Des piratages informatiques facilités en raison d'un personnel trop peu qualifié

Des piratages informatiques facilités en raison d'un personnel trop peu qualifié

EY publie les résultats d'une étude mondiale sur le cybercrime qui fait état des menaces grandissantes auxquelles sont confrontées la plupart des entreprises. Les menaces principales sont notamment le phishing, les logiciels malveillants et la fraude.

Un état des lieux bien réel

La cybercriminalité apparaît aujourd'hui comme une menace globale dont les contours sont difficiles à appréhender. La prolifération de ce type d'agressions, souvent impunies par ailleurs, touche autant le secteur public que privé.

L'étude du cabinet EY intitulée Get Ahead of Cybercrime et menée auprès de 1.825 entreprises dans 60 pays montre que les entreprises ne sont pas suffisamment préparées à faire face aux inévitables attaques informatiques. Ainsi, plus d'un tiers (37%) des entreprises n'ont pas de perception en temps réel des risques cyber et ne disposent pas de la souplesse, du budget et des compétences nécessaires pour lutter contre la cybercriminalité en augmentation.

Dans le monde, 43% des sondés indiquent que leur budget total dédié à la sécurité de l'information restera globalement identique au cours des 12 prochains mois en dépit des menaces

grandissantes. Au Luxembourg, 53% des sondés ont tout de même l’intention d’augmenter de plus de 5% leur budget en matière de sécurité de l’information.

Un personnel trop peu sensibilisé au risque informatique en cause

Mais c’est la négligence des employés, tout autant que leur prise de conscience insuffisante des risques, qui représente la plus importante vulnérabilité face à la cybercriminalité.

54% des sondés ont relevé un manque de ressources qualifiées

dont 6% disposent d’une équipe d’évaluation des menaces et 35% concèdent ne pas être dotés d’un programme d’évaluation des menaces.

Anticiper les attaques
Au Luxembourg, les menaces principales sont notamment le **phishing (25%)**, les **logiciels malveillants (20%)** et la **fraude (17%)**.

«Les entreprises doivent adopter une attitude proactive plutôt qu’une attitude uniquement

réactive, les faisant dès lors évoluer de cibles faciles pour les cybercriminels vers de redoutables adversaires»

conseille Brice Lecoustey, à la tête du département Advisory pour le secteur commercial et public chez EY Luxembourg.

À travers plusieurs recommandations, le rapport encourage les entreprises à considérer la cybersécurité comme une capacité concurrentielle essentielle. Afin d'atteindre cet objectif, l'entreprise est tenue de se maintenir dans un état permanent de préparation, d'anticiper de nouvelles menaces éventuelles et de perdre cet état d'esprit de «victime» devant conduire ses activités dans un état d'anxiété permanent.

«Au-delà des menaces internes, les entreprises doivent mener une réflexion plus large relative à leur 'écosystème' commercial et à l'incidence potentielle de leurs relations avec des tiers et des vendeurs en matière de sécurité», ajoute Olivier Maréchal, à la tête du département Advisory pour le secteur financier chez EY Luxembourg. Avant de conclure:

«C'est uniquement en atteignant un niveau avancé de préparation en matière de cybersécurité qu'une entreprise peut commencer à

réellement bénéficier des investissements consentis dans ce domaine.»

Références :

http://paperjam.lu/news/cybersecurite-les-entreprises-plutot-desarmees

par EY, Brice Lecoustey et Olivier MaréchalEY

cliquez ici pour consulter le rapport