

Une étude à l'échelle mondiale montre l'augmentation des risques pour la sécurité des données de paiement et le manque de confiance dans la sécurisation des modes de paiement mobiles

54 % des professionnels de l'informatique interrogés ont déclaré que leurs sociétés avaient fait l'objet d'une violation de données impliquant des données de paiement, quatre fois en moyenne durant les deux dernières années

Amsterdam, le 26 janvier 2016 – Avec l'arrivée de la solution de paiement mobile et d'autres modes de paiement qui devraient doubler dans les deux prochaines années, une nouvelle étude à l'échelle mondiale montre qu'il est essentiel que les entreprises améliorent leurs pratiques de sécurité en matière paiement. C'est la conclusion qui ressort d'une enquête récente à laquelle ont participé plus de 3 700 professionnels de la sécurité informatique de plus d'une dizaine de grands secteurs industriels. Cette enquête a été menée de manière indépendante par le Ponemon Institute pour le compte de Gemalto (Euronext NL0000400653 GTO), le leader mondial de la sécurité numérique.

Principaux résultats

Selon l'étude indépendante sur la sécurité des données de paiement, plus de la moitié (soit 54 %) des personnes interrogées ont déclaré que leurs sociétés avaient été confrontées à des problèmes de violation de sécurité et de données impliquant des données de paiement, quatre fois en moyenne durant les deux dernières années.

Ceci n'est pas surprenant lorsque l'on se penche sur les investissements, les pratiques et les procédures relatifs à la sécurité soulignés par les personnes interrogées :

- 55 % ont affirmé qu'ils ignoraient où toutes leurs données de paiement sont stockées ou situées.
- La prise en charge de la sécurité des données de paiement n'est pas centralisée ; 28 % des personnes interrogées estiment que la responsabilité incombe au directeur informatique, 26 % qu'elle incombe à l'entité commerciale, 19 % au service de la conformité, 15 % au directeur de la sécurité de l'information et 14 % à d'autres services.
- 54 % ont déclaré que la sécurité des données de paiement ne fait pas partie des cinq premières priorités relatives à la sécurité, un tiers (soit 31 %) seulement pense que leur entreprise consacre suffisamment de ressources à la protection des données de paiement.
- 59 % ont déclaré que leur entreprise permet aux tiers d'accéder aux données de paiement et 34 % d'entre elles seulement utilisent l'authentification multi-facteurs pour sécuriser l'accès.
- Moins de la moitié des personnes interrogées (soit 44 %) ont déclaré que leurs entreprises utilisent l'encodage de bout-en-bout pour protéger les données de paiement, du point de vente au moment où elles sont stockées et/ou transmises à l'établissement financier.
- 74 % ont déclaré que leurs sociétés ne sont pas en conformité avec la norme PCI DSS ou qu'elles n'y sont que partiellement conformes.

« Ces résultats de recherche indépendante devraient alarmer les dirigeants d'entreprises », commente Jean-François Schreiber, Vice-Président senior en charge des Services d'identité, de données et des logiciels chez Gemalto. « Compte tenu des résultats obtenus au sujet des modes de paiement et de la sécurité des données traditionnels, les entreprises concernées par les données de paiement doivent réaliser que la conformité ne suffit pas et repenser entièrement leurs pratiques de sécurité, surtout qu'un tiers des personnes interrogées ont affirmé que la conformité avec la norme PCI DSS ne suffit pas pour assurer la sécurité et l'intégrité des données de paiement. Les répercussions financières des violations de données, et les dommages causés à la réputation de l'entreprise et aux relations clients engendreront un risque potentiel encore plus grand à mesure que de nouveaux modes de paiement sont adoptés », ajoute Schreiber.

Nouveaux modes de paiement à la hausse et augmentation des problèmes de sécurité

Selon l'étude, l'acceptation de nouveaux modes de paiement tels que l'utilisation du mobile, l'utilisation du paiement sans contact et du porte-monnaie électronique va doubler au cours des deux prochaines années. Bien que les personnes interrogées disent que le paiement mobile ne représente que 9 % de tous les moyens de paiements aujourd'hui, ils s'attendent à ce que dans deux ans ce taux augmente à 18 %. Compte tenu des problèmes auxquels les professionnels de l'informatique des entreprises disent être confrontés dans la protection des données de paiement acceptées aujourd'hui à travers les modes traditionnels, les entreprises devront probablement faire face à plus de difficultés pour sécuriser de nouveaux modes de paiement. En fait, l'étude a révélé que près des trois quarts (soit 72 %) des personnes interrogées pensent que ces nouveaux modes de paiement exposent les données de paiement à des risques et que 54 % ne croient pas que – ou ne savent pas si les protocoles de sécurité instaurés dans leur entreprise sont capables de prendre en charge ces plateformes.

