Une Semaine à...

Nancy / NUMÉRIQUE

Cyberattaques : la Région déploie son

La Région, épaulée par de nombreux partenaires, vient de créer **« GRAND EST CYBERSÉCURITÉ »**, un **SERVICE D'ASSISTANCE GRATUIT** installé à Nancy et destiné aux PME, ETI, collectivités et associations du Grand Est **VICTIMES DE CYBERATTAQUES**.


Depuis quelques années, les cyberattaques se multiplient. Entreprises, collectivités, organismes publics et particuliers, personne n'est épargné.
© DR

« **504** *portail expiré* » ou encore « *site actuellement en maintenance* » : voilà ce que l'on pouvait lire, lundi 27 mars, sur la page Internet de l'Assemblée nationale dont les services ont confirmé, en milieu d'après-midi, qu'ils faisaient « *face à un excès de requêtes qui [paralysait] le site* ». Dans le même temps, le groupe de hackers pro-russes NoName057(16) a revendiqué sur Telegram cette cyberattaque, présentée comme une riposte au soutien de la France à l'Ukraine, a repéré le spécialiste Numerama. Une enquête a été ouverte auprès du parquet de Paris pour « *entrave au fonctionnement d'un système de traitement automatisé de données* ».

L'exemple illustre bien le besoin de se prémunir de dispositifs mais aussi de faire preuve de pédagogie et d'accompagnement pour les victimes. « *Pour une simple et bonne raison,* **le numérique est omniprésent, les connexions sont nombreuses, donc nous sommes tous concernés** », explique **Jean-Yves Marion**, directeur du Laboratoire lorrain de recherche en informatique et ses applications (Loria-CNRS, Inria, Université de Lorraine) à Villers-lès-Nancy. Ses équipes s'activent pour mieux comprendre les rouages et stratagèmes des hackers, « **qui ne sont plus des adolescents boutonneux installés dans des garages** *mais bien des entités parfaitement organisées et en capacité de nuire. Avec un budget, des équipes et des moyens de communication. Tout cela lié à des groupuscules ou des États bien évidemment* », poursuit le scientifique. Être en capacité de répondre aux nouvelles attaques et en découvrir les vecteurs, anticiper le plus possible comme développer de nouveaux algorithmes de chiffrement, voilà les défis de la recherche pour ces prochaines années. Une fierté pour **Hélène Boulanger**, présidente de l'Université de Lorraine, et **Edwige Helmer-Laurent**, déléguée régionale de la délégation Centre-Est du CNRS.

Et il faut aller très vite car la menace a explosé ces trois dernières années. Des données confirmées par **Emmanuel Naëgelen**, directeur général adjoint de l'Agence nationale de la sécurite des systèmes d'information (Anssi). « *La menace est massive et n'épargne personne : des entreprises de taille intermédiaire (40 % des rançongiciels traités ou rapportés à l'Anssi en 2022) aux particuliers, grands groupes en passant par les hôpitaux (10 %) ou les collectivités (23 %). Avec des conséquences importantes : des entreprises à l'arrêt, des prestations sociales qui ne sont plus versées ou encore des données personnelles utilisées* », précise-t-il.

Un guichet unique pour les victimes

Via France Relance, l'État a souhaité dès 2021 répondre aux menaces de manière pragmatique via des espaces régionaux de cybersécurité. Un appel entendu très tôt par la majorité régionale conduite à l'époque par Jean Rottner qui s'était impliquée dans la démarche. « *Parmi les premières propositions du Business Act figurait la cybersécurité. Et nous sommes tous touchés de près ou de loin.* **Une attaque de cyberterrorisme se produit toutes les quinze secondes dans le monde !** *Du mail frauduleux à la menace en passant évidemment par le vol de données. Chez moi à Épernay, une entreprise a perdu 15 millions d'euros à la suite d'une cyberattaque. Elle avait les reins solides pour affronter cette vague mais tout de même ! Avec les conséquences que cela implique, il est normal que cette question soit prise en compte dans les problématiques régionales* », explique **Franck Leroy**, le nouveau président de la Région Grand Est, en présence d'Irène Weiss, conseillère régionale déléguée à la cybersécurité.

