DOCUMENT D'INFORMATION

Secteurs à risque courants dans l'industrie de l'hébergement

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 hôtels de toute l'Amérique du Nord doivent être conscients de leurs secteurs vulnérables.

Les terminaux de point de vente (PDV)

L'industrie de l'hébergement arrive en tête en ce qui a trait aux intrusions liées aux points de vente, totalisant 87 % des bris de sécurité à des PDV.[2] Les fraudeurs ont de multiples points d'entrée puisque les données de cartes de paiement se retrouvent partout dans l'hôtel, que la majorité des hôtels possèdent de nombreux terminaux de PDV et que l'hôtel reçoit souvent les renseignements au sujet des cartes bien avant l'arrivée des clients.

Le manque de protection des renseignements personnels

Une recherche révèle que 74 % des hôtels n'ont pas de protection contre les brèches de données. Moins de la moitié des hôtels utilisent le chiffrement de bout en bout, un moyen qui protège les données des titulaires de carte, et la tokenisation, une méthode qui protège les données personnelles et les informations de paiement aux terminaux de paiement.[3]

L'interconnectivité des données au sein de l'hôtel

En raison de l'interconnexion des boutiques et des services dans l'hôtel, comme les restaurants, les services de nettoyage à sec, les spas, les centres d'affaires internes, etc., une brèche de données peut se propager rapidement dans tout le site, la rendant plus complexe et plus coûteuse.

Le roulement élevé du personnel de l'hôtel

Les travailleurs du secteur de l'hébergement sont en première ligne en ce qui a trait au service à la clientèle – et à la sécurité des données. Cependant, le taux de roulement de ces employés a tendance à être élevé, ce qui peut avoir une incidence sur la sécurité des données en temps réel. Certaines études démontrent que le taux de roulement chez les employés d'hôtels ne faisant pas partie des cadres est de près de 50 %.[4]

Les risques provenant des fournisseurs externes

L'industrie de l'hébergement transmet beaucoup de données confidentielles aux compagnies aériennes, aux compagnies de location de voitures, aux organisations de détail et à d'autres fournisseurs tiers. 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.[5]

Les attaques par logiciels rançonneurs

Le vol d'appareils mobiles, de renseignements confidentiels et d'autres biens de valeur demeure toujours une question préoccupante. Toutefois, l'interconnexion des systèmes informatisés signifie qu'une brèche de réseau causée par un logiciel rançonneur ou malveillant peut également toucher les éléments structurels de l'hôtel, notamment les serrures et les systèmes électriques, de chauffage et de ventilation.

Le manque de gestion de la sécurité des appareils mobiles

Dans le cadre d'une récente étude, près du tiers (32 %) des organisations ont admis sacrifier la sécurité des appareils mobiles afin d'accroître le rendement de l'entreprise. La technologie mobile touche de nombreux systèmes dans un hôtel, incluant les systèmes de gestion de la propriété, les systèmes de PDV, les serrures, les systèmes de messagerie, etc.[6]

L'équipement obsolète

Lorsque les hôtels acquièrent de nouvelles technologies ou de nouveaux systèmes ou logiciels, ils peuvent entreposer ou ne pas éliminer adéquatement leur vieux matériel, ce qui peut accroître le risque de brèche de données.

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. 2017 Lodging Technology Study, Hospitality Technology
4. Four Industries That Have High Turnover Rates, and What to Do About It, mai 2017, Business.dailypay.com
5. What CISOs Worry About in 2018 Research Survey, Ponemon Institute and Opus, janvier 2018
6. Mobile Security Index Report 2018, Verizon

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

877-227-5986 | shredit.com/hotel

Shred-it® est une solution Stericycle.

Shred-it®