

MOSELLE

Cyberattaques : les PME dans le viseur des hackers

Près d'une PME française sur cinq a déclaré avoir été victime d'une cyberattaque informatique l'année dernière. Une tendance à la hausse liée à la digitalisation des entreprises mais aussi à l'essor du télétravail. En face, la défense s'organise au niveau régional mais il reste du chemin à parcourir.

Malwares (logiciels malveillants), ransomwares (rançongiciels), spywares (logiciels espions), phishing (hameçonnage)... L'arsenal des pirates informatiques est vaste. Il démontre leur détermination à obtenir ce qu'ils sont venus chercher : de l'argent principalement, mais aussi des données sensibles ou des informations. Leurs cibles : les Petites et moyennes entreprises (PME), les Très petites entreprises (TPE), les collectivités jusqu'aux systèmes de défense d'un État... Polymorphe, la menace pèse sur les entreprises.

« Elles luttent désormais contre des mafias qui agissent parfois pour le compte d'un État »

« Elles ne sont plus face à de petits hackers dans leur garage. Elles luttent désormais contre des mafias qui agissent parfois pour le compte d'un État », indique Régis Lhoste, président de Cyber-Detect, une entreprise nancéienne de protection informatique.

La pression s'accroît sur les PME françaises. Elles seraient une sur cinq à avoir été victime d'une cyberattaque en 2021. Selon l'Agence nationale de sécurité des systèmes d'information (ANSSI), le nombre d'attaques sur les PME a augmenté de 53 % entre 2020 et 2021. « L'usage de plus en plus fréquent de données informatiques en fait des cibles de premier choix », indique Florence Christmann, directrice du bâtiment totem Thi'Pi, à Thionville.

Si les PME sont des cibles de choix, c'est aussi parce que certai-

nes semblent encore minimiser le risque. D'après un récent sondage réalisé par la Commission européenne auprès de 501 PME, seules 19 % se sentiraient menacées. En négligeant leur protection, elles deviennent des proies faciles pour les hackers. Derrière, c'est tout un réseau d'entreprises qui peut tomber : « On se rend compte que les grands groupes peuvent avoir des soucis si les PME avec lesquelles elles travaillent sont attaquées », résume Florence Christmann.

Des techniques simples aux plus perfectionnées

« Il y a une multiplicité des attaques et elles sont de plus en plus sophistiquées », prévient Régis Lhoste. Le chef d'entreprise cite les techniques les plus pointues utilisées par les hackers pour soustraire de l'argent à leurs victimes : usurpation d'identité, cryptage des disques durs... « Ils bloquent votre système et exigent une rançon pour que vous puissiez récupérer vos données », détaille Fabrice Genter, président de la Confédération des petites et

moyennes entreprises de Moselle (CPME).

Une de leur technique en vogue consiste à se faire passer pour un fournisseur et prétexter un changement d'Iban, puis récupérer les fonds sur un compte en banque et s'enfuir avec le magot. Avec des conséquences parfois dramatiques pour les entreprises, qui ne peuvent pas être assurées contre ce type d'escroquerie.

La défense s'organise

En Moselle, les PME semblent enfin avoir pris conscience de la menace. « On travaille dessus depuis plusieurs années. C'est entré dans les mentalités. Les entreprises ont compris l'importance de la sauvegarde de leurs données. Elles savent aussi que la clé, c'est la réactivité », assure Fabrice Genter.

Selon David Glijer, directeur de la transformation digitale d'ArcelorMittal France, il resterait toutefois beaucoup de travail, au niveau régional, pour renforcer la coopération des entreprises. Ce sera tout l'enjeu des rencontres



cyber du Grand Est, qui auront lieu le 14 juin à Uckange (Lire par ailleurs).

Damien GOLINI

Premières rencontres entre acteurs de la sécurité informatique à Uckange



Les rencontres cyber auront lieu au Digital lab d'Uckange, le 14 juin. Photo d'archives RL/Philippe NEU

Quelques jours après le Forum international de la cybersécurité organisé à Lille, un autre événement réunira les acteurs régionaux du cyber. Ce sera en Moselle cette fois, le 14 juin à Uckange, dans le nouveau digital lab d'ArcelorMittal. Ce bâtiment, inauguré il y a quelques semaines, est la vitrine du savoir-faire en termes d'innovation digitale du géant sidérurgique. Il y abrite plusieurs laboratoires de recherche dans les domaines du big data, de l'intelligence artificielle et de la maintenance.

C'est dans son auditorium qu'auront lieu les premières rencontres cyber du Grand Est. Organisées conjointement par le bâtiment totem Thi'Pi de Thionville, le réseau Entreprendre en Lorraine Nord, ArcelorMittal et soutenue par la région Grand Est, ces rencontres ont pour but de créer un réseau professionnel entre acteurs du cyber dans la région. « Il y a, d'un côté, les PME de l'industrie qui ont la nécessité d'améliorer leur cybersécurité dans un contexte de transformation digitale de leur activité et, de l'autre, des acteurs compétents mais peu connus. L'objectif est de les faire se rencontrer afin de tisser des liens et monter un collectif du cyber », résume Florence Christmann, responsable du Thi'Pi à Thionville.

