La sécurité d'un site e-commerce n'est pas l'affaire exclusive de l'hébergeur

Par Julien Mellul, directeur technique d'Ecritel

Un hébergeur responsable offre généralement à ses clients de nombreux outils de sécurité pour protéger les données indispensables à ses activités commerciales. Mais ces dispositions n'exonèrent pas totalement les entreprises qui doivent elles aussi respecter des règles de sécurité et se conformer à certaines normes, comme PCI DSS.
Julien Mellul délivre ici les bonnes pratiques à adopter pour assurer la sécurité d'un site et souligne l'importance de la collaboration entre hébergeur et e-commerçant.

Performances et sécurité

Si la réactivité et la rapidité d'un site sont des paramètres cardinaux du e-commerce, **la résistance aux cyberattaques est devenue au fil des ans le premier impératif**. Selon Imperva, un spécialiste de la cybersécurité, l'an dernier, les agressions ont été plus nombreuses mais surtout plus persévérantes, ce qui manifeste, de la part des attaquants, une réelle volonté de nuire ou d'arriver à pénétrer les systèmes pour voler des données. Les sites e-commerce ont été pour près de la moitié la cible d'attaques. **67% des entreprises déclarent avoir été agressées l'an passé** (coût moyen des dégâts 75 000 €) pour celles qui s'en sont aperçu car il faut parfois 6 mois pour constater les faits.

Au final, selon l'étude PAC « Incident Response Management » de 2015, toutes les entreprises ont été la cible des cyberdélinquants et si, 90% des sociétés s'estiment prêtes à contrer les attaques en France, seules 52% ont élaboré un plan de reprise pour redevenir rapidement opérationnelles.

Des méconnaissances en matière de sécurité

La prise de conscience en matière de cybersécurité dans les entreprises est loin d'être satisfaisante. Côté dirigeants, 79% déclarent n'y rien comprendre, 80% ne protègent ni leurs données ni leurs terminaux (91%) et 83% n'ont rien prévu pour parer la menace. Côté employés, 71% utilisent leurs propres terminaux, voire plusieurs (36%), sur le réseau sécurisé de l'employeur. 35% stockent des données professionnelles sur leur PC personnel que près de la moitié estime non-sécurisé (*). En France, le constat n'est pas meilleur, bien au contraire, malgré les actions pédagogiques du Cigref et de l'Anssi (**). Concernant plus spécifiquement le e-commerce, Dashlane (***) a noté que 70% des sites français n'ont pas de politique responsable de protection des données personnelles de leurs clients puisque 45% envoient identifiant et mot de passe en clair par email à la création de compte, 14% seulement demandent d'utiliser au moins une lettre et un chiffre, 87% acceptent des mots de passe simplistes (ex : 123456) et 83% ne bloquent pas leur saisie au delà de 10 essais erronés. **Pourtant les e-marchands sont directement concernés par les vols de données clients**, commis pour créer des fausses cartes bancaires, sans parler des risques qu'ils courent en terme de perte d'image de marque, de détérioration de référencement ou de baisse de chiffre d'affaires.

Quelles sont les bonnes pratiques à adopter ?

Quelles sont les attaques les plus courantes ? Les dénis de service (DDoS) en tous genres, les injections SQL et autre DNS poisoning sont autant de termes barbares qui traduisent la diversité des menaces et la nécessité d'y parer.

Comment ? D'abord en cryptant les données par l'usage de protocoles et de moyens appropriés (HTTPS/SSL/EVSSL, tunnel de paiement, outils d'administration et de sauvegarde des données) sachant que ces précautions sont désormais prises en compte par les algorithmes de classement de Google. Ensuite, il faut **surveiller en permanence ce qu'il advient dans son système d'information**, **détecter les événements et les alertes**, **procéder à des analyses approfondies, des audits et des tests de vulnérabilité** et **avoir toujours un plan de secours prêt**. La maintenance joue également un rôle préventif si l'on procède dès que possible aux mises à jour dans tous les domaines et à tous les niveaux. Enfin, il faut inlassablement **éduquer**, **rappeler les règles** en expliquant que la survie de l'entreprise est en jeu.

