INNOVATION & SOLUTIONS | ECONOMIE | IDÉES
Publié le 28 août 2021, 05:55. Modifié le 29 août 2021, 14:55.

Cyberattaques: comment continuer à travailler sans trop de contraintes?

par Grégoire Barbey

Les cyberattaques visant des entreprises suisses se sont multipliées ces derniers mois. A tel point que le Centre national pour la cybersécurité (NCSC) a fait part de ses inquiétudes, évoquant de potentielles négligences de la part des entreprises dans leur démarche pour se protéger contre les menaces. L'Association suisse des assureurs évalue le coût des cyberattaques à 9,5 milliards de francs par an rien qu'en Suisse.

Et ce chiffre va encore progresser ces prochaines années. Pandémie oblige, les entreprises se sont mises au télétravail. L'adaptation n'a pas été progressive mais abrupte, empêchant certaines d'entre elles de prendre des mesures pour opérer cette extension du milieu professionnel au domicile des collaborateurs.Dans son communiqué, le Centre national pour la cybersécurité recommande notamment de sécuriser tous les accès à distance à travers une authentification à deux facteurs ou encore de bloquer les pièces jointes à risque. Des mesures simples qui pourtant, constate-t-il, ne sont pas encore suffisamment mises en œuvre par les entreprises.

Mais si tout est si simple, pourquoi les entreprises ne l'ont pas encore fait? L'accusation de négligence portée par le NCSC est rude, et laisse entendre que les entreprises ne seraient pas suffisamment conscientes des risques inhérents à la numérisation de leurs activités. Peut-être que le problème est ailleurs. Quand bien même ces mesures de sécurité sont importantes, elles sont probablement souvent perçues comme des contraintes supplémentaires, notamment par les employés qui peuvent avoir l'impression qu'on les entrave de plus en plus dans leur travail.

La société des codes et des accès

Ingénieur en informatique et docteur en sociologie du numérique, Sami Coll estime que notre société est aujourd'hui caractérisée par une régulation des accès à l'information. «Michel Foucault a théorisé la société de l'ordre disciplinaire. Dans les années 1990, Gilles Deleuze est revenu sur cette vision,

en parlant plutôt d'un contrôle continu, considérant que nous étions entrés dans une nouvelle ère, celle des codes d'accès. On pourrait parler d'une société des codes et des accès.»

Les individus sont quotidiennement confrontés à l'obligation de se connecter partout, de façon consciente mais aussi inconsciente. «Aujourd'hui, chacun de nous est devenu une suite de codes, donnant lieu à des autorisations et des rejets. Cela peut créer un sentiment de fatigue et de frustration», continue Sami Coll.

Puisque les menaces de cybersécurité vont continuer à croître ces prochaines années, tout comme la numérisation de toujours plus d'activités économiques, les procédures d'accès devraient se complexifier d'autant plus. Mais jusqu'à quel point? Lorsque les contraintes sont trop importantes, les individus mettent en place des moyens de les contourner. Avec le risque que ces procédures sécuritaires très complexes ne soient finalement pas appliquées. Le mieux est parfois l'ennemi du bien.

Moins de codes d'accès, plus de traçage des accès

«Les individus redoublent d'ingéniosité quand il s'agit de contourner les règles qu'ils jugent trop contraignantes. C'est une situation que j'ai souvent observée dans mes activités de conseil auprès d'entreprises», relève Sami Coll. Pour y répondre, «des entreprises ont par exemple fait le choix du traçage de l'accès en interne plutôt que du contrôle de l'accès de chaque employé, partant du constat que trop de sécurité tue la sécurité».

Et toutes ces précautions peuvent-elles limiter le facteur de risque le plus incontrôlable, à savoir le facteur humain? Les cybercriminels redoublent d'ingéniosité en matière d'ingénieurerie sociale (social engineering) pour se jouer de la naïveté des individus. Pièces jointes vérolées, manipulation psychologique… sur ce point, ce ne sont pas les contraintes qui peuvent protéger les systèmes d'information des entreprises, mais bien la formation, l'éducation, pour éveiller les consciences.

La course aux contraintes sécuritaires supplémentaires pourrait donc s'avérer en définitive contre-productive. Dans un monde toujours plus numérisé, les entreprises devraient s'interroger sur les éléments qui leur sont nécessaires pour continuer leurs activités en cas d'attaque informatique. Par exemple, si les données indispensables sont uniquement accessibles sur des serveurs soumis à de potentielles attaques, il faudrait songer à les conserver également sur format papier.

A défaut de protéger les entreprises contre des cyberattaques toujours plus sophistiquées, cela augmenterait leur résilience.

Dans un monde où la cybersécurité devient un enjeu de tous les instants, la meilleure stratégie est peut-être encore d'accepter que ce risque existe, et de trouver un juste milieu entre les contraintes d'accès et la négligence.

Economie **Entreprises** **Cybersécurité** **Cyberattaques**