LABEL CYBER SAFE

Aider les PME à se protéger de la cybercriminalité, à prix léger

Le label Cyber Safe a été conçu spécifiquement pour les PME qui n'ont pas les moyens de mandater des sociétés de sécurité informatique pour qu'elles procèdent à des audits de leur système.

PIERRE CORMON

Mandater une société de sécurité informatique pour auditer votre système? La facture peut très vite grimper au-dessus des moyens de nombreuses PME. Elles renoncent donc le plus souvent à ce genre de démarche. C'est précisément pour elles que l'Association suisse pour le label de cybersécurité vient de lancer le label Cyber Safe. Il permet de réaliser un audit de manière beaucoup plus légère et bon marché que ce qui se fait habituellement.

UNE DÉMARCHE PARTICIPATIVE AVEC LES PME

L'idée est née d'une discussion entre deux amis, Nicolas Frey, expert en sécurité informatique, et Christophe Hauert, chargé de cours à la Faculté des sciences sociales et politiques de l'Université de Lausanne. Pour être sûr que leur label corresponde aux attentes des PME, ils ont opté pour une démarche participative, en s'entourant de représentants de différents secteurs. Côté économie, ont notamment participé des responsables de la Fédération des Entreprises Romandes Neuchâtel, de la Fédération patronale et économique de Fribourg, de la Fondation The Ark ou de chambres de commerce.

● Comment se passe le processus de labellisation?

Le processus comprend plusieurs étapes:

⇨l'inscription se fait en ligne, sur le site du label;

⇨un expert effectue une première visite d'environ deux heures. Il aide l'entreprise à remplir un questionnaire analysant différents points liés à la sécurité informatique (quelles sont les pratiques en matière de sauvegarde, de mots de passe? etc.). Il examine les données dont l'entreprise dispose, ainsi que leur valeur (quelles seraient les conséquences si elles étaient perdues, divulguées?). Il effectue enfin une étude poussée du réseau, afin d'identifier d'éventuelles faiblesses;

⇨l'association collecte les adresses e-mail de tous les collaborateurs et, pendant six semaines, effectue des tentatives de *phishing* (en français, hameçonnage, une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance, comme une banque, une administration, etc.) et observe comment les employés y réagissent.

⇨Elle rédige ensuite un rapport sur la base du questionnaire, de l'étude effectuée et des tentatives de *phishing*. Ce rapport chiffre la valeur des données (et donc le préjudice potentiel) et liste les éventuelles faiblesses et les mesures que l'entreprise devrait prendre pour y remédier, classées par ordre de priorité. L'entreprise a un délai de deux semaines à trois mois pour y remédier.

LE PRIX EST PROPORTIONNEL AU NOMBRE D'EMPLOYÉS ET DE POSTES DE TRAVAIL INFORMATIQUES.

⇨Lorsqu'elle s'estime prête, un auditeur revient dans l'entreprise une demi-journée pour vérifier si les mesures préconisées ont été appliquées. Il donne sur cette base une recommandation d'attribuer ou non le label à la société, pour une durée de deux ans.

⇨Si le label est attribué, l'association continue à faire occasionnellement des tentatives de *phishing* ou des études du système informatique de l'entreprise. Celle-ci s'engage à lui faire part d'éventuels changements substantiels dans son infrastructure informatique.

⇨Au bout de deux ans, le processus recommence pour prolonger le cas échéant le label et adapter le système de l'entreprise aux nouvelles menaces.

● Combien cela coûte-t-il?

Le prix est proportionnel au nombre d'employés et de postes de travail informatiques. Il s'échelonne entre trois mille francs pour une entreprise de moins de dix employés et neuf mille neuf cents francs pour une entreprise d'un peu moins de deux cent cinquante employés. «Notre label s'adresse principalement à des entreprises qui n'ont pas plus de cent à cent cinquante employés», remarque Christophe Hauert. Des rabais seront accordés aux membres des organisations ayant participé au projet.

● Sera-t-on protégé contre tout?

Non, c'est impossible. «Nous nous concentrons sur les menaces les plus courantes, ce qui nous permet d'automatiser largement les processus», remarque Christophe Hauert. «C'est ce qui nous permet de proposer un prix bas.» Une attaque sur mesure et personnalisée est beaucoup plus difficile à écarter, mais les petites entreprises en font rarement l'objet. ■

www.cyber-safe.ch