Quelles solutions pour l'hébergeur ?

L'hébergeur joue un rôle essentiel dans la protection des actifs numériques de ses clients. Il dispose pour cela d'une large gamme d'outils lui permettant normalement de solutionner chaque problème. **Il doit posséder des certifications pour son infrastructure, ses process et son personnel** qui garantissent le respect des bonnes pratiques, engagements validés par des tiers indépendants et qui s'appliquent du client final jusqu'au e-commerçant. Il existe des normes générales (ISO 27001) pour garantir la sécurité informatique dans tous types d'entreprise, **des normes spécifiques d'hébergement pour les données de santé** qui sont d'ailleurs applicables aux pharmacies en ligne, **et pour les données bancaires** (PCI DSS).

La norme PCI DSS a été définie par les émetteurs de cartes bancaires et concerne au premier chef tous les acteurs de e-commerce sur le site desquels transitent des données bancaires. Se conformer à la norme PCI DSS limite les fraudes en s'imposant plus de sécurisation ce qui permet d'éviter les pénalités en cas de problème et abaisse les taux de commissionnement sur les paiements en carte bancaire tout en favorisant la participation à certains appels d'offres.

Quelle implication pour l'e-commerçant ?

La norme PCI DSS définit environ 200 exigences et 12 règles auxquelles doivent répondre ensemble l'hébergeur et son client cybermarchand, mais si le premier est certifié cela ne couvre en aucun cas le second. L'hébergeur peut, en effet, n'avoir souscrit qu'à une partie seulement des 220 exigences et il faut savoir que dans le meilleur des cas 10% d'entre elles ne peuvent être couvertes que par le seul client e-commerçant.

Il faut donc bien vérifier ce que couvre vraiment la certification de l'hébergeur mais aussi, le cas échéant, celle du prestataire à qui l'e-commerçant recourt pour gérer le processus transactionnel. Ce prestataire peut choisir les exigences de la norme PCI DSS auxquelles il souscrit et c'est alors à son client e-commerçant de satisfaire aux autres. **La coordination entre l'hébergeur et son client est essentielle** et il faut savoir que plus le niveau de service fourni est élevé, plus le premier doit couvrir un nombre important d'exigences. Il faut donc vérifier le niveau de couverture inclus dans les offres de base qui souvent ne certifient que l'infrastructure dans les couches basses.

« Choisir un partenaire hébergeur ou un prestataire de gestion des transactions électroniques doit se faire dans le dialogue et en toute transparence. Il faut déterminer ensemble qui fait quoi et qui répond précisément aux 220 exigences. La sécurité est donc l'affaire de toutes les parties prenantes au business sur Internet ! », conclut Julien Mellul.

* Source : Bitdefender.

** Cigref et Anssi : Club Informatique des Grandes Entreprises Françaises et Agence nationale pour la sécurité des services d'information

*** Dashlane, éditeur de solution de gestion de mots de passe et de « portefeuille » numérique

---

À propos d'Ecritel

Ecritel est un fournisseur d'hébergement internet et d'infogérance pour les entreprises, principalement des e-commerçants, ainsi qu'un acteur majeur de prestations de Cloud Computing infogéré en Europe. Ecritel bénéficie de 20 années d'expertise IT reconnue dans l'hébergement infogéré. La société propose des services à forte valeur ajoutée adaptés aux besoins des clients grâce à une intégration rapide des technologies les plus innovantes : hébergement infogéré en mode Cloud public, privé ou mixte, accélération de contenus.

Ecritel est présent en France, aux Etats-Unis, au Canada, au Brésil, en Chine et à Hong-Kong et dispose de 10 Data Centers dans le monde. Disposant de son propre backbone international, Ecritel gère plus de 3,5 milliards d'euros de commandes annuelles pour le compte de ses clients.

Plus d'informations sur www.ecritel.com / www.euroasianequities.com
et suivez @Ecritel_France sur Twitter.

Contacts Presse Ecritel
Constance MERCIER, Responsable Communication Marketing :
01 73 02 50 80
cmercier@ecritel.net