SÉCURITÉ INFORMATIQUE

CONFIANCE ET COLLABORATION

Existe-t-il une recette pour assurer la protection de ses données et la sécurité de ses systèmes informatiques ? Lutter contre la menace, cela implique de travailler ensemble, et d'appliquer des règles de bon sens.

Texte : Sébastien Lambotte | **Photo** : Luc Deflorenne

English, read page 58...

Jean Goetzinger, président du Clusil

Jean Goetzinger, chairman of Clusil

FR On a rarement autant parlé de menaces informatiques, de vols de données, d'attaques de systèmes, de failles numériques. La menace est proéminente, le risque latent. À tel point que c'est devenu un sujet de préoccupation majeur pour beaucoup d'entreprises mais aussi pour les autorités, l'information étant devenue une valeur clé de notre société. « *Aujourd'hui, la prise de conscience des enjeux et conséquences liés à la cybercriminalité est bien réelle* », précise Jean Goetzinger, président du Clusil, le Club de la sécurité de l'information – Luxembourg, association indépendante qui fêtera ses 20 ans l'année prochaine et qui fédère 250 membres. « *Pour preuve de cet état de fait, la* cyber resilience *était un des sujets à l'ordre du jour du dernier Forum économique mondial de Davos (WEF). La cybersécurité est désormais au cœur des préoccupations des différents chefs d'État de la planète.* »

La menace évolue sans cesse, dirigée par une réelle économie parallèle, prête à nuire aux uns et aux autres. Les malfrats profitent des failles saillantes qui existent au niveau de nos systèmes informatiques. « *Ces organisations criminelles constituent la première menace. Des pirates infectent des ordinateurs, se donnent la capacité d'en prendre le contrôle, s'accaparent des boîtes e-mail afin de permettre à d'autres d'orchestrer des attaques massives contre des cibles déterminées,* poursuit Jean Goetzinger. *L'autre grande catégorie d'attaques a trait au cyberespionnage. Les attaques de grande envergure sont orchestrées directement par des États ou par de grands groupes privés.* » La menace est portée par des gens très organisés, qui échangent beaucoup d'informations. « *Pouvoir lutter exige de pouvoir mieux collaborer. Aussi, il faut avoir une prise de conscience élevée des risques pour l'économie, pour la société,* précise Jean Goetzinger. *Ce n'est qu'une fois les risques connus que l'on peut décider quoi faire.* » Des réponses sous forme de plans d'action peuvent alors être établies à moyen ou long terme. « *La seule protection n'est cependant plus suffisante. La détection, la réaction ainsi que le recouvrement après des incidents sont aussi essentiels. Les capacités de gestion d'incidents voire de catastrophes informatiques sont aussi la clé dans la survie des entreprises ou autres entités au sein du monde interconnecté dans lequel nous vivons* », déclare Jean Goetzinger.

Bien armé

Le Luxembourg, selon lui, est bien armé face à la menace. Les réponses qui ont été développées se concrétisent derrière des entités comme la Commission nationale pour la protection des données, l'Interdisciplinary Centre for Security, Reliability and Trust (SnT) de l'Université du Luxembourg, les programmes de recherche du LIST, des solutions portées par LuxTrust, la communauté Cert.lu qui œuvrent dans l'analyse et la réponse de la menace, Cases et Bee Secure, actifs dans la sensibilisation et la prévention des risques ainsi que la présence de nombreuses associations internationales. « *Mais ce qui fait la force de la réponse réside dans la collaboration qui peut exister entre toutes ces entités* », poursuit Jean Goetzinger. Cette collaboration, avec l'échange utile d'informations entre les acteurs, exige de pouvoir se faire confiance. Celle-ci doit être confortée à l'échelle internationale pour assurer une sécurité optimale. Demain, une sécurité optimale dépendra d'un bon échange d'informations de vaste envergure afin de toujours mieux comprendre la menace d'être mieux armé pour remonter jusqu'à la source dans le but de la faire tomber. Au-delà c'est en sensibilisant chacun des utilisateurs, employés et particuliers, aux enjeux d'une bonne hygiène informatique que l'on pourra prévenir les attaques. « *La prévention, en expliquant l'enjeu de disposer d'un antivirus, de mettre à jour ses systèmes, d'installer les derniers patches est un élément clé. En effet, chacun doit avoir conscience que son ordinateur personnel, son smartphone, un compte e-mail peuvent être détournés pour être mis au service d'attaques orchestrées par des tiers.* » ✖