L'introduction d'un virus dans un système informatique est souvent de type rançongiciel, monnayant les données contre de l'argent. Rawpixel Ltd

Cyberattaques : « On est tous une cible potentielle »

Depuis plusieurs mois, des entreprises, des collectivités mais aussi des particuliers ont été la cible d'actions malveillantes de hackers sur l'île. Les professionnels de la cybersécurité alertent sur le phénomène et les pouvoirs publics s'organisent

JEANNE-F. COLONNA
jcolonna@corsematin.com

Spontanément, les interlocuteurs évacuent les termes techniques pour décrire l'intrusion d'un virus dans un ordinateur. Il est davantage question d'un « *méchant* » qui a vu « *que la porte d'entrée était ouverte et qui s'est introduit chez vous* ».

Depuis 2019, au moins cinq cyberattaques ont touché des institutions et des entreprises corses. La première victime fut l'Université de Corse. Puis, en 2022, la compagnie maritime Corsica Linea, l'office d'équipement hydraulique de la Corse et l'hôpital de Castelluccio à Aiacciu ont également été la cible d'un virus, souvent de type rançongiciel, monnayant donc les données contre de l'argent. La semaine dernière, c'est la compagnie maritime Corsica Ferries qui a été la cible de hackers pro-russes. Toutes ces victimes ont déposé plainte.

Porter plainte pour affiner la connaissance

Une démarche nécessaire pour lutter efficacement, et à grande échelle, contre les cyberattaques. « *Les entreprises ou institutions victimes d'une cyberattaque ne souhaitent pas toujours en parler à cause d'un enjeu réputationnel. Mais cela ne tient pas. D'une part car l'absence de communication peut tout autant nuire à l'image et d'autre part car les plaintes nous permettent de collecter des informations, que nous pouvons recouper au niveau national. Le parquet parisien spécialisé dans ce domaine et la sous-direction de lutte contre la cybercriminalité peuvent ainsi avoir une vision d'ensemble sur les menaces* », indique la commissaire de police, chef des divisions opérationnelles à la police judiciaire d'Ajaccio, en charge du sujet.

La semaine dernière ce message s'est affiché sur les écrans de la Corsica Ferries au moment de la cyberattaque dr

« *Porter plainte équivaut à travailler pour le collectif, cela nous permet d'affiner nos connaissances sur les méthodes des cybercriminels, que l'on peut retrouver dans d'autres dossiers* », insiste le commandant de l'antenne de lutte contre les criminalités numériques (C3N) de la Section de recherches de la gendarmerie de Marseille.

Cependant, certaines attaques ne font l'objet d'aucun signalement, d'aucune plainte. Cette situation impacte les chiffres s'agissant du nombre réel de victimes tant sur le territoire insulaire que national.

« *Il y a plusieurs raisons qui poussent les victimes à ne pas déposer plainte. C'est difficile d'avouer que quelqu'un s'est introduit chez nous car on a laissé la porte ouverte* », indique un professionnel du secteur.

« Il ne faut en aucun cas payer la rançon. Cela ne règle généralement pas les choses et ce paiement ne garantit pas la récupération des données »

Alors, quand les victimes trouvent d'elles-mêmes une issue positive à une attaque, elles sont encore moins tentées de se tourner vers les autorités, qui les invitent à le faire malgré tout. Paradoxe, la solution à leur problème peut même se cacher sur le darknet - un réseau internet parallèle et moins restrictif, terrain de jeu des hackeurs.

Tous les professionnels consultés insistent sur un point : « *Il ne faut en aucun cas payer la rançon car cela ne règle généralement pas les choses et ce paiement ne garantit pas la récupération des données* ».

En France, 72 % des attaques passent par un mail frauduleux selon les chiffres de l'agence nationale de la sécurité des systèmes d'information. « *Quand on a plusieurs centaines d'employés qui ouvrent des mails toute la journée, cela demande un véritable travail pédagogique pour expliquer aux gens qu'il faut faire attention à ce que l'on ouvre* », note un chef d'entreprise insulaire, lui-même victime d'une cyberattaque.

