Conférence

CYBERATTAQUES: PERSONNE N'EST ÉPARGNÉ

Moment marquant, déstabilisant et de plus en plus fréquent en entreprise, notamment dans l'immobilier, le hackage des données fait peur. Voici quelques retours d'expériences et conseils afin d'éviter le pire.

Grandes sociétés comme petites PME sont soumises à cette menace d'un nouveau genre.

Pete Linforth Pixabay

Il vous reste 23 heures, 45 minutes et 12 secondes. Le message est clair, sobre, efficace... Pourtant, dans la tête de celui qui le lit, panique, peur et perte de contrôle sont souvent de mise. Et pour cause, lorsqu'un criminel sous couvert d'anonymat détient vos données et accepte de vous les rendre contre un montant à plusieurs zéros, la terre s'arrête de tourner. Du moins, pendant 23 heures, 45 minutes et 12 secondes.

E-mails, le fameux clic de trop

A l'image du groupe DBS (régies Domicim, Brolliet, etc.), lui aussi victime l'an dernier d'une cyberattaque de grande ampleur. Son directeur général, Christophe Hubschmidt, est revenu sur cet épisode mémorable lors d'une conférence organisée conjointement par l'Institut d'études immobilières et RICS, le leader du conseil en immobilier d'entreprise. Un témoignage qui prouve que peu importe la taille (ici 800 employés) ou les moyens d'une société, personne n'est épargné et surtout nul n'est réellement préparé à ce type de crise.

L'attaque qui a permis aux criminels de s'introduire dans le système est simple: un e-mail au nom d'une fiduciaire de confiance, un clic, et c'est fini. Le cryptage des données peut ensuite se dérouler sans encombre durant la nuit. Au petit matin, un collaborateur tente de se connecter au bureau. N'y parvenant pas, il cherche à joindre le service informatique qui se met à enquêter. Puis, tout s'accélère. «Vers 7h30, nous avons compris que nos systèmes de fichiers étaient cryptés et que tout était en train de tomber. Même nos backups externes étaient touchés», se remémore Christophe Hubschmidt. Une course contre la montre commence alors.

Le groupe de régies DBS et la société d'ingénierie Ingeni ont témoigné de leur expérience de cyberattaque fin novembre. DR

En jeu: des baux à loyers, des bulletins de versements avec coordonnées bancaires ou encore des devis et correspondances. Mais pour le groupe DBS, il n'est pas question de payer une rançon. «Nous avons décidé de couper les connexions réseau mais de ne pas éteindre les machines, car sinon nous allions perdre les traces du logiciel malveillant, mais aussi d'interrompre les liaisons bancaires et de mettre en place une cellule de crise», décrit son CEO. En résumé, casser pour mieux reconstruire. S'ensuivent alors des problèmes de communication interne et externe. «Sans intranet, il fallait prendre contact avec chaque collaborateur pour le prévenir de ne pas se rendre au travail, avertir les clients et surtout contenir les porte-paroles», poursuit le dirigeant.

Plusieurs jours de gymnastique informatique et logistique qui se termineront finalement bien pour ce groupe aux reins solides. Un grand nettoyage des appareils, quelques clients perdus et remise en route des systèmes plus tard, DBS peut enfin se remettre au travail. «Nous avons essuyé des pertes mais cet épisode aura tout de même servi de révélateur de talents, d'accélérateur de mises à jour de nos logiciels et surtout d'expérience, car nous savons que cela va se reproduire. Nous avons beau informer et tester tout le monde, devant le fait accompli, c'est plus fort que nous, on clique», conclut Christophe Hubschmidt.

Les cas de ransomware (demande de rançon) faisant suite à un vol des données sont de plus en plus nombreux. Unsplash

Les PME, tout autant à risque

Un peu plus tôt, l'an passé, un autre événement du même type n'a pas autant marqué la presse mais aura gravé à vie les esprits des 100 collaborateurs d'Ingeni, société d'ingénierie genevoise. «Comme l'anniversaire de mes enfants, je n'oublierai jamais cette date», témoigne Jérôme Pochat, un de ses ingénieurs civils. Ce 16 août 2021, Jérôme revient de vacances et se prépare comme chaque matin à aller au bureau. A la seule différence que son téléphone se met à sonner. Une fois, puis deux, puis trois. Il décroche enfin. L'heure est grave: leur prestataire informatique s'est fait hacker. «Que fait-on lorsqu'il vous reste 0,00 données, que tout est crypté, vos backups détruits et que vous avez 30 grues à alimenter au quotidien avec des promoteurs immobiliers peu enclins aux retards?», lance-t-il à l'assemblée.

