traduit par un faible taux de transformation des visites en acte d'achat. Pourrait-on imaginer que 90 % des clients d'une grande surface en ressortent avec un chariot vide ?

Par ailleurs, les débats sur la d'échanges internationaux concernant des transactions d'un faible montant, les recours sont complexes et difficiles à exercer.

● Internet est souvent utilisé comme un outil de prospection, rents acteurs et les utilisateurs.

Toutefois, convaincus par les projections exponentielles du développement de l'Internet, les pionniers pensaient que le seul fait de se faire connaître par la publicité leur permettrait d'at- hier des charges dont le respect est contrôlé par un tiers de confiance. La certification peut, par exemple, porter sur la sécurité des données personnelles ou la fiabilité des processus commerciaux.

sécurité des systèmes d'information.

Prochain article : les droits du cyberconsommateur

interview

OLIVIER VELIN *Consultant en sécurité chez IBM*

« Créer un service et un budget suffisants pour la sécurité »

LE FIGARO ÉCONOMIE. – Constate-t-on une plus grande sensibilité des sites d'e-commerce aux problèmes de sécurité ?

Olivier VELIN. – L'actuelle situation de l'e-commerce est paradoxale car la fréquentation des sites de commerce en ligne s'accroît alors que l'internaute répugne à régler ses achats par cartes bancaires. Cette réticence est due à l'absence de confiance dans la sécurité des transactions. A ce jour, près de 80 % des internautes sont méfiants vis-à-vis de l'e-commerce et préfèrent l'achat en magasin. C'est pourquoi l'e-commerce se développe moins bien que prévu.

La méfiance des internautes est justifiée par l'accroissement des utilisations frauduleuses de leurs numéros de cartes bancaires. De plus, l'impact médiatique d'une fraude met en cause la crédibilité de l'entreprise touchée. Déjà, aux Etats-Unis, les sites d'e-commerce renforcent leurs mesures de sécurité, mentionnent des clauses de confidentialité ou affichent le logo d'une entreprise de sécurité spécialisée. La sécurité est une des clefs de l'e-commerce.

Quels sont les moyens dont ces entreprises se dotent afin d'atteindre un niveau de sécurité satisfaisant ?

En B to C (« business to consumer »), l'écart flagrant entre les équipements informatiques des contractants oblige l'entreprise à déployer des mesures de protection. L'entreprise doit sécuriser ses accès et réseaux informatiques, prendre toutes les mesures de protection et de sauvegarde de ses fichiers et bases de données. Mais les efforts réalisés sont très insuffisants. On se contente souvent d'un outil de sécurité du marché. Or aucun ne résout tous les problèmes rencontrés. De plus, les mesures de sécurité doivent évoluer avec la capacité de nuisance des fraudeurs. D'où l'importance de développer un état d'esprit sécurité dans l'entreprise, de créer un service et un budget suffisants pour se consacrer à cette tâche.

Olivier Velin : « Les efforts réalisés sont très insuffisants. » (DR.)

Peut-on identifier une typologie des incidents de sécurité ?

On distingue les escroqueries par création d'une entreprise fictive, règlements par titre de paiement volé, fraudes sur site d'enchères C to C (« consumer to consumer »), promesses de gains exceptionnels, chaîne pyramidale, club d'acheteurs, etc.