Commerce et e-commerce : comment se protéger avant des cyberattaques à la chaîne ?

Marco Genovese, Stormshield Network Security Product Manager

Les commerçants traditionnels et autres professionnels de l'e-business évoluent dans un environnement concurrentiel,
a fortiori
en cette période de soldes d'hiver. Commerçants comme acheteurs ont besoin d'interagir en toute sécurité, via une continuité de service et des communications infaillibles. Une sécurité remise en question par l'arsenal grandissant des cyber menaces, du vol de données aux ransomwares en passant par l'usurpation d'identité. Et tandis que les consommateurs réclament des services toujours plus rapides, fiables et efficaces, de nouvelles réglementations continuent de peser sur le secteur du commerce. Dès lors, comment conjuguer protections face aux cyber menaces et obligations règlementaires ?

Mettre en place et gérer un réseau sécurisé, protéger vos données et celles de vos clients, surveiller vos zones de vulnérabilité et protéger vos applications web sont autant d'impératifs pour développer vos ventes en toute sécurité. Des impératifs listés dans le standard mondial Payment Card Industry Data Security Standard (PCI DSS), qui vise notamment à réduire la fraude bancaire en ligne. Elle se base sur un ensemble d'exigences, comme la mise en place d'un pare-feu et d'un système de prévention d'intrusion actif.

Sécuriser ses serveurs et applications web

Le web est un vecteur d'attaques privilégié par les cyber pirates : on ne compte plus les sites web piratés ou le nombre de failles découvertes chaque semaine depuis le début de l'année. La protection de votre serveur et de vos applications web est donc un enjeu capital de votre sécurisation. Celle-ci passe également par une véritable chasse aux vulnérabilités.

Une des principales tâches quotidiennes d'un administrateur réseau doit être de vérifier en permanence si de nouvelles vulnérabilités ont été découvertes. Dans le cas où une nouvelle vulnérabilité affecterait son réseau, il doit alors se renseigner pour vérifier si un correctif existe déjà et l'installer. À ce jour, trop peu d'administrateurs effectuent ce travail, pourtant indispensable. L'utilisation d'un pare-feu implémentant une fonctionnalité d'évaluation des vulnérabilités en temps réel et en continu permettrait ainsi de faciliter cette tâche de veille sans avoir à mettre en place un équipement ou une solution complémentaire.

Cette chasse peut en complément passer par la mise en place d'une protection complète sur l'ensemble de votre système bureautique. En effet, les cyberattaquants peuvent rebondir de votre environnement de travail vers vos serveurs web et e-commerce si les bonnes mesures de sécurité ne sont pas mises en place. En associant une protection jumelée de vos applications et des postes de travail de vos collaborateurs, vous enrichissez votre activité d'une double barrière de sécurité

pour vous protéger contre les attaques les plus sophistiquées.

Garantir les transactions même en cas de panne

Face à ces attaques, qu'elles soient sophistiquées ou plus basiques, il vous faut garantir la continuité de votre service. Une approche dite en « haute disponibilité » assure cette continuité, même en cas de dysfonctionnement d'un équipement. Le contrôle de la bande passante, la priorisation de trafic, la lutte contre les attaques par déni de service (Ddos) et la gestion de la redondance des liens réseaux sont donc des axes-clés à aborder pour assurer le développement de votre activité.

Assurer une bonne gestion des données client

D'ici mai 2018, le compte à rebours est lancé. L'entrée en vigueur des réglementations européennes sur la protection des données personnelles (Règlement Général sur la Protection des Données ou General Data Protection Regulation) va impliquer un nombre non négligeable de contraintes sur la gestion des données des clients : confidentialité, lieu de stockage, droit de retrait, récupération des données. Autant de problématiques à prendre en compte dans le domaine du commerce et e-commerce. Une mise en conformité de votre enseigne grâce à un dispositif éprouvé est donc également à prendre en considération dans votre approche de cybersécurité.

En tant que professionnels du commerce et e-commerce, vous devez donc positionner le sujet de la cybersécurité au coeur de votre stratégie de croissance. Ainsi, vous pourrez alors vous concentrer sur le développement de vos activités et éviter de nombreux désagréments comme la perte de chiffre d'affaires ou de réputation. En prenant ces bonnes décisions, vous pourrez alors créer un espace de confiance avec vos clients.
