Phishing, ransomware, virus : TPE et PME, sortez couverts !

La menace cyber est réelle et ne pèse pas que sur les grands groupes, « bien au contraire même », alerte la House of Cybersecurity. Encore (trop) souvent négligée par de (trop) nombreuses PME, la sécurisation des infrastructures connectées ne figure pas suffisamment au rang de leurs priorités. Un comportement à risque difficilement justifiable alors même que des solutions de protection, commercialisées à un tarif « raisonnable » – et subventionnées –, sont sur le marché.

Les virus

Premier constat, première erreur commise par un grand nombre de TPE et de PME au Luxembourg : « *Je suis trop petit pour intéresser des hackers.* » Cette croyance, partagée par une frange d'entrepreneurs sous-estimant le niveau de la menace cyber, s'avère totalement fausse : «

Elle est même dangereuse et nourrit les appétits malveillants », avertit Dominique Kogue, head of the National Cybersecurity Competence Center of Luxembourg. Le NC3 (pour les intimes) est l'une des deux entités, avec le Computer Incident Response Center (CIRCL), qui composent la House of Cybersecurity. Chacune évolue dans son registre : pour schématiser, NC3 agit sur le terrain de la prévention tandis que CIRCL réagit en cas d'intrusion, « *quand c'est déjà trop tard et que l'attaque a atteint ou paralysé un système. Comme des pompiers, ils éteignent le feu.* »

Ravageurs, ces incendies en ligne gagnent en intensité, année après année.

Pour se convaincre du niveau critique de la menace, rien que sur le seul mois de septembre 2025, le bras armé de la House of Cybersecurity a enregistré plus de 1.000 tickets liés à des incidents de cybersécurité. Toutes ces tentatives ou intrusions avérées ne ciblent pas que des poids lourds de la finance ou des acteurs institutionnels de renom. Derrière les attaques médiatisées de ces derniers mois – celle qui a paralysé durant de longues heures le réseau de télécommunications de l'opérateur Post en juillet dernier a marqué les esprits – sévit une myriade d'opérations hostiles menées dans le cyberespace des PME. Ces entreprises de moindre envergure constituent des cibles privilégiées car plus facilement atteignables : « *Les banques et les grosses entités disposent d'un environnement numérique très sécurisé. La plupart des PME n'ont pas cette culture. Leur système présente de nombreuses failles, de nombreuses portes d'entrée pour les attaquants.* »

« Les données clients, cela vaut plus que de l'or ou du pétrole »

[Dominique Kogue, head of the National Cybersecurity Competence Center of Luxembourg]

Facteur aggravant : les cyberagressions se révèlent plus sophistiquées que dans un passé encore récent. Sans surprise, la cybercriminalité tire profit, elle aussi, de l'émergence de l'IA pour corrompre des systèmes. Le *phishing* (hameçonnage en français), technique frauduleuse largement répandue qui consiste à se faire passer pour une personne de confiance par le biais de messages falsifiés (emails, SMS, etc.) en est l'exemple parfait : « *Avec les progrès en traduction réalisés par l'IA, il est de plus en plus aisé de rédiger des courriels sans faute en anglais ou même en luxembourgeois.* »

Cet art du camouflage numérique permet de duper sa cible en l'amenant à ouvrir un lien corrompu ou à l'inciter à partager des identifiants de connexion, des numéros de carte bancaire, des informations personnelles et professionnelles. Nombre d'entrepreneurs n'ont pas conscience de la valeur de ces données: « *Cela vaut pourtant plus que de l'or ou du pétrole,* illustre Dominique Kogue*. Elles sont très recherchées sur le dark web, notamment pour entraîner des modèles d'IA.* »

La House of Cybersecurty propose aux entreprises un exercice immersif de simulation de crise cyber, durant lequel les participants font face à une cyberattaque réaliste (crédit : Jean-Michel Cavalli).

Les antidotes

Deuxième constat, deuxième erreur commise par un grand nombre de TPE et de PME au Luxembourg : « *Je n'ai pas de temps à consacrer à ces questions de cybersécurité et je n'ai pas*

les moyens d'investir ». Pour le directeur du NC3, ce discours n'est plus justifiable, du moins au Luxembourg.

Son entité déploie des outils pour auditer les capacités de résilience des entreprises. Car avant de songer à contrer la menace, encore faut-il mesurer l'épaisseur de son propre cuir. À ce titre, la plateforme d'autoévaluation *Fit4Cybersecurity* permet aux organisations d'évaluer leur niveau de maturité en cybersécurité. Un rapport est généré automatiquement avec des recommandations. Autre plateforme au nom évocateur, *Testing Platform* enjoint les PME à réaliser des tests de base sur leur infrastructure et leurs systèmes; ici, l'objectif consiste à identifier et à corriger les vulnérabilités courantes susceptibles d'être exploitées. Les applications *Pandora* et *Spambee* sont, elles, préconisées respectivement pour l'analyse de fichiers ou documents suspects et la vérification des e-mails douteux reçus. Enfin, la plateforme *Observatory* offre un panorama complet sur les menaces cyber (CTI) observées au Luxembourg, présenté de manière accessible pour les PME.

La question de l'évaluation réglée, demeure celle relative à l'investissement requis pour rendre plus robuste sa défense cybernétique. C'est là qu'intervient la politique de subventionnement mise en place par le gouvernement avec le soutien, notamment, de la House of Entrepreneurship de la Chambre de Commerce. Le 11 mars dernier, le ministre de l'Économie Lex Delles a dévoilé le lancement de deux nouveaux SME Packages, dont l'un spécifiquement dédié à la cybersécurité. Concrètement, l'aide financière couvre potentiellement 70 % des coûts engagés par une PME pour renforcer sa cyberdéfense. Précision : le montant du projet doit se situer entre 3.000 et 25.000 euros (HTVA). De l'avis (expert) de Dominique Kogue, cette somme serait « *suffisante* » pour muscler l'environnement numérique des petites et moyennes entreprises. Des prestataires listés par son organisation sont en mesure d'implémenter de nombreuses solutions visant, par exemple, à rendre moins perméable l'identification de mots de passe via des gestionnaires ou à cloisonner les réseaux en limitant les accès et les données collectées.

À ce jour, une soixantaine de PME ont exploré la voie de ces SME Packages pour une trentaine de dossiers instruits. Encourageant ou insuffisant selon les points de vue, ce démarrage témoigne surtout d'une prise de conscience naissante des PME des dangers qui menacent leur fonctionnement, voire leur existence : « *Certaines PME victimes d'une cyberattaque ont parfois mis un mois à s'en remettre. D'autres ne se sont même jamais relevées.* »