Rapport 2019 sur la sécurité des paiements

Gros plan sur le retail

verizon business ready

Jamais le retail n'a été un marché si âprement disputé. Pour s'y illustrer, les acteurs de la distribution doivent rester à l'écoute de leurs clients. Et la protection des données et de la vie privée fait plus que jamais partie des attentes des consommateurs.

Ainsi, seuls 7 % des clients se disent prêts à refaire confiance à une enseigne victime d'une compromission de données, tandis que 69 % passeraient leur chemin même si l'offre était plus attractive que celle de ses concurrents[1]. Face à de tels chiffres, on comprend mieux à quel point la sécurité des cartes de paiement représente un facteur clé de différenciation.

Maintenir des contrôles de sécurité efficaces pour se conformer au standard PCI DSS (Payment Card Industry Data Security Standard), c'est gagner la confiance de ses clients et prendre l'avantage sur ses concurrents. Mais pour y parvenir, les programmes de conformité et de protection des données (DPCP) doivent évoluer et gagner en maturité.

Pour les acteurs de ce marché, le rapport Verizon sur la sécurité des paiements (PSR) s'impose donc comme une lecture incontournable. L'édition 2019 ne déroge pas à la tradition en leur livrant des éclairages inestimables, à commencer par l'importance de nouveaux outils comme notre Cadre 9-5-4 d'évaluation des performances des programmes de conformité.

Même avec les codes PIN, les données sont exposées

Il y a quatre ans, les compromissions de données survenaient surtout au point de vente.[2] Depuis, la technologie Europay, Mastercard et Visa (EMV) a manifestement réduit le nombre de fraudes aux paiements sur présentation de la carte. Désormais, les compromissions de données se produisent principalement sur le web.[3] Toutefois, les retailers auraient tort de baisser la garde. La protection des données de carte doit rester un combat de tous les instants.

Le rapport PSR 2019 inclut des corrélations plus détaillées des investigations forensiques PCI (PFI) menées par l'équipe Verizon Threat Research Advisory Center (VTRAC) | Investigative Response entre 2016 et 2018. Conclusion : sur le long terme, les tendances montrent que le retail a subi la plus grande proportion de compromissions de données par rapport aux autres secteurs étudiés (hôtellerie, services financiers et services IT).

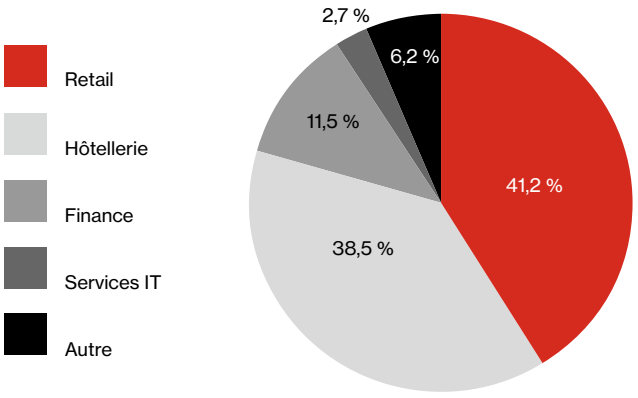

Figure 1 : Compromissions de données par secteur sur six ans, nombre d'investigations Verizon PFI à l'échelle mondiale, 2010-2016

D'après nos données, la plupart des compromissions concernent les boutiques en ligne. Selon le rapport d'enquête Verizon 2019 sur les compromissions de données, les attaquants s'en prennent aux données des retailers pour des raisons diverses : l'appât du gain bien sûr, mais aussi le cyberespionnage ou simplement le fun. Les données personnelles des programmes de fidélité n'y échappent malheureusement pas.

Sécurité des cartes de paiement : un enjeu vital, mais une conformité loin d'être totale

La bonne nouvelle, c'est que de axes d'amélioration existent. D'après les 55 entreprises interrogées pour le rapport PSR 2018, elles sont 18 %, tous secteurs confondus, à ne pas avoir défini un programme de conformité et de protection des données. Par ailleurs, aucune ne fait état d'un niveau de maturité optimal de son programme.

18 % des entreprises, tous secteurs confondus, n'ont pas défini de programme de conformité et de protection des données. Aucune ne fait état d'un niveau de maturité optimal de son programme.

