Centre Patronal

Service d'information

Publication hebdomadaire

N° 3223 – **30 janvier 2019**

Ne négligez pas la sécurité informatique!

La sécurité informatique constitue une responsabilité individuelle et collective. Les règles de prudence doivent être connues et appliquées de manière systématique et rigoureuse, en ayant conscience que le piratage est devenu un enjeu financier considérable, tant pour les pirates que pour leurs victimes.

Le piratage informatique devient une véritable industrie

Les risques liés à l'informatique et à la numérisation font l'objet d'innombrables publications et de mises en garde régulières. Est-il encore utile d'écrire quelque chose sur ce sujet? Gageons que oui, dans la mesure où les pratiques individuelles évoluent lentement et où l'on constate encore certains manques de prudence au sein des entreprises et de leurs collaborateurs. Or l'économie helvétique, de par sa prospérité, attire la convoitise de nombreux pirates. On entend dire que la Suisse figure à la troisième place des pays européens les plus ciblés. A cela s'ajoute que le piratage informatique est maintenant devenu une véritable industrie, avec des entreprises criminelles qui recrutent des spécialistes de divers domaines et offrent ouvertement leurs services à d'autres entreprises, contre rémunération.

A l'ampleur du phénomène répond une préoccupation politique croissante. La mission première de l'Etat, dans ce domaine, est de protéger ses propres systèmes (cyberdéfense) et de sécuriser la cyberadministration – voire la cyberdémocratie, avec le développement contesté mais probablement inéluctable du vote électronique. Les pouvoirs publics doivent en outre veiller à faire évoluer certains aspects de la législation et à offrir une infrastructure permettant de vérifier l'identité de nos interlocuteurs sur internet (identité électronique). Ils peuvent soutenir l'action des hautes écoles, qui développent de nouvelles solutions techniques et de nouvelles formations dans le domaine de la cybersécurité.

L'administration fédérale met à disposition divers services permettant d'aider les entreprises à évaluer et à améliorer leur sécurité. Le plus connu est la centrale d'information «MELANI», qui fait régulièrement le point sur les risques les plus actuels, sur leurs conséquences et sur les moyens de s'en protéger. On peut encore citer la présence en ligne d'un test rapide de cybersécurité pour les PME, proposé par l'association faîtière ICTswitzerland avec le soutien de la Confédération et d'autres partenaires.

Une liste (non exhaustive) de mesures de sécurité

Toutes les entreprises devraient exploiter au mieux ces différents outils afin de renforcer leur sécurité, en se souvenant que les entreprises peu connues ou de taille modeste ne sont pas moins visées que les autres: d'une part, les pirates les considèrent comme des proies plus faciles; d'autre part, elles peuvent servir de portes d'entrée vers des entreprises plus importantes. A l'inverse, les grandes entreprises doivent être conscientes que leurs sous-traitant peuvent parfois représenter les «maillons faibles» de leur sécurité.

Suite au verso

Impressum

Editeur:
Centre Patronal
Rédacteur responsable:
P.-G. Bieri

Route du Lac 2
1094 Paudex
Case Postale 1215
1001 Lausanne
T +41 58 796 33 00
info@centrepatronal.ch

Kapellenstrasse 14
3011 Bern
T +41 58 796 99 09
cpbern@centrepatronal.ch

www.centrepatronal.ch

Service d'information

L'économie helvétique, de par sa prospérité, attire la convoitise de nombreux pirates. La Suisse figure à la troisième place des pays européens les plus ciblés.

D'un point de vue pratique, il importe de lister et d'évaluer chaque type de risque: perte ou blocage de données, paralysie d'infrastructures stratégiques, pertes financières découlant de vols ou de rançons, atteintes à la réputation. Quant aux mesures de sécurité à respecter, elles sont généralement connues: être extrêmement prudent avec les courriers électroniques reçus, vérifier leur expéditeur, se méfier des liens qu'ils contiennent de même que des pièces jointes; vérifier les certificats d'identité des sites sur lesquels on navigue, surtout si on doit y entrer des informations; recourir, là où c'est possible, à des procédures de double authentification (confirmation par le téléphone portable) et adopter dans tous les cas des mots de passe complexes et différents pour chaque service, en suivant l'évolution de la technologie (des mots de passe inviolables aujourd'hui risquent de devenir inopérants avec le développement des ordinateurs quantiques).

Tendances actuelles: objets connectés et ingénierie sociale

Certains risques restent encore trop souvent négligés, par exemple la multiplication des objets connectés: éclairages télécommandés, télésurveillances, voire de simples photocopieuses. Si ces objets sont mal sécurisés, ils peuvent offrir un accès facile à tout le réseau d'une entreprise. Un autre danger délicat à maîtriser est l'ingénierie sociale, où des pirates, en s'aidant de données informatiques, tentent d'exploiter des failles humaines, par exemple en se faisant passer pour un cadre ou un dirigeant de l'entreprise, ou pour un fournisseur. Le réseau le mieux sécurisé ne sert à rien si un collaborateur régulier se laisse convaincre d'opérer un versement non contrôlé ou de divulguer un mot de passe.

D'une manière générale, tous les collaborateurs doivent être sensibilisés et formés aux cyber-risques et à la manière de s'en prémunir. La sécurité informatique constitue une tâche collective, autant à l'intérieur d'une entreprise que pour l'ensemble de l'économie helvétique, dont elle peut devenir un précieux atout concurrentiel.

Pierre-Gabriel Bieri

Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI :
www.melani.admin.ch

Formulaire d'annonce d'événement pour les entreprises :
www.melani.admin.ch/melani/fr/home/meldeformular/unternehmen.html

Test rapide de cybersécurité pour PME proposé par ICTswitzerland :
www.cybersecurity-check.ch