« À mesure que les entreprises décident d'accepter de nouveaux moyens de paiement, elles doutent de leur capacité à pouvoir protéger ces données. La majorité des personnes interrogées estiment que la protection des données de paiement n'a pas été la priorité absolue au sein de leur entreprise, et que les ressources, les technologies et le personnel en place sont insuffisants. Malgré la tendance à mettre en œuvre de nouveaux modes de paiement, celles qui sont dans le domaine de la sécurité informatique ne pensent pas que leurs entreprises sont prêtes. Il est évidemment essentiel que les entreprises recherchent des solutions et y investissent pour combler ces lacunes en matière de protection des données, et ce rapidement », a conclu Schreiber.

Pour consulter l'intégralité de l'étude et les résultats et données par pays, cliquer [ici](#).

À propos de l'enquête :

L'enquête a été menée par le Ponemon Institute pour le compte de Gemalto auprès de 3 773 professionnels de l'informatique et de la sécurité informatique aux États-Unis, au Royaume-Uni, en Allemagne, en France, en Belgique, aux Pays-Bas, au Japon, en Inde, en Russie, au Moyen-Orient et en Afrique du Sud. Les industries représentées comprennent les télécommunications, le divertissement et les médias, les services financiers, les gouvernements, la santé, l'hôtellerie, les services informatiques, le commerce de détail, la technologie, le transport et les services publics. Toutes les personnes interrogées connaissent bien l'approche de leurs sociétés en matière de protection des données de paiement et y participent. La plupart des personnes interrogées participent à la détermination des priorités et à la sélection des fournisseurs et sous-traitants dans l'écosystème de paiement de leurs entreprises.

Ressources associées

- [Résumé graphique – Tendances mondiales de la sécurité des données de paiement](#)
- [Vidéo : Secure the Breach : une approche en trois étapes de la sécurité des données](#)

À propos de Gemalto

Gemalto (Euronext NL0000400653 GTO) est le leader mondial de la sécurité numérique avec un chiffre d'affaires 2014 de 2,5 milliards d'euros et des clients de premier plan dans plus de 180 pays.

Dans un monde numérique de plus en plus interconnecté, Gemalto aide à établir des relations de confiance mutuelle. Des milliards de personnes à travers le monde veulent un mode et un cadre de vie plus agréables et intelligents. Ils veulent être libres de communiquer, acheter, voyager, faire des transactions bancaires, se divertir et travailler – à tout moment et en tous lieux – de façon agréable et sûre. Dans ce monde mobile et numérique en évolution rapide et constante, nous donnons aux entreprises et aux administrations les moyens d'offrir une large gamme de services numériques pratiques et sûrs en sécurisant les transactions financières, les services mobiles, les « clouds » publics et privés, les systèmes d'e-santé, l'accès aux services d'e-gouvernement, l'« Internet des objets », et les systèmes de billettique et de transports.

Notre portefeuille unique, qui s'étend des logiciels cryptographiques embarqués dans une variété d'objets du quotidien, à nos plateformes de back-office extrêmement robustes et évolutives pour l'authentification, le cryptage et la gestion des identifiants numériques, est mis en œuvre par nos équipes qui assurent un service de niveau mondial. Présent dans 46 pays, Gemalto emploie plus de 14 000 salariés travaillant depuis 99 bureaux, 34 centres de personnalisation et de données et 24 pôles de Recherche et de Développement logiciel.

Pour plus d'informations, visitez nos sites www.gemalto.com/france, www.justaskgemalto.com, blog.gemalto.com, ou suivez [@GemaltoFrance](https://twitter.com/GemaltoFrance) sur Twitter.

Contacts presse Gemalto :

Philippe Benitez
Amérique du Nord
+1 512 257 3869
philippe.benitez@gemalto.com

Peggy Edoire
Europe et CEI
+33 4 42 36 45 40
peggy.edoire@gemalto.com

Vivian Liang
大中华地区 ((Grande Chine)
+86 1059373046
vivian.liang@gemalto.com

Ernesto Haikewitsch
Amérique Latine
+55 11 5105 9220
ernesto.haikewitsch@gemalto.com

Kristel Teyras
Moyen-Orient et Afrique
+33 1 55 01 57 89
kristel.teyras@gemalto.com

Pierre Lelievre
Asie-Pacifique
+65 6317 3802
pierre.lelievre@gemalto.com

Le texte de ce communiqué, issu d'une traduction, ne doit en aucune manière être considéré comme officiel. La seule version du communiqué qui fasse foi est celle du communiqué dans sa langue d'origine, l'anglais, qui prévaut donc en cas de divergence avec la traduction.