DOCUMENT D'INFORMATION

# Secteurs à risque courants dans l'industrie des services financiers

## LE SAVIEZ-VOUS?

**En 2017, une brèche de données moyenne touchait plus de 24 000 dossiers.** [1]

Avec autant de documents exposés à des risques, les fournisseurs de services financiers de toute l'Amérique du Nord doivent être conscients de leurs secteurs vulnérables.

### Les attaques par déni de service :

Les attaques par déni de service, incluant les attaques par déni de service distribué et les attaques par déni de service organisées à l'aide de réseaux de zombies (botnet), sont les escroqueries les plus communes touchant l'industrie des services financiers.[2] Les cybercriminels submergent de requêtes un réseau ou des machines ou envoient des informations visant à faire planter le système et privent ainsi les utilisateurs, comme les titulaires de comptes, de services.

### La numérisation :

Les banques et les fournisseurs de services financiers communiquent de plus en plus avec leurs clients par l'entremise de sites Web ou de leurs téléphones cellulaires ou appareils connectés à l'internet des objets. Toutefois, certains dispositifs en réseau ne sont pas toujours sécurisés.

### Les escroqueries par hameçonnage :

L'envoi d'un courriel frauduleux qui semble provenir d'un dirigeant de l'entreprise (Business Email Compromise scam) est l'une des arnaques les plus courantes utilisées pour tromper une victime afin d'obtenir de l'argent et des données financières confidentielles. Un fraudeur accède à un compte de messagerie d'affaires, puis usurpe l'identité du propriétaire pour frauder l'entreprise.

### Les cybercriminels :

La principale menace externe qui pèse sur l'industrie des services financiers est constituée des cybercriminels (40 %). Viennent ensuite les États nations (18 %), les cyberactivistes (16 %) et les entreprises concurrentes (13 %).[6]

### Les maliciels financiers :

Avec plus de 1,2 million de détections annuellement, les maliciels financiers représentent une énorme menace et sont 2,5 fois plus communs que les logiciels rançonneurs. (4) Dans une récente étude, on apprend que 75 % des 20 principales banques commerciales des É.-U. ont été contaminées par un malicie.[5]

### L'équipement obsolète :

Les cabinets de services financiers intègrent constamment de nouvelles technologies ou de nouveaux systèmes ou logiciels à leurs opérations, et leurs systèmes informatiques existants proviennent souvent d'organisations acquises par le passé. Mais les anciens équipements – et le fait de les accumuler – peuvent rendre l'organisation vulnérable aux attaques.

### Les initiés :

Un récent rapport révèle que 60 % des répondants de l'industrie financière mondiale ont indiqué que les utilisateurs privilégiés sont la menace interne la plus importante, suivis par le personnel de direction (48 %) et les travailleurs contractuels (38 %).[6] Les transferts frauduleux d'argent et l'utilisation des renseignements personnels d'un client pour voler son identité sont des exemples d'abus de privilège.

### La négligence des employés :

De nombreuses recherches indiquent que les employés négligents qui ne respectent pas les politiques en matière de sécurité représentent la plus grande menace liée à la sécurité au sein des organisations.[7] En divulguant leurs mots de passe, en emportant inutilement des renseignements confidentiels et en laissant des appareils mobiles sans surveillance hors des lieux de travail, ils rendent leur organisation vulnérable aux attaques.

### Les partenaires tiers :

Beaucoup de fournisseurs de services financiers font appel à de multiples vendeurs, partenaires et autres tierces parties. Des études révèlent qu'environ 60 % des chefs de la sécurité de l'information ont une certaine inquiétude quant aux pratiques en matière de sécurité des tierces parties et aux risques d'une brèche de données.[3]


# 3 conseils pour protéger votre entreprise

### Repérez tous les secteurs de risque potentiels.

Effectuez une inspection de vos bureaux. Signalez tous les risques que vous voyez et prenez des me-sures pour les atténuer. Cette inspection vous permettra de découvrir les points faibles de votre entre-prise et de renforcer votre stratégie en matière de sécurité de l'information afin de protéger vos données.

### Mettez en place des politiques sur la sécurité des lieux de travail.

En établissant des politiques exhaustives, comme une politique de tout déchiquetage et une politique de bureau rangé, vous incitez vos employés à réfléchir avant d'agir lorsqu'ils sont au travail. Ils seront ainsi poussés à se conformer aux règles et à protéger vos données.

### Créez une culture de sécurité totale.

En adoptant une approche descendante et en intégrant la sécurité de l'information dans l'ensemble de votre entreprise, vous ferez en sorte que la culture de sécurité totale fasse partie intégrante du quotidien de vos employés. Par le fait même, ceux-ci seront amenés à considérer d'un œil neuf la destruction sé-curitaire des renseignements confidentiels.

**Sources:**
1. 2017 Cost of Data Breach Study, Ponemon Institute, 2017
2. 2017 Data Breach Investigations Report, 10e édition, Verizon
3. What CISOs Worry About in 2018, Ponemon Institute et Opus, 2017
4. Internet Security Threat Report, Financial Threats Review 2017, Symantec
5. 2016 Financial Industry Cybersecurity, Security ScoreCard
6. 2017 Thales Data Threat Report, Financial Services Edition, Thales e-security
7. Promoting Data Security in the Workplace infographic, University of Alabama à Birmingham; 2016 State of the Endpoint Report, Ponemon

Apprenez-en davantage sur la sécurité de l'information dans l'industrie financière :

**1-877-227-5986 | shredit.com/finance**

Shred-it® est une solution Stericycle.



Shred-it®