LES FAQ DU JURISTE

Faille de sécurité de l'USB : quel impact pour l'entreprise ?

La découverte d'une importante faille de sécurité de l'USB, baptisée « BadUSB », par deux chercheurs en sécurité informatique allemands, présentée à la conférence Black Hat à Los Angeles en août dernier suscite de nombreuses inquiétudes. L'exploitation de cette faille, liée à l'absence de protection interne des firmware de périphériques USB, en particulier des clés USB permettrait potentiellement l'intrusion dans un système infecté, le vol d'informations stratégiques ou encore de données à caractère personnel (dont la sécurité est une obligation légale lourdement sanctionnée).

Pour l'heure, il n'existerait pas de protection technique efficace. C'est pourquoi, pour pallier cette vulnérabilité, la mise en place d'une protection juridique est nécessaire et peut être l'occasion de revoir la sécurisation de ses systèmes, mais aussi de développer ou d'étendre l'utilisation de plateformes et d'outils de partage en ligne et dans le cloud.

Dans un premier temps, peuvent être mises à jour les politiques internes de sécurité, en concertation avec la DSI, pour minimiser les risques et définir les nouveaux outils. Concernant les solutions de stockage, partage et travail en ligne, le cadre contractuel avec le prestataire est crucial et il convient d'être particulièrement attentif aux essentiels que sont la sécurité et la propriété des données ou encore la réversibilité et la responsabilité.

Conformément aux choix stratégiques opérés, la charte informatique de l'entreprise, le livret et guide associés pourront être mis à jour. Les salariés pourront ainsi être sensibilisés à la dangerosité des périphériques USB et informés des nouvelles règles, restrictions d'usage ou interdiction des clés USB, ou encore de la connexion d'autres appareils tels que les smartphones.

Enfin, il convient de s'assurer avoir anticipé la procédure en cas d'intrusion, par quelque moyen que ce soit. Sur le plan technique, il s'agit principalement des mesures de surveillance, détection, diagnostic et information de la direction. Sur le plan juridique, les infractions d'accès et de maintien frauduleux dans un système de traitement automatisé de données permettent, le cas échéant, d'agir contre les auteurs de telles atteintes..

Par E. Barbry, avocat, directeur du pôle Droit du numérique au cabinet Alain Bensoussan, et Katharina Berbett, avocat.