L'Est républicain, 8 mars 2020 (édition Nancy)

GRAND EST Politique

Région Grand Est : la riposte après la cyberattaque

L'institution régionale a réglé discrètement en quelques jours l'attaque par un rançongiciel dont elle a fait l'objet en février. Elle a relevé son niveau de sécurité. Aucune donnée personnelle n'a été touchée, assure l'entourage de Jean Rottner.

Que s'est-il exactement passé sur le réseau informatique du conseil régional dans la nuit du 13 au 14 février ? Peu de détails filtrent. Une enquête est en cours, commencée à Strasbourg par la police judiciaire, puis transférée à Paris.

Selon la chronologie et les pièces versées au dossier, un mail de demande de contact a été envoyé par un hacker, en vue de fixer une rançon. Aucun montant n'est annoncé sur le mail qui a été transmis par la Région à la PJ dès le 14 février, suivi dans la foulée d'un dépôt de plainte.

Jean Rottner évoque rapidement une attaque extérieure et de fermeture de serveurs lors de la commission permanente. Mais l'ampleur n'est pas précisée. Principe de précaution ? C'est le premier réflexe quand une collectivité, une entreprise fait l'objet d'une intrusion.

Le système informatique de la Région est placé en mode dégradé pendant 72 heures, couvrant le week-end qui suit. L'intranet est bloqué le temps des vérifications. L'entourage de Jean Rottner assure aujourd'hui que ni les données personnelles des agents ni des données protégées (coordonnées bancaires, notes financières, virements) n'ont été affectées par la tentative de hacking. Dès le mardi, soit quatre jours après l'intrusion, les agents et les élus sont de nouveau autorisés à envoyer des mails avec des pièces jointes.

« Niveau de sécurité relevé »

« Nous avons tiré les leçons de ce hacking en relevant notre niveau de sécurité plus que largement, en moins d'une semaine, le fonctionnement normal de l'informatique était rétabli », confie un proche de Jean Rottner. Parmi les premières mesures, la vérification approfondie de tous les réseaux et des 1. 700 postes, puis le changement des mots de passe. Les ordinateurs sous exploitation Linux, la majorité des postes, n'ont pas été impactés, contrairement à ceux fonctionnant sous Windows, indique la Région. La veille est renforcée, les précautions dans la circulation de documents sensibles multipliées. « Avant même cette cyberattaque, nous avions déjà pris déjà l'habitude de ne pas passer par les réseaux pour les dossiers les plus sensibles qui sont transmis via des messageries cryptées », ajoute-t-on à la Région.

Le réseau informatique du Conseil régional a été la cible d'un e tentative de piratage dans la nuit du 13 au 14 février dernier. Photo d'illustration Alexandre MARCHI

Ph. R.

« Les hackers de plus en plus professionnels »

Dernière victime d'une cyberattaque cette semaine : l'entreprise de lingerie Lise Charmel, qui vient d'annoncer s'être placée en redressement judiciaire après avoir vu son système informatique frappé par un rançongiciel. Un rançongiciel, c'est un code malveillant empêchant la victime d'accéder au contenu de ses fichiers afin de lui extorquer de l'argent en appliquant un chiffrement de fichiers ou en créant un code de sabotage. C'est ce qu'explique le rapport sur l'état de la menace du rançongiciel publié en février dernier par l'Agence nationale de sécurité des systèmes d'information (Anssi) à l'intention des entreprises et des institutions.

En back-office

Le rançongiciel, c'est une menace que connaît très bien Jean-Yves Marion. Directeur du Laboratoire lorrain d'informatique et ses applications (Loria), fondateur du Laboratoire de haute sécurité (LHS), il dirige une équipe qui fait référence bien au-delà de l'Hexagone. Depuis le LHS, en collaboration avec un centre homologue au Japon, les chercheurs scrutent la carte mondiale des attaques sur la toile. « Notre métier est de faire de la recherche fondamentale, pas des enquêtes, mais nous sommes parfois consultés par des organismes d'État en back-office », indique Jean-Yves Marion. Ses chercheurs ont été par exemple sollicités aux États-Unis suite aux immixtions dans la campagne américaine, ciblant Hillary Clinton, de cybercriminels réputés proches du Kremlin. La cybercriminalité des États est une réalité, toujours difficile à prouver, déplore Jean-Yves Marion. Tout comme l'identité des hackers, très rapidement loups solitaires, mais plutôt représentants d'officines malveillantes ou de puissants groupes mafieux.

1. 500 milliards de dollars

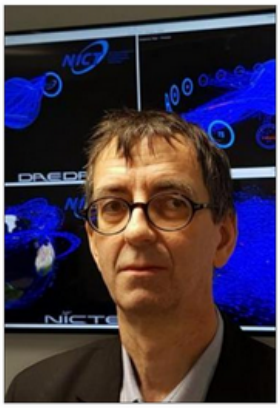
La recherche de profits financiers et l'espionnage constituent les deux principales motivations des cybercriminels, précise le patron du Loria. « Les cybercriminels de plus en plus professionnels mènent des attaques de plus en plus ciblées ». L'Anssi évalue l'économie du hacking à 1. 500 milliards de dollars en 2018, offrant un bénéfice annuel de 2 milliards à ses acteurs.

La plus grosse attaque récente a émané en 2017 du logiciel malveillant WannaCry qui a infecté 300. 000 ordinateurs dans 150 pays. Entreprises, collectivités, mais aussi les particuliers sont visés. Et tenus de déclarer le moindre incident, même si l'image de marque en prend un coup et cause un préjudice.

« Renforcer sa sécurité informatique »

Bouygues Construction a été paralysé par une cyberattaque en début d'année. L'année 2019 a vu des attaques contre Altran en janvier, la ville de Sarrebourg en juin, le CHU de Rouen en novembre. « Les systèmes sont de mieux en mieux protégés, c'est la surface d'attaque qui s'accroît avec tous les objets connectés, téléphones, box, montres, il est difficile de barricader tous les postes », relève Jean-Yves Marion. Il invite les particuliers à la vigilance : « Comme c'est virtuel, on se dit à quoi bon prévoir une sécurité robuste, et on achète au rabais, comme si on choisissait d'acquérir une voiture sans frein pour la payer moins cher ».

« À chaque attaque, il faut tirer les leçons et ne pas hésiter à renforcer sa sécurité informatique ». La première des précautions est élémentaire : ne pas laisser traîner ses codes sur un post-it collé sur un coin du bureau…



Jean-Yves Marion, directeur du Loria. Photo ER/Philippe RIVET

Philippe RIVET