La sÃ©curitÃ© : un impÃ©ratif pour le e-commerce B2B
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 16/11/2022 14:00:00

Les entreprises, organisations et structures publiques sont aujourdâ□□hui toutes confrontÃ©es Ã la cybercriminalitÃ©. Dans ce contexte, les cyber attaques sont responsables de nombreux problÃ¨mes comme une perte de rÃ©putation, de CA, une rupture dâ□□activitÃ©, etc. Lâ□□industrie du e-commerce ne fait pas exception.

En effet, la trÃ¨s forte montÃ©e en puissance du e-commerce (notamment en B2B) est dÃ©sormais une tendance durable qui conduit les professionnels Ã positionner la sÃ©curisation de leurs plateformes comme une donnÃ©e stratÃ©gique.Â

De plus, il y a encore peu de temps, peu de transactions B2B Ã©taient rÃ©alisÃ©es par rapport au B2C.

De fait, le e-commerce B2B Ã©tait encore relativement Ã©pargnÃ© par les cyberattaques. Ce n'est plus le cas dÃ©sormaisi au regard des forts volumes de transactions rÃ©alisÃ©s Ã lâ□□Ã©chelle mondiale. Il est donc stratÃ©gique de positionner la sÃ©curitÃ© au centre de son projet.

Mettre en place des standards de paiements sÃ©curisÃ©s

Il est fondamental de sâ□□appuyer sur des normes reconnues. Un consortium de sociÃ©tÃ©s de cartes de crÃ©dit ainsi que le Conseil des normes de sÃ©curitÃ© de l'industrie des cartes de paiement (PCI) ont Ã©tabli des normes pour assurer la sÃ©curitÃ© des donnÃ©es par toute entreprise qui traitait les cartes de crÃ©dit.

Ces normes sont appelÃ©es normes de sÃ©curitÃ© des donnÃ©es (DSS) et s'appliquent aux entreprises qui traitent des transactions en face Ã face ainsi qu'aux entreprises de commerce Ã©lectronique.Â

L'objectif de PCI DSS est alors tout simplement de gÃ©rer en toute sÃ©curitÃ© les informations de paiement des acheteurs utilisant des cartes de crÃ©dit. Les e-commerÃ§ants doivent Ãªtre conformes Ã cette norme.

Garantir quâ□□il sâ□□agit bien du bon site marchand

Sur ce point, il est important de sâ□□appuyer sur des certificats de confiance. Mettre en place un HTTPS et des SSL sont des Ã©lÃ©ments centraux qui permettent Ã lâ□□internaute de sâ□□assurer quâ□□il est bien sur le bon site en vÃ©rifiant lâ□□exactitude du certificat et quâ□□il peut Ã©changer de bout en bout ses informations en toute confiance.

De fait, il sâ□□agit dâ□□une premiÃ¨re Ã©tape engageante pour proposer une expÃ©rience dâ□□achat de qualitÃ©. On notera aussi que sâ□□appuyer sur un HTTPS est Ã©galement aujourdâ□□hui un incontournable pour pouvoir Ãªtre bien rÃ©fÃ©rencÃ© sur les moteurs de recherche.

Choisir la bonne plateforme e-commerce

Les entreprises doivent apporter un soin particulier pour sÃ©lectionner une plateforme adaptÃ©e

Ã leur besoin et qui garantit un haut niveau de sÃ©curitÃ©.Â

En ce sens, attention Ã bien Ã©valuer ce point et Ã Ã©viter les dÃ©veloppements sur mesure difficiles Ã maintenir et qui nâ□□intÃ¨grent pas en continu les derniers standards et nouveautÃ©s Ã mettre en place pour garantir au web marchand comme Ã lâ□□acheteur une sÃ©curitÃ© optimale.

On notera Ã©galement que les aspects liÃ©s au RGPD doivent Ãªtre pris en compte.

Auditer son site en continu

La sÃ©curitÃ© informatique est un sujet mouvant qui ne cesse dâ□□Ã©voluer. Dans ce contexte, il convient de mener des audits rÃ©guliers de son site pour sâ□□assurer que ce dernier est bien en capacitÃ© de protÃ©ger ses utilisateurs contre les derniÃ¨res menaces.Â

Câ□□est aussi un Ã©lÃ©ment clÃ© pour lâ□□e-commerÃ§ant qui peut sâ□□assurer quâ□□il ne sera pas impactÃ© dans son exploitation par des cyberattaques.

Bien dâ□□autres sujets sont possibles pour Ã©lever le niveau de cybersÃ©curitÃ© des sites e-commerce B2B. Une chose est sÃ»re, la cybersÃ©curitÃ© est bien plus quâ□□un Ã©lÃ©ment technique, câ□□est bien une prioritÃ© stratÃ©gique qui se positionne au centre de la qualitÃ© de lâ□□expÃ©rience dÃ©livrÃ©e aux acheteurs.

Laurent Desprez, Vice President and General Manager for Europe at Oro Inc.