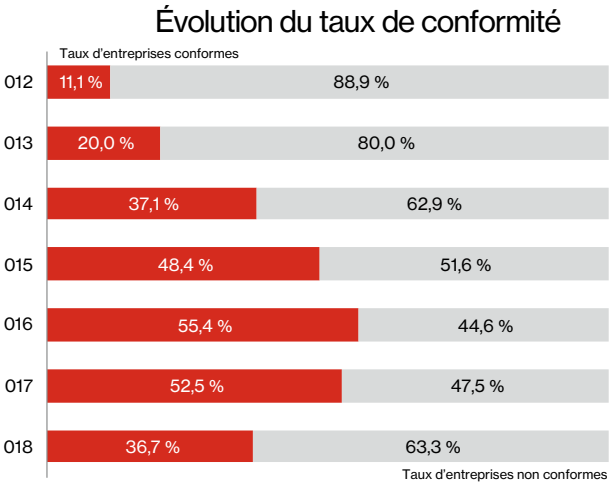

Figure 2 : Taux de conformité totale des entreprises par an

Depuis la première publication du PSR il y a neuf ans, nous avons constaté une hausse annuelle du taux de conformité PCI DSS dans tous les secteurs jusqu'en 2017. Toutefois, depuis deux ans, la tendance s'est inversée dans toutes les industries étudiées. Les données d'autres évaluateurs de sécurité qualifiés (QSA) viennent étayer ce constat.

Qu'est-ce que le standard PCI DSS ?

Les principales marques de cartes de paiement ont instauré le standard PCI DSS (Payment Card Industry Data Security Standard) pour aider les entreprises à réduire la fraude dans ce domaine. Si le standard vise à protéger les données de carte de paiement, il repose néanmoins sur des principes de sécurité éprouvés qui s'appliquent à tous les types de données. PCI DSS couvre des thèmes comme les politiques de conservation, le chiffrement, la sécurité physique, l'authentification et le contrôle des accès. Pour en savoir plus, rendez-vous sur pcisecuritystandards.org.

Bien que le PSR 2019 indique une chute du taux de conformité global, l'écart de conformité PCI DSS, qui mesure l'intervalle exact séparant une entreprise de la pleine conformité, est quant à lui resté stable par rapport à l'année dernière (7,2 %). Lorsque l'on se penche uniquement sur le cas des entreprises ayant échoué à leur audit intermédiaire, l'écart de conformité a heureusement perdu 6,2 points de pourcentage en un an, pour descendre à 10,2 % dans la dernière édition du rapport.

Sur le plan géographique, les entreprises de la région Asie-Pacifique (APAC) s'en sortent mieux que les autres puisque 69,6 % d'entre elles sont 100 % conformes au standard PCI DSS. La zone EMEA (Europe, Moyen-Orient et Afrique) affiche un taux de conformité totale de 48,4 %, tandis que moins d'un quart des entreprises de la zone Amériques (20,4 %) sont 100 % conformes.

Le mauvais cap du retail

D'après le rapport PSR 2019, tous les secteurs connaissent une véritable dégringolade de leur taux de conformité PCI DSS. Pour les enseignes de la distribution, ce taux chute à 36,4 % cette année, contre 56,3 % en 2018 et 50 % en 2017.

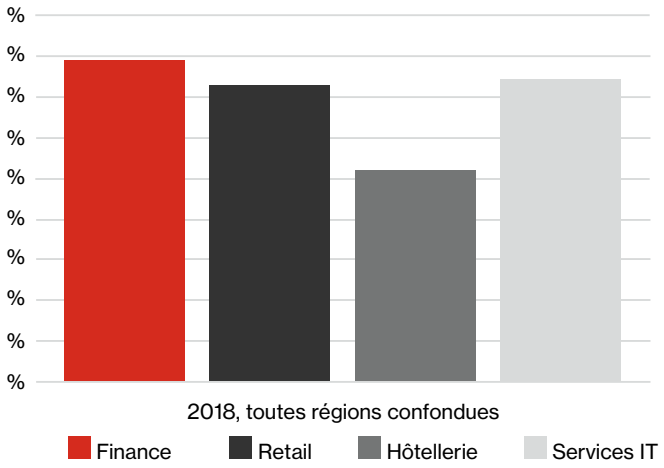

Figure 3 : Taux de conformité mondial par secteur

Cette année, les retailers devancent l'hôtellerie (26,3 % de taux de conformité) et sont à égalité avec les services IT. En revanche, ils font moins bien que les services financiers. ensemble, les quatre secteurs étudiés affichent un taux de conformité PCI DSS de 39 %.

Bons points

D'après le rapport PSR 2019, le retail s'est illustré dans les domaines du chiffrement des données en transit (condition 4 du standard PCI DSS) et de la protection antimalware (condition 5). Il a en effet surclassé les autres secteurs en réduisant ces deux écarts de conformité, ce qui le rapproche d'une conformité totale à ces deux conditions.

De même, les distributeurs s'en tirent plutôt bien dans le domaine de l'authentification des accès (condition 8) pour prévenir le vol de données. Dans ce domaine, ils ont en effet réduit leur écart de conformité et atteint un taux de conformité totale de 70,5 %, devançant au passage les services financiers et informatiques.