Durant trois jours, PME, jeunes pousses, collectivités et prestataires de services spécialisés vont pouvoir échanger autour de ce thème. Des représentants de grands groupes nationaux (Schneider Electric, Orange, ArcelorMittal) présenteront les enjeux concrets et apporteront des solutions à la cybermenace. Ce premier rendez-vous sera reconduit plusieurs fois par an.



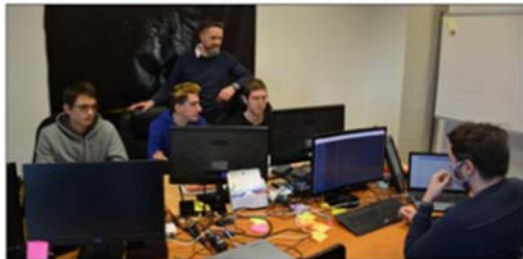
La menace s'accroît sur les PME, cibles privilégiées des hackers. Photo d'illustration ER/Lionel VADAM

Dans le Grand Est, des compétences mais peu de reconnaissance

Régis Lhoste est président de la société nancéienne Cyber-Detect. Créée en 2017 par des chercheurs du Loria (Laboratoire lorrain de recherche en informatique et ses applications, Université de Lorraine), elle a pour cœur de métier d'assurer la cybersécurité des entreprises. « Nous sommes un maillon de la chaîne de leur protection », résume-t-il.

Ses clients : de grands groupes industriels mais également des entités du secteur de la Défense. « Les pirates créent des variants de virus préexistants, qui ont été modifiés pour cibler une entreprise. Ils dorment parfois plusieurs mois sur un réseau pour en extraire les données. Notre métier consiste à détecter et supprimer ces variants », explique Régis Lhoste.

En quelques années, Cyber-Detect s'est fait un nom dans le secteur de la cybersécurité dans le Grand Est. Elle n'est pas la seule : le marché est en pleine croissance. Pour-



Installée dans le campus Artem à Nancy, la start-up Cyber-Detect sait repérer un virus russe. Photo ER/Guillaume DECOURT

tant, ces sociétés peinent à être reconnues au plan national. « Par rapport à d'autres régions comme la Bretagne ou l'Île de France, il n'y a pas de pôle cyber Grand-Est. Les acteurs sont nombreux mais chacun avance de son côté, sans coordination. Il faudrait que les entreprises, les start-up et l'université puissent se rapprocher pour travailler en collaboration. » Et que les collectivités prennent, enfin, la me-

sure de l'enjeu, souffle-t-il en filigrane. De ce côté-là, un timide frémissement s'opère. La région Grand Est tiendra, pour la première fois, un stand au Forum international de la Cybersécurité (FIC) à Lille (du 7 au 9 juin), pour y représenter ses acteurs. Le thème de cette FIC 2022 : l'Europe. Tout, sauf un hasard pour une région qui la pratique au quotidien...

D.G.

QUESTIONS À

David Glijer, directeur de la transformation digitale chez ArcelorMittal France

« Pour ne pas subir, il faut s'unir »

En quoi la cybersécurité est-elle un enjeu majeur pour ArcelorMittal ?

« ArcelorMittal France a l'ambition d'être leader de l'industrie 4.0. Notre stratégie de transformation digitale comprend deux programmes phares que sont le déploiement de la 5G Steel et la création de nos deux digital lab (à Uckange et Dunkerque). Le déploiement de la 5G offre de nouvelles solutions de mobilités mais dans ce contexte, il est certain que le risque de cyberattaques devient un enjeu majeur. »



David Glijer est directeur de la transformation digitale chez ArcelorMittal France.

Photo RL/Armand FLOHR

Quels sont les moyens dont vous disposez pour vous défendre ?

« Pour ne pas subir, il faut s'unir et créer des écosystèmes au niveau local, régional, national et international. Dans cette optique, ArcelorMittal a intégré le campus cyber France et nous candidaton à la reconnaissance d'un campus cyber régional. Le but est de fédérer autour de nous un écosystème fort, avec tous les acteurs régionaux du Grand Est. La meilleure des défenses, c'est aussi d'adopter des comportements adaptés et réduire la surface d'attaque. Responsabiliser les collaborateurs, les former et partager avec nos partenaires et nos entités notre expertise. »

Vous sentez-vous investis d'une mission de conseils et d'expertise vis-à-vis des PME/TPE industrielles locales en matière de cybersécurité ?

« Bien sûr. Quand une PME est touchée, elle peut mettre la clé sous la porte. Elles sont plus sensibles qu'une grosse structure comme ArcelorFrance. 19% des PME disent avoir été attaquées l'année dernière, c'est bien moins que la moyenne européenne, mais cela ne signifie pas qu'elles le sont effectivement moins. Cela veut surtout dire qu'elles le détectent moins bien. Il y a un décalage de perception et un énorme travail à faire. C'est pourquoi nous voulons fédérer autour de nous, afin d'éviter les dépôts de bilan et les pertes d'emploi. »

Propos recueillis par D.G.

LE CHIFFRE

FRANCE

53 %

Selon l'Agence nationale de sécurité des systèmes d'information (ANSSI), le nombre d'attaques sur les PME françaises a augmenté de 53 % entre 2020 et 2021.

Elles seraient une sur cinq à avoir été victime d'une cyberattaque en 2021.