut aussi dispenser une sensibilisation des utilisateurs sur les meilleures pratiques à suivre ainsi qu'avoir en place des procédures internes ou une gestion par un service tiers. Par ailleurs, avec l'évolution des cyberattaques, une protection efficace aujourd'hui risque de ne plus l'être un mois plus tard. L'agilité est donc un facteur déterminant.

Comment se porte le domaine du droit de la cybersécurité en Suisse?

J.d.W. et Y.B. Le droit du numérique et de la cybersécurité est en plein développement en Suisse et à l'étranger et suscite un intérêt croissant de la part des étudiants et du monde professionnel.

Quelle est l'importance d'un juriste en cybersécurité pour une PME?

S.M. Le droit, les obligations et les privilèges dans le contexte de la cybersécurité sont en évolution. La nouvelle LPD va bientôt entrer en vigueur, de nombreux corps de métier sont régulés et les tribunaux exigent une responsabilisation des dirigeants et du conseil d'administration sur les procédures de protection des données. Connaître ces règles et ces enjeux est important et donne de nouvelles responsabilités aux juristes des entreprises.

Comment voyez-vous l'avenir de ce domaine?

S.M. La cybersécurité est un besoin pour des entreprises de tous types et toutes tailles, mais elle relève aussi de la responsabilité de chaque employé. Les études d'avocats doivent se protéger de façon adéquate et les entreprises vont avoir de plus en plus besoin de juristes qui les conseillent sur les problématiques de la cybersécurité et l'exposition aux risques digitaux.

J.d.W. et Y.B. La cybersécurité sera de plus en plus importante pour toutes les parties concernées, qu'il s'agisse d'entreprises, d'individus ou d'entités publiques. Il est essentiel que les secteurs publics et privés continuent de collaborer afin d'assurer un niveau de cybersécurité aussi élevé que possible. Dans notre monde interconnecté, le niveau de cybersécurité dépend de celui du maillon le plus faible: s'il est attaqué, les autres sont aussi en danger. En fin de compte, la cybersécurité est une tâche qui relève des organes dirigeants des entreprises publiques et privées dont ils assument la responsabilité.

Interview **Andrea Tarantini**