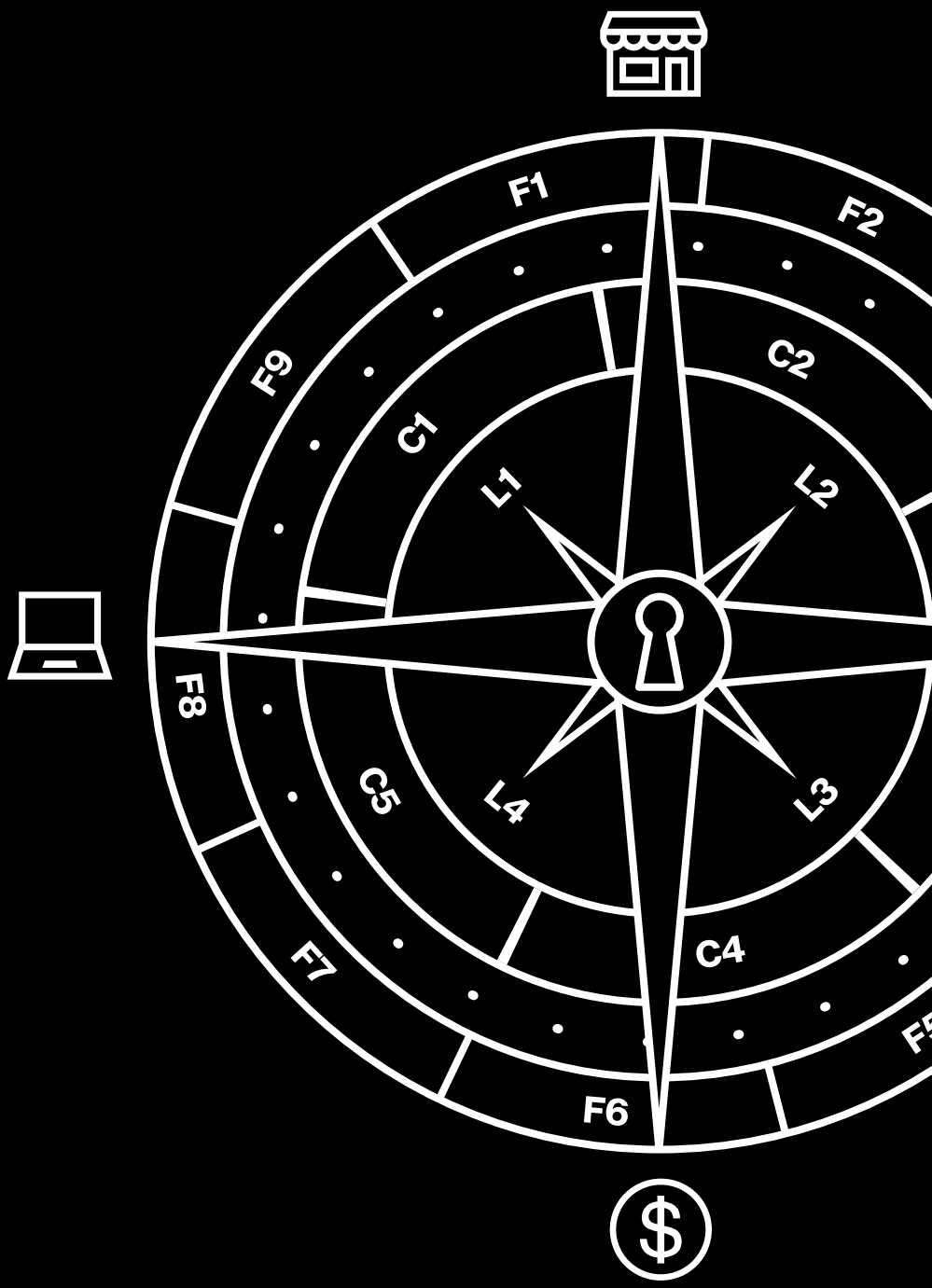
Rapport 2019 sur la sécurité des paiements

Gros plan sur l'hôtellerie



verizon business ready

Pour l'industrie de l'hôtellerie, l'amélioration de l'expérience client est un axe stratégique prioritaire. Pourtant, sur le plan de la cybersécurité, les choses laissent sérieusement à désirer. À tel point que les acteurs de ce secteur arrivent en dernière position du rapport Verizon 2019 sur la sécurité des paiements (PSR).

Nouveauté de cette année, le PSR inclut les corrélations détaillées des investigations sur les compromissions de données effectuées par l'équipe Verizon Threat Research Advisory Center (VTRAC) | Investigative Response. Ainsi, il apparaît que le taux de conformité PCI DSS (Payment Card Industry Data Security Standard) du secteur hôtelier est passé de 42,9 % en 2017 à 38,5 % l'année dernière, pour chuter à 26,3 % dans le rapport PSR 2019. Sur le long terme, les tendances montrent que les entreprises d'hébergement, les voyagistes et les services de réservation sont les plus compromis. Alors que les attaques de plusieurs grandes chaînes hôtelières sont encore dans tous les esprits, l'heure est venue de remettre à plat les pratiques de conformité et de protection des données des cartes de paiement.