La réponse est sans équivoque puisque vous vous asseyez sur le trottoir avec vos collègues et vous vous dites que vous êtes morts. «C'est déconcertant de voir à quel point, du jour au lendemain, vous perdez votre outil de production, 100 personnes se retrouvent potentiellement au chômage et de l'autre côté, c'est juste un business. Si vous ne versez pas l'argent, le hackeur ira voir ailleurs, la PME du voisin», relate l'ingénieur. L'équipe comprend alors rapidement qu'il faudra payer, coûte que coûte. Ils se rendent également compte qu'ils n'étaient pas prêts à vivre ce genre d'expérience aux faux airs de série Netflix, mais la société non plus. Il y a d'abord un premier réflexe, celui de porter plainte au poste de police en espérant trouver de l'aide. Trois heures d'attente plus tard, pas de solution à l'horizon et l'on vous conseille de ne pas payer, c'est illégal. Les minutes passent, vient le moment de créer un compte en bitcoins car les cybercriminels n'acceptent pas le cash. C'est évident, moins dans la pratique.

Toujours dans l'urgence, il faut ensuite transférer de l'argent sur ce nouveau compte, un montant colossal qui demande l'approbation du banquier. Autrement dit: expliquer la nécessité de verser une somme conséquente de son compte bancaire vers un compte en monnaie numérique, nouvellement créé, afin de payer une rançon. Ce à quoi le banquier répond gentiment: «Nous allons examiner votre requête à notre siège, à Zurich, nous vous rappelons la semaine prochaine». Bien entendu, le chronomètre n'attend pas. Il vous reste 18 heures, 24 minutes et 3 secondes. Le prestataire informatique hacké ayant touché d'autres victimes, Ingeni s'allie au consortium pour rassembler le million de francs exigé. Aussitôt dit, aussitôt fait. Le problème est réglé, enfin en partie. «Que fait-on après? Non seulement, les entreprises se retrouvent démunies face à ces menaces, un univers qu'elles ne connaissent pas, mais elles n'ont aucune solution à disposition et surtout aucune information. Comment inscrit-on une transaction illégale dans une déclaration fiscale par exemple?», pointe Jérôme Pochat.

> *«Que fait-on lorsqu'il vous reste 0,00 données, que tout est crypté, vos backups détruits et que vous avez 30 grues à alimenter au quotidien?»*
>
> **Jérôme Pochat, ingénieur chez Ingeni**

Se préparer, pour ne pas sombrer

Heureusement, Ingeni a survécu, mais ce n'est pas le cas de tout le monde. L'ingénieur avertit: «Si cela vous arrive, tous les mécanismes joueront contre vous alors que le temps file. Il faut essayer au maximum de prévenir ces événements au sein de son entreprise. Jusqu'à ce jour, nous pensions faire juste et ne pas être la cible de ces attaques mais ça arrive et à présent, on ne se demande même pas si cela se reproduira, mais plutôt quand?».

Steven Meyer, fondateur de Zendata et spécialiste en cybersécurité, a ainsi distillé quelques bonnes pratiques pour se prémunir de ces menaces d'un nouveau genre, bien que le risque zéro n'existe pas. «L'an dernier, nous sommes intervenus dans la région sur pas moins de 70 attaques ransomware (rançongiciel). On parle de montants d'un million pour des PME à plusieurs dizaines de millions de francs pour les grosses structures», souligne l'expert. Face à ces dangers, comme toujours, on peut soit les éviter (ne plus avoir d'ordinateur), les transférer (contracter une assurance pour les aspects financiers, mais pas pour la confiance des clients et les données perdues), ou enfin les mitiger. Pour ce dernier point, voici quelques mesures à appliquer dans son entreprise selon le maître en la matière:

- Avoir des mots de passe solides, voire installer du multi-facteurs ou un gestionnaire de mots de passe.
- Effectuer les mises à jour de son appareil, sinon cela facilite l'entré du hackeur en quelques clics.
- Configurer correctement ses outils, on n'oublie pas l'antivirus, le firewall etc.
- Former les employés, car l'utilisateur a un grand rôle dans la probabilité de se faire hacker.
- Définir des procédures claires, rien ne s'improvise, notamment pour les paiements.
- Savoir quelles données protéger à tout prix, il faut connaître son seuil de tolérance face à ce risque grandissant.
- Valider si ce que vous faites fonctionne, on peut tester ses employés, imposer un processus depuis le haut, etc.
- Avoir un champion, en interne ou en externe, quelqu'un qui s'y connait en cybersécurité.

Julie Müller