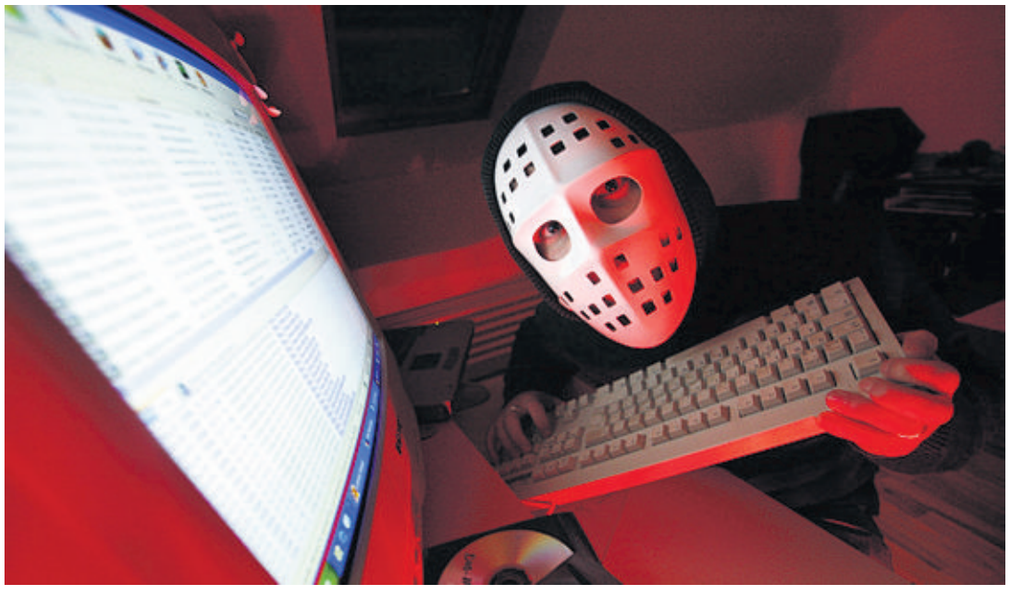
Entreprise

La sécurité informatique, un défi stratégique

Le 2e Meyrin Economic Forum s'est tenu le 27 mai. Son thème portait sur la cybercriminalité. Un danger minimisé par pas mal de sociétés

Elisabeth Tripod-Fatio
Service de la promotion économique de Genève (SPEG)



La cybercriminalité intéresse notamment les mafias, pour lesquelles le trafic illégal de données piratées est un marché très profitable. FLORIAN CELLA

«Même si une majorité d'entreprises, de collectivités publiques ou d'individus sont armés a minima contre la cybercriminalité, certains acteurs ne disposent encore d'aucun système de sécurité». C'est le cri d'alarme lancé par Solange Ghernaouti, professeur à la HEC de Lausanne et spécialiste en cybersécurité, la semaine dernière, lors de la deuxième édition du Meyrin Economic Forum (MEF).

Un dispositif minimum, «bien qu'insuffisant s'il est mal réalisé», consiste non seulement à installer un logiciel adapté, mais également à mettre au point une stratégie, ainsi qu'à acquérir des ressources et des compétences nécessaires.

Menace internationale

Au niveau global, pour être percutante, la lutte contre une menace qui dépasse les frontières doit également se faire aux niveaux institutionnel et juridique. Solange Ghernaouti recommande un cadre légal applicable au niveau national et compatible au niveau international, une police opérationnelle efficace et un système d'entraide coordonné entre chaque Etat. Une préconisation peu suivie pour le moment, puisque «treize ans après son adoption en 2001, seul un quart des Etats ont ratifié la Convention européenne de lutte contre la cybercriminalité, seul instrument d'envergure planétaire existant.» Les seules avancées notables dans ce combat sont la création en 2013 de l'European Cybercrime Centre d'Europol à La Haye et le centre INTERPOL Global Complex for Innovation à Singapour.

«Pour une PME, une fuite de 40 000 contacts équivaut à des pertes de 488 000 francs en amendes et frais associés»

Dominique Vidal
Fondateur de SecuLabs

«Une entreprise qui aura la réputation de se protéger efficacement gagnera la confiance des consommateurs»

Solange Ghernaouti
Spécialiste en cybersécurité

Guerre économique

Pour l'experte, la situation est d'autant plus inquiétante qu'internet est devenu une véritable arme de guerre économique: «La cybercriminalité n'est pas uniquement le fait de criminels. Les mafias sont en concurrence avec les entreprises respectables pour engager les spécialistes informatiques les plus compétents, d'où qu'ils viennent. Le trafic illégal de données est un marché très profitable.»

Les PME touchées aussi

Même s'ils ont pris conscience des dangers, nombreux sont encore ceux qui minimisent le risque. Pourtant, pour un hacker expérimenté, une attaque est parfois d'une simplicité déconcertante et peut être effectuée en quelques minutes seulement. Dominique Vidal, fondateur de SecuLabs, l'a prouvé en réalisant des démonstrations de piratage qui font froid dans le dos. L'une de celles-ci se nomme «l'injection SQL». Face à un public meyrinois médusé, il a ainsi montré avec quelle facilité il est possible, en exploitant une faille de sécurité d'un site web, de s'emparer des données d'un internaute qui a simplement entré son login et son mot de passe. Une attaque semblable a, par exemple, permis à des pirates de dérober 1,3 million de données de clients d'un célèbre opérateur de télécommunication en France.

«Ce cas montre que toutes les entreprises, quelle que soit leur taille, peuvent être touchées», prévient le capitaine des «routards», l'équipe vice-championne du monde de hacking. Et les pertes liées à une attaque ne sont pas négligeables: «Pour une PME, par exemple, on estime qu'une fuite de 40 000 contacts équivaut à des pertes de 488 000 francs en amendes et frais associés.»

Veille permanente

Face aux nombreux dangers et aux risques engendrés pour la vitalité même de l'entreprise, une protection efficace se traduit par une veille permanente pour détecter les menaces et les vulnérabilités, ainsi qu'un système de sécurité autant informatique que physique. Solange Ghernaouti tient à souligner que cette lutte ne doit pas uniquement être vue comme un centre de coûts: «Une veille peut également permettre de découvrir des opportunités pour son marché, des informations stratégiques ou de nouveaux clients. De même, une entreprise qui aura la réputation de se protéger efficacement gagnera la confiance des consommateurs.»

Les deux intervenants s'accordent à dire que c'est d'abord à chacun, individu, entreprise ou collectivité publique, de se protéger. «Le choix d'un bon système de sécurité, parmi les nombreuses offres existantes, n'est pas aisé. Il faut prendre le temps de comparer et éventuellement se faire conseiller par un spécialiste. Ensuite, sensibiliser ses collaborateurs aux bonnes pratiques est fondamental. Appliquer les quelques règles d'or de la sécurité informatique permet déjà d'éviter la grande majorité des attaques», conclut Patrick Schefer, conseiller aux entreprises au sein du SPEG.

Pour en savoir plus sur l'aide que le SPEG peut apporter aux sociétés: *www.ge.ch/entreprises*.