Enfin, le retail s'est illustré dans la traçabilité et la surveillance des accès aux données (condition 10). Des quatre secteurs étudiés, c'est lui qui obtient la plus haut taux de conformité sur ce terrain (81,8 %).

Mauvais points

Trop souvent, les acteurs du retail se sont mis à la faute en conservant de nombreux paramètres de sécurité par défaut sur des composants soumis à la condition 2 du standard PCI DSS. Dans ce domaine, son écart de conformité atteint pas moins de 12,4 %.

Dans le même temps, les distributeurs ont vu chuter le niveau de conformité de leur gestion de la sécurité (condition 12). L'écart de conformité s'est creusé de 18,2 points de pourcentage par rapport à l'année dernière, pour atteindre 56,8 %.

Faits intéressants

De tous les secteurs étudiés, les enseignes de la distribution sont les moins bien préparées à faire face à des incidents de sécurité. Les difficultés sont multiples :

- Identification des utilisateurs et adaptation des droits d'accès à leurs rôles respectifs (condition 10.2.5)
- Respect des contrôles de rigueur lors de la sélection de fournisseurs de services (condition 12.8.3)
- Détection des points d'accès sans fil non autorisés (condition 11.1.2)
- Maintien d'un plan de réponse à incident (IR) (condition 12.10)

Recommandations

Modifiez vos paramètres de sécurité par défaut.

Le remplacement des mots de passe par défaut et autres paramètres de sécurité d'usine est un premier pas vers plus de sécurité. Les enseignes doivent en faire une priorité. La bonne nouvelle, c'est que les équipes internes possèdent certainement les compétences nécessaires pour effectuer ces modifications.

Investissez dans votre préparation aux incidents.

Les incidents de cybersécurité sont inévitables. Ce qui compte vraiment, c'est la capacité d'une entreprise à y répondre. Ainsi, les retailers qui sauront identifier les incidents de sécurité potentiels, réagir rapidement et maintenir leur plan IR à jour pourront déclencher les investigations et limiter les dégâts. Pour en savoir plus sur les avantages et la mise en place de plans IR, consultez le rapport Verizon de préparation et de réponse à incident (VIPR).

Pourquoi se conformer aux conditions PCI DSS ?

Nous avons établi un recoupement entre les taux de conformité PCI DSS et les statistiques de compromission de données de carte de paiement depuis 2008. Résultat : parmi les entreprises conformes aux 12 conditions du standard PCI DSS, aucune n'a été victime d'une telle compromission.

Maturation de votre programme de conformité

La faiblesse de certains programmes de conformité n'a évidemment rien de volontaire. Le problème s'explique d'abord par la difficulté de la tâche. Toutefois, avec les bons outils, tout devient possible.

C'est dans cet esprit que nous avons conçu le Cadre Verizon 9-5-4 d'évaluation des performances des programmes de conformité. Fusion des éditions passées et de nouvelles recommandations, cette nouveauté du PSR 2019 offre une véritable boussole qui permettra aux entreprises d'améliorer leur programme de conformité PCI DSS. Le Cadre Verizon 9-5-4 renforce leur niveau de visibilité et de contrôle, avec à la clé des processus plus homogènes et reproductibles, des résultats plus prévisibles, une protection plus forte des données et une conformité assurée.

Figure 4 : Modèle relationnel des 9 facteurs d'efficacité et de pérennité des contrôles

Sécurité des paiements, une question d'image

Ce n'est pas parce que le taux de conformité PCI DSS est en forte baisse dans le retail que vous devez suivre la tendance. Malgré des performances d'ensemble en demi-teinte en 2019, nous avons également rencontré des enseignes très en pointe sur les questions de conformité PCI DSS. Inspirez-vous de leur exemple pour créer une marque qui rassure ses clients et fait de la sécurité des données un vecteur de compétitivité.

Plus d'infos

Pour définir vos priorités en matière de sécurité et améliorer votre programme de conformité, rendez-vous sur enterprise.verizon.com/resources/reports/payment-security/ ou contactez votre représentant Verizon.

verizon business ready

1 Données issues du rapport Verizon 2019 intitulé « Gagner la bataille de l'expérience client : risques et récompenses d'une expérience client de nouvelle génération », rédigé au terme d'une enquête en ligne menée auprès de 6 000 consommateurs de 15 pays et d'entretiens approfondis avec des experts de l'expérience client (CX) Étude menée par Longitude, une entreprise du Financial Times https://enterprise.verizon.com/resources/reports/2019/winning_the_cx_war.pdf

2 Rapport d'enquête Verizon 2019 sur les compromissions de données https://enterprise.verizon.com/resources/reports/dbir/

3 Ibid.