7 leçons tirées des plus grandes violations des données de 2020

VOICI UN RÉCAPITULATIF

Récemment, nous avons recensé les violations de données les plus marquantes de 2020. Voici un récapitulatif :

- 300 000 utilisateurs ont été touchés par une campagne massive de détournement de comptes chez Nintendo.
- Plus de 500 000 comptes Zoom ont été piratés, puis offerts sur le dark web.
- Une brèche de sécurité chez Easyjet a exposé les données de 9 millions de clients, y compris certains documents financiers.

- Un ingénieur en sécurité a piraté son employeur, Cisco, ce qui a coûté 2,4 million de dollars à la compagnie pour se remettre sur pied. L'employé a écopé plus tard d'une peine de 2 ans de prison.
- Wattpad a subi une violation de données qui a exposé près de 271 millions de dossiers.
- Les comptes Twitter de certaines des personnalités les plus connues au monde ont été compromis par des pirates qui ont utilisé des attaques de harponnage pour diriger du trafic vers des fraudes Bitcoin.
- Le groupe de pirates ShinyHunters a divulgué la base de données appartenant à Mashable.com, exposant plus de 5,2 Go de données.
- Des pirates ont inséré du code malveillant dans une mise à jour du logiciel de SolarWinds, appelé Orion. Ce piratage s'appelle une attaque de la chaîne d'approvisionnement, parce qu'il infecte le logiciel lors de son assemblage. SolarWinds a déclaré qu'environ 18 000 clients ont installé la mise à jour contaminée sur leurs systèmes. Ces attaques doivent être prises au sérieux et sont très puissantes. Cette attaque a eu (et a toujours) un impact énorme, alors qu'on découvre encore de nouvelles informations au fil du temps.

L'assaut continue

Juste au cas où quelqu'un espérait que les pirates informatiques fassent une pause après une année 2020 très chargée… **Ça ne se passera pas comme ça malheureusement.** En fait, les attaques se poursuivent : début janvier 2021, la société de cybersécurité Safety Detectives a découvert une fuite au sein de l'entreprise en démarrage chinoise de médias sociaux Socialarks. Cette fuite impliquait 400 Go de données, exposant plus de 200 millions d'utilisateurs de Facebook, Instagram et LinkedIn. L'histoire se répète…

Leçons tirées

Voici sept leçons tirées des plus grandes violations de données de 2020 (question de défendre ses données, ses clients et sa réputation) :

1. La question n'est pas de savoir SI une PME sera attaquée, mais QUAND (ou combien de fois déjà).

Des recherches ont montré que 66 % des PME ont subi au moins une cyberattaque au cours des 12 derniers mois. En plus, de nombreuses PME ont été attaquées sans qu'elles s'en aperçoivent. **Tout ça signifie que les**

PME ne devraient pas se demander « si » elles seront attaquées, mais devraient plutôt se préparer à « quand » elles seront attaquées (ou attaquées à nouveau).

Les PME devraient donc disposer d'un plan de réponse aux incidents de cybersécurité (mieux connu sous le nom CSIRP pour cybersecurity incident response plan). Les PME devraient aussi se doter d'un plan de reprise après un incident. Sans ces plans, l'impact d'une cyberattaque pourrait être catastrophique. En 2020, le coût total moyen d'une violation de données dans les petites organisations était de 2,35 millions de dollars.

2. C'est essentiel de classer, surveiller et contrôler l'accès aux comptes privilégiés.

Bien que 80 % des incidents de piratage sont causés par des identifiants compromis, de nombreuses PME demeurent vulnérables par rapport à ça. Par exemple, un sondage de la société de cybersécurité Varonis a révélé que :

- **Seulement 5 % des documents sont correctement protégés.**
- **15 % des entreprises ont plus de 1 000 000 de documents ouverts pour chaque employé.**
- **17 % de tous les dossiers sensibles sont accessibles à tous les employés.**
- **60 % des entreprises ont plus de 500 comptes avec des mots de passe qui n'expirent jamais.**

Ces résultats sont conformes aux conclusions de l'**enquête de Devolutions sur le portrait de la cybersécurité dans les PME en 2020-2021.** Cette enquête a révélé que si 78 % des PME considèrent qu'une solution de gestion d'accès privilégiés est importante, 76 % d'entre elles n'en utilisent pas actuellement. Notre rapport contient des recommandations pratiques et stratégiques pour vous aider à régler ce problème (et ça devrait être votre priorité absolue pour 2021).

