

Cybersécurité : l'État aide les entreprises à se protéger

Les entreprises sont toutes concernées par la sécurité de l'information. La digitalisation de l'économie est porteuse de grandes opportunités mais aussi de nouveaux risques. Les menaces contre la sécurité de nos informations se développent constamment. Chaque semaine nous apporte son lot de révélations sur des fuites de données ou autres incidents informatiques impliquant des grandes marques.

Certains seraient tentés de croire qu'étant « petits » et peu visibles, ils présentent moins d'intérêt pour les *hackers* et seraient à l'abri des attaques. C'est une erreur. Les attaques contre les systèmes d'information sont la plupart du temps menées par des robots qui utilisent les vulnérabilités les plus connues pour tenter de prendre le contrôle d'un ordinateur ou d'un serveur. De ce fait, les victimes ne se rendent pas toujours compte qu'elles le sont. Une fois entrés, les attaquants ne se font pas forcément remarquer. Ils peuvent simplement utiliser nos ordinateurs pour mener d'autres attaques.



Il est donc primordial de protéger correctement son système d'information et les données qui y sont stockées. Le gouvernement luxembourgeois a développé différents outils que les PME peuvent utiliser pour progresser dans ce domaine. Voici les 4 mousquetaires de la cybersécurité :

1. Start-up Security Kit
2. Diagnostic CASES
3. Analyse des risques
4. Aides publiques (nouveau)

Le Start-up Security Kit est un outil d'évaluation en ligne permettant aux entreprises de faire un check-up rapide de leur niveau de sécurité. L'outil s'adapte aux différents secteurs d'activité au travers d'un questionnaire modulable. Il comporte également une dimension progressive en permettant aux entreprises d'avancer à leur rythme à travers 3 niveaux de protection : Start, Fit et Top. Les entreprises qui veulent progresser davantage et bénéficier d'un regard externe sur leur sécurité peuvent s'adresser à CASES pour un diagnostic gratuit.

Ensuite, rien de tel qu'une analyse complète des risques pour pouvoir les gérer d'une manière systématique. CASES propose à ce stade une méthode spécialement dédiée aux PME, qui permet à ses utilisateurs d'économiser beaucoup de temps et d'argent grâce à la capitalisation réalisée sur les analyses de risques antérieures. Cette méthode baptisée MONARC (Méthode Optimisée d'Analyse des Risques CASES) a l'immense avantage d'abaisser considérablement la barrière d'accès à une analyse de risques complète. Il s'agit d'un outil performant qui s'use uniquement si on ne s'en sert pas.

Enfin, la cerise sur le gâteau est d'ordre financier : les entreprises qui feront appel à des experts en matière de sécurité de l'information pourront recevoir des aides allant jusqu'à 50 % des frais. Le conseil ET l'implémentation des mesures de protection sont éligibles à ces aides.

Cette aide financière est destinée aux PME artisanales et commerciales. Celles-ci doivent disposer d'une autorisation d'établissement octroyée par la Direction générale PME et Entrepreneuriat du ministère de l'Économie pour des services fournis par des conseillers extérieurs et prestés occasionnellement pour des projets ponctuels. La demande d'aide se fait à l'aide d'un formulaire disponible sur le Guichet Entreprises.

Lors de la journée *Cybersecurity4Success* qui s'est déroulée à la Chambre de Commerce, la secrétaire d'État Francine Closener a rappelé que la cybersécurité faisait partie intégrante de la stratégie économique du Luxembourg. Elle a indiqué que les entreprises qui désirent relever le défi du marché unique numérique peuvent compter sur le soutien du ministère de l'Économie. Carlo Thelen, directeur général de la Chambre de Commerce, a pour sa part insisté sur la nécessité pour les entreprises de se protéger davantage « face à la multiplication des risques numériques et à la recrudescence des cyberattaques de plus en plus sophistiquées ». Plusieurs entreprises ont ensuite témoigné de l'importance de la formation et de la valeur ajoutée du Diagnostic CASES. A bon entendre...

www.cases.lu