En Grand Est, les TPE et PME ont plus particulièrement besoin d'être accompagnées, à l'instar des collectivités territoriales de petite et moyenne taille. Pour apporter des solutions face à cette menace, un collectif de partenaires (État, Région, Anssi, Gendarmerie, Loria, Inria, CNRS, Université de Lorraine) s'est formé autour d'objectifs communs : coordonner, identifier les offreurs de solutions et proposer une seule porte d'entrée en Grand Est avec une véritable organisation afin de prévenir, sensibiliser, équiper et ainsi être le plus efficace possible dans la gestion de crise. Une de ses traductions : la création de « Grand Est Cybersécurité », le centre d'assis-

▶ L'ACTEUR

Soteria Lab : des experts de la sécurité informatique

C'est une **PÉPITE NANCÉIENNE** passée de deux salariés à près de dix en quelques mois. Spécialisée dans la sécurisation des systèmes d'information, l'entreprise a **DOUBLÉ SON CHIFFRE D'AFFAIRES** en un an. Preuve d'une demande croissante. **CLÉMENT JOLIOT**, à la tête de Soteria Lab, explique.

▶ Il sensibilise à tout-va. Il y a quelques jours, lors de la matinale d'Aprofin, l'association des professionnels de la finance et du chiffre de Lorraine, devant un public de banquiers, assureurs, experts-comptables, notaires, avocats mais aussi étudiants, Clément Joliot a délivré des messages d'anticipation et de « *premiers secours* » face aux risques numériques. Son entreprise accompagne tout type d'organisation pour la sécurisation des systèmes d'information. « *Cela se traduit par une action de notre part en quatre points. Le premier s'illustre par la gouvernance :* **quelle politique de sécurisation est mise en place dans la structure ?** *Le deuxième revient à effectuer un audit de sécurité. Nous allons ainsi inspecter minutieusement l'organisation, ses process comme ses technologies afin d'observer les systèmes et les failles potentielles. Nous activons aussi la technique avec la réalisation de tests d'intrusion. Nous pénétrons ainsi les systèmes, non pas pour semer totalement le bazar et faire perdre des données à l'organisation mais bien pour confirmer que les vulnérabilités existent et que des risques importants en découlent par la suite* », explique le chef d'entreprise.

La troisième opération de Soteria Lab est de passer dans une phase curative : trouver les réponses aux incidents en aidant à la fois à la gestion de crise et à la reconstruction. « *Il faut immédiatement s'interroger en se demandant où, par où et surtout comment corriger ces incidents et ces failles béantes dans le système, puis dans un second temps, celui de la reconstruction, prioriser les systèmes. C'est ce que l'on appelle dans le jargon, un "sanity check"* », détaille Clément Joliot.


Le président de Soteria Lab connaît une activité en forte croissance.
© DR

Enfin, dernier pilier de l'action de l'entreprise : la formation. À destination des dirigeants comme des collaborateurs qui vont bien souvent avoir les mains dans les process et sont donc susceptibles de détecter en premier les intrusions. « **L'utilisateur reste un élément central et essentiel dans la sécurité des processus.** *La formation au hacking permet d'expliquer de quelle manière les attaques sont organisées et orchestrées* », confie le passionné de sécurité informatique.

« Ce guichet unique répond à un besoin croissant »

Depuis sa création en 2016, Soteria Lab est en pleine croissance. Avec toujours plus de cyberattaques chaque année, et même un potentiel record en ce mois de mars 2023 selon le site spécialisé Zataz, la prise de conscience de la part des acteurs économiques, collectivités et autres structures se veut de plus en plus large. « **N'oublions pas que les cyberattaques sont une réelle industrie et sont devenues la première économie parallèle au monde.** *Avec des chiffres d'affaires qui s'élèvent à plusieurs milliers de milliards de dollars par an. C'est assez incroyable ! Les conséquences pour les entités touchées sont tout autant gigantesques voire catastrophiques. Il est donc de plus en plus important de se prémunir face à ces risques* », prône Clément Joliot.

