L'AGEFI HEBDO
Pays : FR
Périodicité : Hebdomadaire

Date : Du 09 au 15 avril 2020
Page de l'article : p.12-13
Journaliste : ALEXANDRA OUBRIER

RETAIL & SERVICES

Les banques sont plus exposées aux cyber-risques en période de crise

La généralisation du télétravail dans les banques comme chez leurs clients impose une vigilance accrue face aux cyberattaques.

PAR **ALEXANDRA OUBRIER**
@AlexOubrier
+ EMAIL *aoubrier@agefi.fr*

L'heure est à la cybervigilance. La plupart des banques ont contacté leurs clients pour leur rappeler les bonnes pratiques de sécurité lors de leurs connexions à la banque en ligne ou de leurs opérations sensibles. Mais la crise actuelle ouvre un nouveau champ de vulnérabilité car avec le confinement, ces établissements ont dû faire basculer la quasi-totalité de leurs collaborateurs en télétravail. « *Le passage au télétravail dans des délais très courts a mis les systèmes d'information sous tension*, explique Jean-Philippe Bernard, associé chez RSM. *Les VPN ('virtual private networks'*, communications cryptées) *et les applications sont très sollicitées. De plus, les collaborateurs travaillent sur leur propre réseau wifi et parfois sur leur propre matériel, qui sont généralement moins sécurisés.* » Travailler sur des ordinateurs non sécurisés comporte le risque qu'un *malware* puisse être transmis au système central, malgré l'usage d'un VPN. « *C'est pourquoi certaines banques ont préféré envoyer par coursier à leurs employés des ordinateurs configurés et sécurisés, prêts à l'usage, quitte à ce que le déploiement des machines prenne quelques jours durant lesquels les personnes ne peuvent pas travailler* », indique Lionel Vincke, président d'Azzana Consulting.

Malgré ces précautions, les collaborateurs peuvent être tentés d'utiliser une messagerie instantanée gratuite qui contourne les mesures de sécurité de la banque pour aller plus vite. Des données confidentielles peuvent alors être exposées. Pour Eric Barbry et David Masson, avocats chez Racine, « *il y a deux bêtises majeures : l'extraction de données sensibles des applications métier téléchargées sur le disque dur, souvent pour pouvoir travailler plus rapidement, et les documents imprimés jetés à la poubelle recyclable* », là où n'importe qui peut les récupérer.

SÉCURISER SANS RELÂCHE

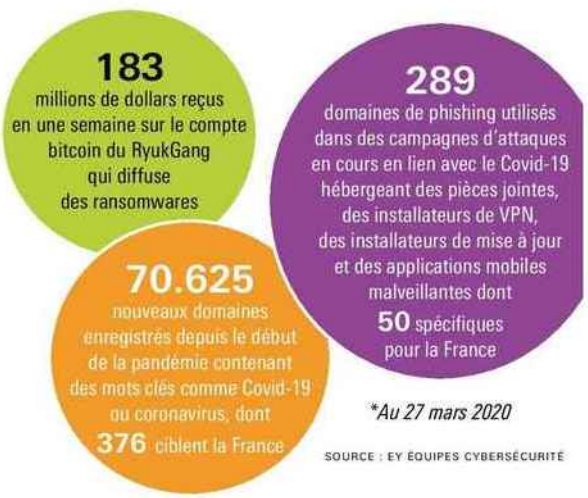
Autre risque : les attaques de *phishing* se sont multipliées, utilisant des mots clés qui suscitent la curiosité comme Covid-19, coronavirus, masques à vendre… Des collaborateurs peuvent cliquer machinalement et se retrouver sur des sites qui volent leurs données. Pour Bertrand Trastour, *head of B2B sales*, et Pierre Delcher, chercheur en sécurité chez Kaspersky, « *ce sont les mêmes attaques que d'habitude, la parade reste l'authentification avec des mots de passe robustes ou multifacteurs, la sensibilisation des collaborateurs aux règles de sécurité de l'entreprise et la communication de sources fiables auprès desquelles ils peuvent se renseigner.* »

D'ailleurs, les banques ont conscience qu'elles sont davantage exposées, plusieurs ont fait appel à leurs fournisseurs spécialisés pour renforcer leur niveau de sécurité. « *Dès le début de la crise, tous nos clients ont appelé pour étendre les solutions d'authentification multifacteur et de surveillance des réseaux* », révèle Bernard Montel, *EMEA CTO field* pour RSA Security qui commercialise différentes offres de cybersécurité, dont certaines spécifiques pour les institutions financières, et un service d'alerte et de suppression des sites malicieux où les pirates attirent les internautes. *Désormais, en phase 2, RSA accompagne les SOC ('security operation centers') des entreprises dans la détection des attaques de 'phishing' et la gestion des risques liés.* »

En phase 3, lorsque les collaborateurs réintégreront leur poste de travail, d'autres vérifications seront nécessaires. Mais en attendant, Marc Ayadi, associé et *cybersecurity leader* chez EY, recommande aux équipes de sécurité « *de passer en revue leurs infrastructures d'accès à distance, de sécuriser au plus vite les applications sur lesquelles des vulnérabilités ont été publiées mais non traitées, et de vérifier la protection des systèmes vitaux. Il est temps également d'ajuster les capacités de réaction en*

cas d'incident, car ces équipes ont un rôle majeur à jouer lors des attaques dans la détection, le diagnostic, la préservation de la scène de crime et l'investigation. Ce sont elles qui établiront les dommages commis et le mode d'action de pirates, ce qui servira à la protection future de système d'information ». A

LA VAGUE DE CYBERATTAQUES*



*Au 27 mars 2020

SOURCE : EY ÉQUIPES CYBERSÉCURITÉ