Voyages d'affaires et transports en commun : confidentialité et sécurité des données

La menace du « piratage visuel » dans les avions, les trains et autres transports publics ne fait pas beaucoup parler d'elle en matière de sécurité des données. Mais elle peut s'avérer être une réelle menace, surtout si le contenu de votre écran révèle des données commerciales hautement confidentielles et susceptibles de vous compromettre avec un client ou un concurrent.

Tout le monde s'est déjà retrouvé assis dans un train à côté d'une personne tapant nerveusement sur son clavier d'ordinateur, ignorant complètement le fait que quelqu'un est en train de lire par-dessus son épaule et a accès à toutes sortes de données confidentielles. Entre de mauvaises mains, ces données pourraient la mettre dans une situation délicate... Et si cela peut sembler tiré par les cheveux pour certains, réfléchissez-y à deux fois la prochaine fois que vous êtes en route pour un rendez-vous client important ou sur le chemin du retour après une réunion qui s'est mal passée. Des conversations et des regards de personnes assises autour de vous sur le contenu de vos écrans peuvent s'avérer extrêmement impactantes et embarrassantes. Surtout si d'autres passagers travaillent dans votre secteur d'activité...

Ne divulguez pas les secrets commerciaux de vos concurrents

Vous ne voulez pas que vos concurrents ou clients potentiels connaissent les informations sur votre entreprise, alors pourquoi en parler ou écrire des emails confidentiels dans les transports en commun ? Le piratage visuel est une véritable menace pour la sécurité et la confidentialité des données et ne doit surtout pas être ignorée.

De plus, la protection de la vie privée visuelle se révèle être très importante pour la satisfaction des employés, ce qui se traduit même par une réduction de 50% de leur productivité s'ils estiment que cette dernière est en danger.

Plus de la moitié des entreprises françaises ont déjà fait face à une cyberattaque avec des conséquences sur leur activité au cours des 24 derniers mois. Parmi elles, 13% ont mis plus de 24 heures à prendre conscience de l'attaque et près de 20% ne savent toujours pas comment cette dernière est survenue. Au final, 60% n'ont pas été en mesure d'identifier le ou les responsables[1]. Ces résultats soulignent la lourde tâche des enquêteurs spécialisés qui se retrouvent face à des entreprises parfois mal préparées et des criminels qui ne le sont parfois que trop bien. La bonne nouvelle c'est que les entreprises sont de plus en plus conscientes du risque et ne cessent d'améliorer leur défense.

Conseils pratiques pour bien sécuriser les données lors de vos déplacements

Les voyageurs qui répondent aux emails et consultent des documents à la vue de tous pendant leurs déplacements sont un excellent exemple de la rapidité avec laquelle des données sensibles et précieuses peuvent tomber entre de mauvaises mains. Il existe un certain nombre de moyens de traiter cette question dont les employés et les responsables informatiques doivent vraiment être conscients. La première étant de toute évidence de ne pas le faire !

Toutefois, il n'est ni raisonnable ni déraisonnable d'empêcher les gens de travailler durant leurs

déplacements, si vous devez vraiment traiter des informations confidentielles dans un train de banlieue bondé ou sur un vol d'affaires long courrier, vous pouvez également utiliser un écran de confidentialité, qui agit comme un filtre assez puissant pour décourager les curieux.

Une étude récente d'IDC a mis en évidence que la raison la plus courante pour laquelle les entreprises britanniques acquièrent des écrans de confidentialité est de protéger leur image, qui se révèle être prioritaire sur la perte de données ou les préoccupations de confidentialité. Bien que les écrans de confidentialité ne soient pas dotés de capacités de chiffrement avancées, ils restreignent la vue des observateurs, ce qui signifie que seule la personne devant l'écran peut voir ce qu'il contient.

De plus, alors que nous faisons face à l'un des changements les plus importants en matière de protection des données personnelles depuis une génération - le Règlement général sur la protection des données (RGPD) - les entreprises risquent bien plus que la simple perte de données confidentielles si elles ne parviennent pas à protéger leurs informations clients.

Mieux vaut prévenir que guérir

Les entreprises s'efforcent de se concentrer sur les produits et services technologiques les plus récents et adaptés pour prévenir de la cybercriminalité.

Récemment au Royaume-Uni, la Nationwide Building Society a été condamnée à une amende de 980 000 livres à la suite du vol d'un ordinateur portable ayant eu lieu au domicile d'un employé. Cela peut paraître un peu sévère, mais pas si l'on considère que l'ordinateur portable en question contenait des données confidentielles clients, qui mettent en danger les coordonnées de près de 11 millions de contacts. Après avoir initialement constaté que la sécurité n'était pas à la hauteur, la Financial Services Authority (FSA) a alors déclaré que les clients de Nationwide avaient été exposés à un risque de criminalité financière. Malgré les excuses adressées aux 11 millions de clients concernés, l'incapacité de Nationwide à surveiller ou à gérer les téléchargements de données sur les périphériques de stockage signifiait qu'elle avait un contrôle limité sur les informations stockées, notamment sur ordinateur portable, ainsi que sur la façon dont elles étaient utilisées.

Ne laissez pas une faille dans la sécurité de vos données

Pour que les entreprises puissent mettre en oeuvre avec succès une stratégie de sécurité efficace, elles doivent aller au-delà de la simple utilisation de logiciels sophistiqués et accorder une plus grande importance à la sécurité purement physique et à l'impact croissant que cette dernière a sur l'ensemble des activités. De la même manière que les violations à grande échelle peuvent avoir des répercussions non seulement financières, structurelles et commerciales, l'exposition de la sécurité physique va aussi de pair avec la réputation. Si les données clients et d'entreprise tombent entre de mauvaises mains, ces derniers ne se soucieront pas de savoir si elles ont été volées en ligne ou en personne, les répercussions seront exactement les mêmes.

Cela est devenu encore plus important depuis que le RGPD est entré en vigueur, car les entreprises ne sont plus en mesure d'éviter les questions sur la manière et l'endroit où elles stockent les données des clients et sont obligées d'être transparentes. Les conditions de consentement sont renforcées et les entreprises sont pénalisées si elles utilisent des termes et conditions illisibles et indigestes concernant le consentement aux données.

Ainsi, pour que les entreprises aient vraiment une chance de progresser dans le jeu de la sécurité, il devient urgent de se pencher sur des petites solutions simples, souvent « oubliées » de la sécurité des données.

[1] Source : étude Kaspersky Lab réalisée auprès des décideurs informatiques de 1800 entreprises en Europe, dont 300 en France.