Le centre de réponse aux incidents cyber (Csirt) qui ouvrira en janvier - piloté par la Collectivité de Corse - a pour vocation de prodiguer les premiers secours. « *Notre objectif,* explique Christophe Appietto qui dirigera le Csirt, *est tout d'abord de contenir l'incident. Nous sommes là pour ça* ». En quelque sorte pour limiter la casse. « *Nous faisons alors appel à des entreprises labélisées, il en existe en Corse avec lesquelles nous allons travailler pour procéder aux remédiations, c'est-à-dire remettre en place l'activité de l'entreprise, rapidement. Ensuite, il y a un travail de coordination avec toutes les entités* », détaille Christophe Appietto. Et notamment avec les autorités. « *Nous sommes complémentaires* », assure la commissaire de police d'Ajaccio. Elle insiste enfin sur une prise de conscience collective : « *Tout le monde doit se sentir concerné, car on tous une cible potentielle. Le travail de prévention est capital tant sur les ressources humaines que sur les aspects techniques* ». Christophe Appietto le confirme : « *100 % des systèmes sont testés quotidiennement pour voir s'il y a une faille* ». Le Csirt a aussi pour objectif de collecter des données afin d'avoir une vision plus affinée du risque sur le territoire insulaire.

Les failles

Parmi les principaux vecteurs d'attaques informatiques, l'e-mail est le plus largement utilisé et représente 72 % des cyberattaques constatées par les entreprises en 2022. De ce fait, de nombreux hackers se servent de l'e-mail pour obtenir des données ou véhiculer des logiciels malveillants en utilisant des techniques comme l'usurpation d'identité ou encore l'envoi de pièces jointes vérolées. Les hackers profitent aussi de l'exploitation d'applications et de navigations web, de systèmes informatiques ou encore des connexions à distance. Les données mobiles peuvent également être une porte d'entrée. **Pour se prémunir d'une attaque,** il est conseillé de réaliser régulièrement des mises à jour sur les systèmes, d'installer des pare-feu et des antivirus et de se méfier des pièces jointes se terminant par « *.scr, .cab ou .exe* ».

J.-F. C.

La Capa vote un plan de cybersécurité

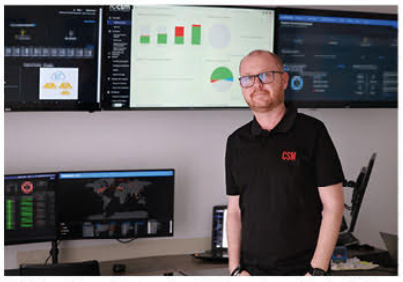
Les chiffres sont édifiants. Selon Christophe Mondoloni, élu de la communauté d'agglomération du pays ajaccien (Capa), délégué au numérique, 74 % des très petites et petites et moyennes entreprises (TPE et PME) ont déjà été victimes d'une cyberattaque, « *plus au moins importante* ». Parallèlement, 83 % des entreprises, « *se sentent peu ou pas exposées aux risques Cyber* ». « *Un paradoxe* », selon l'élu qui témoigne « *du risque encouru* ». Pour lutter, ou plutôt se prémunir contre ces attaques, souvent aléatoires, la Capa déploie un plan d'action qui a été voté jeudi soir lors du conseil communautaire. « *L'objectif est d'informer, de sensibiliser et d'accompagner les TPE et les PME qui sont les acteurs économiques les plus directement touchés en cas d'une cyberattaque. Cette action entend cibler, aussi, le secteur du commerce et de l'artisanat qui n'est pas épargné par ce phénomène et qui représente une part importante des entreprises qui déposent le bilan après avoir subi une telle crise* », développe Christophe Mondoloni. Plusieurs partenaires, comme l'Adec, le Csirt ou encore la gendarmerie nationale vont participer au déploiement de ce plan. « *Ce dernier a pour objectif d'apporter des conseils adaptés, de fédérer tous les acteurs dans le domaine de la cybersécurité, ce qui représente un avantage pour les entreprises. Et surtout, dans ce cadre, nous allons organiser des visites sur site dans les entreprises pour mieux expliquer les risques aux dirigeants et leur proposer une expertise si nécessaire* », insiste Christophe Mondoloni.

J.-F. C.

« 60 % des entreprises déposent le bilan dans les deux ans suivant une attaque »

Consultant en sécurité informatique, à Bastia, Boris Brunel est un spécialiste de la cybersécurité. Le cabinet qu'il a fondé, CSM, est labellisé expert cyber par cybermalveillance.gouv.fr, le dispositif national d'assistance aux victimes d'attaques informatiques.

