

## GRAND EST

# Cybersécurité : la Région sort la grosse artillerie

Plus la digitalisation des entreprises, des collectivités et des hôpitaux avance, plus le risque d'attaque par des pirates informatiques est grand. Pour faire face à la menace, la Région vient de se doter de nouveaux outils. Objectif : assurer sa cybersécurité.

Sacrée coïncidence. Alors que le gouvernement annonçait que le site internet de l'Assemblée nationale avait été victime d'une cyberattaque menée par des hackers russes, la région Grand Est dévoilait son plan de cybersécurité. Mardi 28 mars à Nancy, le laboratoire de recherche en informatique et ses applications (Loria) a accueilli des professionnels de la cyberdéfense. Des gendarmes, des policiers, en présence de Blaise Gourtay pour représenter Josiane Chevalier préfète de la grande région, Emmanuel Naëgelen, directeur général adjoint de l'Agence nationale de Sécurité des systèmes d'information (ANSI) et bien sûr le nouveau patron de l'exécutif régional, Franck Leroy. Des officiels et un collectif de partenaires pour montrer que face à la



La signature du plan de cybersécurité à Nancy le 28 mars 2023 avec Sylvain Dorschner, directeur général chez Grand E-nov, Franck Leroy, président de la région Grand Est, Blaise Gourtay, représentant Josiane Chevalier, préfète de la région Grand Est, Irène Weiss, conseillère régionale déléguée à la cybersécurité. Photo ER/Magalie DELLE-VEDOVE

multiplication des attaques par des pirates informatiques la Région organise sa « cyber-riposte. »

## Une menace pour les petites entreprises

La cybersécurité, ce n'est pas de la science-fiction. Emmanuel Naëgelen, spécialiste de la sécurité des systèmes d'information l'a démontré en rappelant quelques exemples d'incidents récents. En avril dernier, le

groupe hospitalier de territoire Grand Est (GHT) a été victime d'une cyberattaque. Les pirates informatiques, on s'en souvient, avaient mis aux enchères les fichiers récupérés dans les hôpitaux de Vitry-le-François et Saint-Dizier. Dans la foulée, Clestra Hauserman, une entreprise alsacienne, a été elle aussi victime d'une cyberattaque de type ransomware (rançongiciel). Pendant 3 mois, l'entreprise n'a plus eu accès à sa comptabilité, à son système de paye et à sa base commerciale. « Pour cette entreprise, a précisé Emmanuel Naëgelen, le coût de l'attaque a été estimé entre 2 et 3 millions d'euros »

Tout le problème est là. Pas question de laisser des pirates ruiner la santé économique régionale. Mais quand une entreprise est prise en otage par des pirates informatiques, elle n'a pas forcément les moyens d'assurer sa défense. « Il est d'autant plus important de pouvoir agir,

a précisé le président de la Région Franck Leroy, qu'on sait qu'une entreprise attaquée sur deux ferme dans les six mois. » Grâce à une dotation d'un million d'euros obtenue dans le cadre du plan France Relance, le Grand Est a donc orchestré sa défense numérique avec ses partenaires (l'État, la gendarmerie, le Loria, le CNRS et l'université de Lorraine).

## Le centre de cybersécurité régional basé à Nancy

La stratégie de cybersécurité de la Région prévoit des actions de sensibilisation contre les cybermenaces, une proposition de diagnostic de sécurité gratuit pour les entreprises et un accompagnement en cas d'attaque par des professionnels de la cyberdéfense. Et puisqu'en la matière, il faut former des talents aptes à parer l'ingéniosité des pirates, le plan prévoit aussi des formations. « Le besoin est réel, a rappelé Franck Leroy. Depuis le lancement fin 2022 d'une proposition de diagnostic en cybersécurité, 50 entreprises du territoire ont déjà déposé une demande d'aide. » Les entreprises qui ont déjà appelé à l'aide et toutes celles qui vont suivre seront dirigées vers le centre de cybersécurité du Grand Est basé à Nancy. Elles profiteront d'une assistance gratuite. Des hackers éthiques, professionnels de l'informatique qui connaissent bien les pirates et leurs techniques, ont été recrutés pour les épauler. Le service est complet : de l'accompagnement personnalisé jusqu'à la judiciarisation du dossier.

Magalie DELLE-VEDOVE

■ Centre de cybersécurité du Grand Est : 0970 512 525 ou [cybersec@grandest.fr](mailto:cybersec@grandest.fr)

## LE CHIFFRE

# 40 %

Le rançongiciel consiste à envoyer à la victime un logiciel malveillant qui chiffre l'ensemble de ses données et à lui demander une rançon en échange de la clé de déchiffrement. 40 % des rançongiciels traités en 2022 touchaient des petites entreprises. Dans 23 % des cas, les victimes étaient des collectivités territoriales et dans 10 % des cas, des établissements de santé.

## Du « hacking éthique » pour s'entraîner

Mardi dernier, lors de la présentation du plan de cybersécurité régionale, il n'y avait pas que des VIP. Il suffisait de descendre de deux étages dans le bâtiment du Laboratoire lorrain de recherche en informatique et ses applications (Loria) pour changer d'ambiance. Là, une vingtaine d'étudiants, les yeux rivés sur leurs ordinateurs, font face à un véhicule à quatre roues. Leur mission ? Endosser le rôle des « méchants » et prendre le contrôle du robot à l'aide de leurs ordinateurs. Du « hacking éthique », en somme. Leur adversaire d'un jour a été conçu par Vincent Person, du groupe d'expertise en ingénierie Englab.

### Étudiants contre robot

Un cyber-entraînement sous la forme d'une bataille acharnée... Les étudiants n'ont que quelques informations à leur disposition pour infiltrer le système du robot et le faire rouler. L'ambiance est à la compétition : quel groupe sera le plus rapide ? « Bon courage pour nous rattraper ! », lancent Thi-



C'est une course pour ces étudiants en informatique : quel groupe arrivera à hacker leur cible en premier ? Photo ER/Laura MAX

bault et Tristan à leurs camarades. Les deux étudiants, en deuxième année à Telecom, école d'ingénieurs en informatique et en sciences du numérique, sont en avance. Tous les participants, qu'ils soient de Telecom, de Polytechnique ou d'ailleurs, se sont portés volontaires pour participer à ce « cyber-affrontement ».

### « Premiers secours » pour les victimes de cyberattaques

Tels des guides bienveillants, d'autres pros du numérique

passent entre les étudiants. Ce sont les membres du CSIRT, le tout nouveau Centre de réponse d'urgence aux incidents de cybersécurité régional basé à Nancy. S'ils s'amuse au petit concours en train de se dérouler, ils seront confrontés à des attaques un peu plus offensives... Leur challenge à eux est désormais de procurer les « premiers secours » aux victimes de cyberattaques, mais aussi de mettre ces dernières en relation avec des prestataires de confiance pour limiter la

casse. Dernière étape de leur mission : inviter les victimes à contacter les forces de l'ordre, pour inciter à porter plainte. Plus tôt dans la matinée, la conseillère régionale Irène Weiss avait fait remarquer que « se faire hacker, c'est comme se faire cambrioler ». Une menace qui n'est donc pas prise à la légère, si ce n'est le temps de quelques heures dans la salle remplie de « hackers éthiques », où les cerveaux s'activent face à la difficulté du défi !

Laura MAX