24heures

Trois outils de cybersécurité pour les PME et les communes

Informatique

Le programme vaudois Seal accompagne le développement de solutions techniques et préventives à paraître l'an prochain.

«La question, ce n'est pas de savoir si on va être attaqué, mais quand!» Le ton était donné dès l'ouverture de la table ronde sur la cybercriminalité à l'attention des dirigeants de PME, des administrations publiques et organisations locales. Mercredi soir dernier, la discussion a apporté des conseils pour organiser sa défense numérique et présenté les premiers outils développés par le programme public baptisé Seal. La rencontre s'inscrivait en marge de Black Alps, un sommet international réunissant 600 spécialistes de la cybersécurité à Yverdon-les-Bains.

Le récit de la cyberattaque subie en 2020 par la Fondation Les Oliviers, au Mont-sur-Lausanne, est venu illustrer une menace en forte hausse: +43% de plaintes en 2023 et 27 millions de francs de pertes dans le canton. Pas du tout préparé, l'organisme de réinsertion pour personnes dépendantes avait fonctionné en mode dégradé pendant plus de deux mois, peinant à délivrer les traitements médicaux à ses résidents, à payer ses 120 collaborateurs et à honorer les commandes des clients.

«Si les petites structures montrent moins de naïveté en matière de cybersécurité depuis la crise sanitaire, elles sont toujours désespérées, car elles manquent de moyens et il existe peu de solutions adaptées pour elles», relève Sandy Wetzel. C'est justement la vocation du programme Seal d'innovation en confiance numérique et cybersécurité que l'ancien directeur d'Y-Parc dirige depuis un an. Financé à hauteur de 3 millions de francs par le Canton de Vaud, il met à contribution les ressources de l'EPFL, de l'UNIL et de la HEIG-VD.

Un capteur de sécurité

Trois projets ont été sélectionnés cet été et sont en cours de développement pour renforcer la sécurité numérique des petites entités privées et publiques. Ils aboutiront l'an prochain. Une solution technique baptisée Watchdog se matérialise sous la forme d'un boîtier à brancher contenant un capteur de sécurité, pilotable à distance et facile d'utilisation. Il sera commercialisé à moins de 1000 francs par mois par l'entreprise de cybersécurité morgienne Hacknowledge.

Deux autres outils, dématérialisés, verront le jour. Iris proposera un serious game simulant des cyberattaques à contrer, spécialement conçu pour le personnel des collectivités publiques par l'agence veveysanne Marvelous. L'École des sciences criminelles de Lausanne participe au niveau de l'analyse du comportement des joueurs. Enfin, des solutions techniques, organisationnelles et juridiques gratuites doivent émerger pour aider à combattre le phishing (hameçonnage).

Sommairement, les experts de la table ronde ont conseillé de mener une analyse de menaces, de former ses collaborateurs et de préparer un plan de continuité pour les services critiques en cas d'attaque. Plusieurs solutions consistent à utiliser un gestionnaire de mots de passe, avoir un antivirus à jour et un filtre DNS, installer un scanner de logiciels malveillants, voire chiffrer les disques durs pour décourager les hackers. Certains peuvent envisager une certification, comme le label cyber-safe.

Par ailleurs, la filière informatique et systèmes de communication de la HEIG-VD propose gratuitement de mener des tests d'intrusion. «Quand

on parvient à sortir les fiches de salaire de l'entreprise depuis l'extérieur, ça peut motiver le patron à prendre des mesures», confie Jean-Marc Bost, professeur en cybersécurité.

Fabien Lapierre