3. La gestion des vulnérabilités doit se faire de manière active et non passive.

Si corriger les vulnérabilités est essentiel, les PME ne doivent pas s'arrêter là. Elles doivent être proactives et détecter/traiter en continu toutes les menaces, y compris celles qui n'ont pas encore eu lieu. Dans le cadre de leur plan de gestion des vulnérabilités, **les PME doivent également analyser toutes les failles potentielles provenant des entités extérieures.** Plusieurs violations de données très médiatisées en 2020 (par exemple Blackbaud, Mailfire, Clearview AI, etc.) impliquaient des tiers.

4. Tous les employés doivent avoir une formation en cybersécurité.

L'une des choses les plus troublantes par rapport aux violations de données de 2020, c'est que beaucoup d'entre elles auraient pu être évitées avec une formation efficace en cybersécurité. En fait, des recherches ont montré que, dans les dernières années, près de la moitié (47 %) de toutes les violations de données sont dues à la négligence ou à l'imprudence des employés.

La mauvaise nouvelle, c'est que les utilisateurs finaux seront toujours le maillon le plus faible de la chaîne de défense en matière de cybersécurité. La bonne nouvelle, c'est que les PME peuvent (et doivent) offrir **à tous leurs employés** une formation en cybersécurité. L'option la plus efficace et la plus abordable est d'inscrire leur personnel à une plateforme de formation en ligne.

5. Les menaces provenant de l'interne sont un problème croissant.

Une autre tendance inquiétante est le nombre d'attaques qui ont impliqué des utilisateurs malhonnêtes (par exemple Postbank, Cisco, etc.). Pourtant, malgré ça, l'enquête de Devolutions a révélé que **seulement 17 % des PME pensent que l'augmentation des menaces provenant de leurs employés sera une préoccupation majeure dans les trois prochaines années.**

Corriger cette vulnérabilité implique un **mélange de contrôles techniques et non techniques**. Dans le cas des contrôles techniques, on parle par exemple de gestion d'accès privilégiés et d'authentification à deux facteurs ou multifacteur. Pour les contrôles non techniques, il est question de vérification des antécédents et l'implantation de bonnes pratiques comme la séparation des tâches, le principe du moindre privilège et la confiance zéro (qui aide aussi avec le concept de Défense en profondeur).

6. Les PME doivent établir des partenariats avec des fournisseurs de services gérés

La plupart des PME n'ont pas de spécialistes en cybersécurité à l'interne pour établir, surveiller et optimiser toute la gamme de contrôles techniques et non techniques nécessaires pour déjouer les pirates. En plus, avec la pénurie d'employés spécialisés en cybersécurité, on ne s'attend pas à ce que cette expertise devienne plus abordable en 2021. Les PME doivent donc s'associer à un bon fournisseur qui leur donnera **accès aux experts, aux conseils et aux ressources dont elles ont besoin, mais à un prix qui correspond à leur budget.**

7. Les travailleurs à distance sont une cible privilégiée.

Les recherches menées par Malwarebytes ont montré que 20 % des entreprises ont subi une cyberattaque visant à des travailleurs à distance pendant la pandémie. L'objectif des pirates est de compromettre les terminaux, puis de se déplacer latéralement sur le réseau sans être détectés. **La montée en flèche du télétravail a provoqué de nouveaux maux de tête aux PME en lien avec l'utilisation de réseaux privés virtuels.** Notons les contraintes de bande passante, la perte de productivité des utilisateurs et la difficulté à configurer des systèmes requis sans expertise interne. De plus, les travailleurs à distance peuvent laisser tomber la garde en utilisant un ordinateur personnel et ainsi ouvrir la porte à une brèche dans le réseau de l'entreprise.

Pour se protéger contre les menaces, **les PME devraient sérieusement considérer l'implantation d'une architecture Confiance zéro.** En présumant que rien n'est digne de confiance et en authentifiant chaque opération et appareil, la stratégie Confiance zéro aide les PME à améliorer leur posture de sécurité, tout en augmentant l'efficacité et la productivité.

Le mot de la fin

Il a été dit que « ceux qui ne se souviennent pas du passé sont condamnés à la répéter ». À la lumière de cette citation, toutes les organisations **– mais surtout les PME, qui sont la cible préférée des pirates informatiques –** devraient tenir compte des leçons décrites ci-dessus, afin d'éviter les coûts et les conséquences d'une cyberattaque en 2021.