L'agence nationale de la sécurité des systèmes d'information (ANSSI) estime que le nombre de cyberattaques a été multiplié par quatre entre 2021 et 2022. Quelle ampleur ce phénomène a-t-il en Corse ?
Nous ne disposons pas de données par région. Nous sommes néanmoins souvent sollicités pour des attaques, des piratages de sites web ou le signalement de pièces malveillantes. Nous avons parfois tendance, ici, à nous sentir à l'écart de certains phénomènes mondiaux. Mais ce genre d'attaque ne connaît pas de frontières. Dès lors que vous disposez d'un ordinateur et d'une connexion Internet avec une adresse IP sur le réseau, vous êtes potentiellement concerné. En Corse comme ailleurs.


Boris Brunel, consultant en sécurité informatique, à Bastia. CHRISTIAN BUFFA

Quel impact ce type d'attaque peut-il avoir sur les entreprises ?
Les statistiques sont terribles : 60 % des TPE et PME déposent le bilan dans les 18-24 mois suivant un grave incident informatique. Ces attaques se traduisent souvent par des difficultés juridiques en raison de fuites de données personnelles de clients, des atteintes à l'image ou tout simplement un arrêt total de la production. Souvent, elles ne peuvent plus travailler. Parfois durant plusieurs jours ou semaines. Dans nombre d'entreprises, la dépendance à l'informatique est de l'ordre de 100 %.

Que leur conseillez-vous ?
D'abord de s'y intéresser, en comprenant que cela n'arrive pas qu'aux autres, et en appliquant les règles d'hygiène informatique édictées par les agences gouvernementales comme l'ANSSI. J'ajoute qu'il ne faut jamais payer les rançons réclamées par les hackers. Rien ne garantit qu'ils vous donneront la clé de déchiffrement permettant de débloquer votre système informatique, que vos données seront intactes et qu'elles ne seront pas exploitées de façon malveillante. Les hackers sont des criminels qui font du business et appartiennent à des réseaux plus vastes, parfois mafieux, ayant des activités comme le trafic de drogue. En payant, vous participez au financement de ces activités.

Votre cabinet a développé un logiciel pour durcir les systèmes d'information d'entreprises ou organismes. Mais peuvent-ils se prémunir eux-mêmes de ces actes malveillants ?
C'est possible, mais cela reste compliqué. Les entreprises peuvent-elles entretenir leurs véhicules de société, faire le ménage de leurs bureaux ou leur comptabilité ? Oui, jusqu'à un certain point. Toutes ces tâches sont souvent sous-traitées car elles nécessitent un savoir-faire. C'est pareil pour la cybersécurité : cela nécessite souvent d'avoir recours à des experts qui soient capables de tout faire, en amont, pour éviter les vulnérabilités propices à ces attaques.

JULIAN MATTEI
jumattei@corsematin.com

Comment reconnaître et parer une attaque ?

RECYM
RÉSEAU DES EXPERTS CYBER-MENACES DE LA DIRECTION NATIONALE DE LA POLICE JUDICIAIRE

Police et gendarmerie ont des services spécialisés dans ce domaine. DTPJ

Les professionnels font le distinguo entre une cyberattaque et une cyberarnaque. Les escroqueries représentent la part la plus importante des phénomènes criminels, avec 80 % des procédures judiciaires ouvertes en zone gendarmerie en 2022. Il s'agit principalement de fraudes bancaires ou d'escroquerie aux faux investissements.

S'agissant d'une attaque informatique, les enquêteurs listent des signes qui permettent de comprendre qu'un système est compromis : « *Impossibilité à se connecter à la machine, fichiers disparus, modifications du coffre-fort de mots de passe, connexions ou activités inhabituelles, ralentissement du système…* ». Les autorités conseillent de déconnecter la machine tout en la maintenant sous tension puis de réinstaller le système d'exploitation à partir d'une version saine.

Elles ajoutent : « *Alerter au plus tôt c'est préserver les preuves numériques* ».

Dans un temps court, les professionnels amenés à intervenir sur une cyberattaque peuvent en stopper l'évolution et récupérer des données. Si un paiement a été effectué, dans le cadre d'une demande de rançon, il peut être interrompu avant de disparaître à l'étranger.

Pour la gendarmerie, il existe une structure de prévention, de contact et de première assistance en ligne via le site internet magendarmerie.fr ou les réseaux sociaux. Au sein de la police judiciaire de Corse, deux adresses mail distinctes sont à disposition de la population. Une première axée sur la prévention et la sensibilisation - cybermenaces-corse@interieur.gouv.fr - et une seconde en cas d'attaque - lion-drpj2a@interieur.gouv.fr - ainsi qu'un numéro de téléphone : 04 95 11 16 10. Le Csirt Corse prendra pour sa part ses fonctions en janvier (lire page 2).

J.-F. C.