Son entreprise fait partie intégrante de Grand Est Cybersécurité. Une évidence d'être aux côtés de ce dispositif d'accompagnement avec des partenariats protéiformes. « *Quand les entreprises ou organismes publics sont touchés, ils sont paniqués et ne savent pas du tout vers qui se tourner. Là, avec ce guichet unique qui répond à un besoin croissant, nous saurons agir de manière coordonnée avec davantage d'efficacité et d'efficience. C'est une très bonne chose et Soteria Lab est très fière de pouvoir y contribuer* », conclut Clément Joliot.

BZ

plan de défense

La conseillère régionale déléguée, Irène Weiss, et le président de la Région Grand Est, Franck Leroy, ont présenté les contours de « Grand Est Cybersécurité ».

© Région Grand Est

tance aux victimes d'attaques informatiques. Cette plateforme permet désormais aux PME, ETI, collectivités et associations du Grand Est, victimes de cyberattaques, de bénéficier d'un service d'assistance gratuit. **Opérationnel depuis le 14 février dernier**, il est localisé à Nancy et opéré par Grand E-Nov +, l'agence d'innovation et de prospection internationale de la Région Grand Est. Ce service d'assistance comprend une prise en charge personnalisée et immédiate avec préqualification de l'incident et une assistance de premier niveau ; une mise en relation avec des prestataires qualifiés pour répondre à l'incident ; un suivi de l'incident jusqu'au rétablissement de la situation ; un accompagnement à la judiciarisation ; un suivi des statistiques d'incidentologie à l'échelle régionale. Pour accompagner les victimes, des entreprises partenaires spécialistes du domaine. « *Il est aujourd'hui essentiel d'apporter des gestes de premier secours car* **il y a des choses à faire immédiatement quand on est victime d'une cyberattaque. Déjà, il ne faut pas avoir honte d'en parler.** *Même quand on est chef d'entreprise et que l'on craint les répercussions. Ensuite, les procédures techniques s'enchaînent* », explique Emmanuel Naëgelen, directeur général adjoint de l'Anssi.

Un plan régional et un campus dédié

Convaincu qu'il est nécessaire de **procéder à de « l'hygiène numérique »** pour reprendre les mots d'Irène Weiss, **la Région Grand Est veut mettre le paquet dans la prévention, l'anticipation et la formation**. Elle a donc pour objectif de lancer, au second semestre 2023, un « Campus Cyber Grand Est » ouvert à tous les acteurs de la cybersécurité du territoire et travaillant en réseau pour rapprocher la cybersécurité des utilisateurs. Destiné à devenir à terme la référence sur le sujet, ce Campus coordonnera et mutualisera les efforts et ressources de la communauté régionale. « *Ce sera un lieu totem qui regroupera tout l'écosystème. En matière de sensibilisation, de développement des compétences, de partages de données, d'innovations et de coopérations transfrontalières* », complète **Irène Weiss**.

Par ailleurs, approuvé par les élus de la Région Grand Est le 23 mars dernier, le plan régional cybersécurité 2023-2025 s'articule autour de la prévention et la préparation des acteurs aux cybermenaces en accroissant leur niveau de résilience en cybersécurité. « *Cela passe notamment par le "diagnostic cybersécurité" déjà mis en place par la Région pour les entreprises. Depuis son lancement en novembre 2022, plus de 50 entreprises régionales ont déposé une demande d'aide pour mettre en œuvre ce diagnostic. Son élargissement à l'ensemble des collectivités et associations régionales permettra de* **faire de la gestion du risque cyber un réflexe dans le Grand Est** », explique Franck Leroy. L'accompagnement de la gestion de la crise cyber, avec l'appui de Grand Est Cybersécurité, l'animation et le développement d'une filière régionale de la cybersécurité avec des partenariats protéiformes comme le développement des compétences pour répondre aux besoins croissants des entreprises et de la filière assurent le positionnement du Grand Est sur un marché mondial de la cybersécurité en forte croissance.

Baptiste Zamaron

Pour joindre Grand Est Cybersécurité, un numéro de téléphone (0 970 51 25 25) et un site Internet (cybersecurite.grandest.fr).