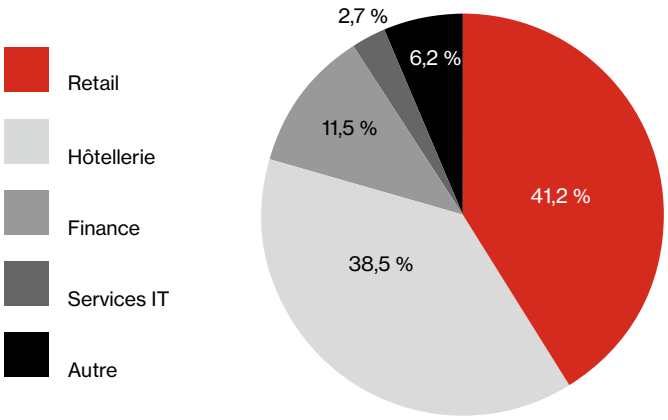
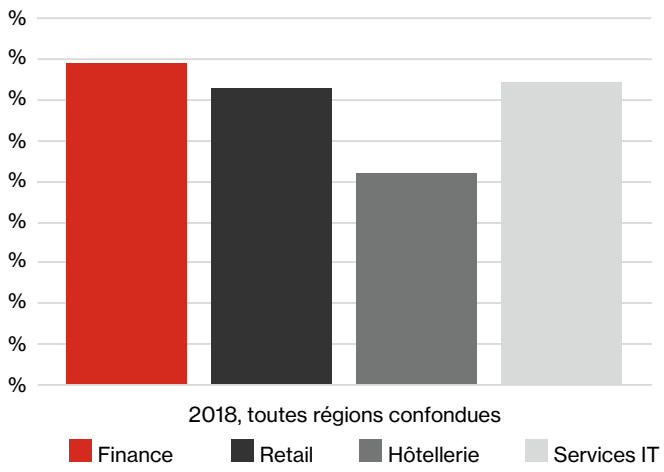


Figure 1 : Compromissions de données par secteur sur six ans, nombre d'investigations forensiques PCI menées par Verizon à l'échelle mondiale, 2010-2016

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

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. Les données d'autres évaluateurs de sécurité qualifiés (QSA) viennent étayer ce constat. Parmi tous les secteurs étudiés, l'hôtellerie enregistre la plus grosse chute.



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 le rapport PSR 2019.

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. 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.

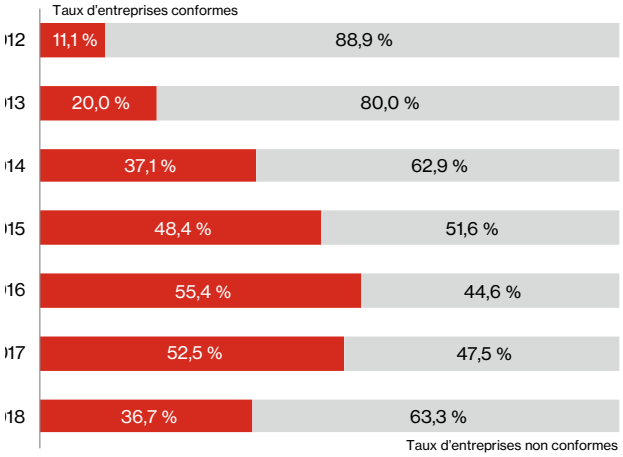


Figure 3 : Taux de conformité totale des entreprises par an

Cette diminution globale du taux de conformité met en lumière l'importance de créer, mais aussi de maintenir un programme de conformité PCI DSS mature sur la durée. Pour y parvenir, les entreprises doivent faire évoluer leur programme de conformité et de protection des données (DPCP). D'après les 55 entreprises interrogées pour le rapport PSR 2018, elles sont 18 %, tous secteurs confondus, à ne pas avoir défini de programme DPCP. 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.

Des mesures proactives pour inverser la tendance

Pour devenir un vecteur de compétitivité, la protection des données des clients et des titulaires de carte doit faire l'objet d'une démarche proactive de la part des entreprises. C'est dans cet esprit que Verizon vient de publier sa nouvelle édition du rapport PSR, source d'éclairages inestimables pour les professionnels des paiements par carte. Les auteurs y parlent notamment de l'importance de nouveaux outils comme notre Cadre 9-5-4 d'évaluation des performances des programmes de conformité.

Bilan du secteur hôtelier

Bons points

L'hôtellerie a tout de même progressé sur quelques points.

Même si le taux de chiffrement des données en transit (condition 4 du standard PCI DSS) reste le plus bas de tous les secteurs étudiés, il est le seul à avoir progressé par rapport à l'année dernière. Les acteurs de ce secteur ont également renforcé leur protection contre les malwares (condition 5). Ils enregistrent d'ailleurs la plus forte progression dans ce domaine, avec un nouveau taux de conformité de 84,2 %.

De toutes les industries passées en revue pour le PSR 2019, l'hôtellerie est la seule à avoir amélioré son contrôle des accès physiques (condition 9) sur un an. Dans ce domaine, son taux de conformité a gagné 9,3 points pour atteindre 63,2 %.

Mauvais points

Parmi les quatre secteurs étudiés (les trois autres étant le retail, les services financiers et les services IT), l'hôtellerie arrive en dernière position sur un certain nombre de conditions PCI DSS essentielles :

- Maintien d'une configuration de pare-feu (condition 1)
- Modification des paramètres de sécurité par défaut du fournisseur (condition 2)
- Protection du stockage des données stockées des titulaires de carte (condition 3)
- Chiffrement des données en transit (condition 4)
- Développement et maintenance de systèmes sécurisés (condition 6)
- Restriction des accès (condition 7)
- Test des systèmes et processus de sécurité (condition 11)

La liste ne s'arrête malheureusement pas là. Outre un faible taux de conformité dans ces domaines, le secteur affiche les plus gros écarts de conformité pour les conditions 1, 2, 6 et 11. Concernant les conditions 3, 6, 7 et 11, les écarts de contrôles enregistrent la plus forte hausse de tous les secteurs étudiés.

L'autre fait marquant de ce bilan en demi-teinte, c'est le très net recul de l'hôtellerie dans sa capacité à développer et maintenir des systèmes sécurisés (-21,9 points), à limiter les accès (-21,5 points) et à authentifier ces derniers (condition 8, baisse de 11,7 points pour un taux de conformité de 42,1 % en 2019).

Sachant que ces conditions étaient autrefois remplies, on en déduit que les acteurs du secteur peinent surtout à concevoir et maintenir des programmes PCI DSS matures et homogènes dans la durée.

Faits intéressants

Certes, l'hôtellerie est à la traîne en matière de protection du stockage des données de cartes de paiement (condition 3). Mais elle a aussi dû composer avec des problématiques qui lui sont propres, comme notamment le manque de solutions adaptées aux spécificités de ces établissements.

Cela dit, la réponse à incident s'avère souvent tout aussi importante que la prévention. Là encore, le rapport fait état des grandes difficultés des métiers hôteliers dans les domaines de l'identification et de l'authentification des utilisateurs (condition 10.2.5), de la revue et des tests du plan de réponse à incident (condition 12.10.2) et de la formation des collaborateurs chargés de cette réponse (condition 12.10.4).

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.

Recommandations

Contrôlez les accès.

Les acteurs de l'hôtellerie vont devoir réagir à la chute vertigineuse des taux de conformité aux obligations de restriction et d'authentification des accès, surtout à une époque où tant de fournisseurs et de solutions existent. Le Cadre Verizon 9-5-4 d'évaluation des performances des programmes de conformité peut également les aider à établir des contrôles d'accès plus stricts.

Misez sur la maturité.

L'hôtellerie peine de plus en plus à se conformer à un certain nombre de ses obligations PCI DSS. Les lacunes observées sont révélatrices d'un besoin urgent de processus plus cohérents et plus matures pour évoluer au rythme des changements dans la sécurité des paiements.

Pour commencer, elles peuvent suivre la recommandation suivante.

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

Développez la maturité de votre programme.

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 leurs programmes de conformité et de protection des données. Le Cadre Verizon 9-5-4 renforce leur niveau de visibilité et de contrôle, avec à la clé des processus plus homogènes et reproductibles, et des résultats plus prévisibles.

Une sécurité des paiements efficace et intégrée

Dans l'hôtellerie, le soin et l'attention du client sont le b.a.-ba du métier. Et le traitement des données de carte de paiement en fait partie intégrante. Pour les groupes hôteliers qui prennent très au sérieux les questions de sécurité, les opportunités ne manqueront pas. En clair, la création d'un programme cohérent de contrôle et de protection des données les aidera à apporter une garantie de sérénité à leurs clients.

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

© 2019 Verizon. Tous droits réservés. Verizon, le logo Verizon et tous les autres noms, logos et slogans identifiant les produits et services de Verizon sont des marques commerciales et des marques de service, déposées ou non, de Verizon TrademarkServices LLC ou de ses filiales aux États-Unis et/ou dans d'autres pays. Les autres marques commerciales et marques de service citées sont la propriété de leurs détenteurs respectifs. 11/2019