NTT Security

Présentation

La cybersécurité dans la grande distribution

Les nouvelles technologies ont révolutionné le monde du retail, aussi bien pour les clients que pour les enseignes. Dans un monde hyperconnecté, la transformation numérique des chaînes d'approvisionnement de ce secteur est bel et bien entamée.

Puces RFID, "self-edge" électronique, livraisons par des drones, programmes de fidélité basés sur les blockchains... les nouvelles technologies s'invitent dans tous les domaines de la grande distribution, nous rapprochant peu à peu du "magasin du futur".

Or, ces avancées élargissent également la surface d'attaque. Résultat : les grandes enseignes sont exposées à toutes sortes de cyberattaques car les mines d'informations qu'elles détiennent (données personnelles des clients, données des cartes bancaires) en font des cibles alléchantes pour les cybercriminels.

Ici, la principale menace reste le vol de données. En effet, les masses de données clients stockées par les enseignes se monnaient très cher dans le monde du cybercrime. Mais, elles peuvent aussi attiser la convoitise d'éléments internes mal intentionnés. Bien que difficile à chiffrer, l'impact d'un vol de données se ressent fortement sur le bilan d'une entreprise victime (érosion de la réputation, chute du cours de l'action, exode des clients vers la concurrence, etc.).

Côté conformité, le retail fait partie des secteurs les plus concernés par le RGPD, compte tenu des volumes colossaux de données clients qu'il traite. La sécurité du stockage de données n'a donc jamais été aussi cruciale, surtout qu'on ne connait pas encore l'étendue des amendes auxquelles s'exposent les entreprises contrevenantes.

Qu'on se le dise : le risque zéro n'existe pas. La cybercriminalité est aujourd'hui une réalité bien ancrée et les acteurs de la grande distribution sont plus que jamais dans le viseur des malfaiteurs. C'est pourquoi les enseignes doivent protéger leurs données clients. Elles doivent pour cela renforcer leur niveau de préparation aux cyberattaques pour maintenir la confidentialité des informations qu'elles détiennent.

Les défis de la cybersécurité dans la grande distribution

- Cloud, IoT, paiements mobiles et en ligne, Big Data... la généralisation de ces nouvelles technologies élargit la surface d'attaque des entreprises et, par ricochet, la vulnérabilité des données sensibles aux cyberattaques et violations de sécurité.
- Chaque technologie déployée en magasin (caméras de vidéosurveillance, systèmes POS, puces RFID, kiosques, tablettes de magasin, etc.) élargit un peu plus la surface d'attaque.
- La conformité au RGPD exige des enseignes de maîtriser les données qu'elles stockent (emplacements, accès, partage) et garantir leur sécurité.
- La norme PCI DSS permet de réduire la fraude aux paiements, mais son efficacité dépend de la capacité des entreprises à maintenir en permanence les contrôles de sécurité en place.
- Le champ des menaces ne cesse d'évoluer, avec l'apparition constante de nouvelles menaces et une complexification des menaces existantes.
- Le *turnover* augmente le risque de menaces internes liées à des salariés négligents ou mal intentionnés.
- L'absence de consolidation contraint les entreprises à faire appel à de multiples prestataires pour protéger différents départements de l'entreprise.

Selon une étude du British Retail Consortium, plus de la moitié (53 %) des fraudes enregistrées dans la grande distribution s'effectuent en ligne, ce qui représente un coût total direct d'environ 100 millions d'euros.

Enquête annuelle du British Retail Consortium sur la cybercriminalité

- Le nombre croissant de terminaux personnels connectés au réseau augmente les risques liés aux communications clients, aux interactions avec des tiers et à l'intégration de contractuels aux effectifs de l'entreprise.
- La pénurie de compétences internes en sécurité empêche les entreprises de surveiller et protéger toute leur infrastructure de manière continue et efficace.

Des fonctionnalités exclusives

Sécurité, conformité, gestion du risque... nous mettons à votre disposition une vaste gamme de services managés. Notre rayon d'action mondial est doublé d'une forte présence locale. Et nos experts sont à l'écoute des problématiques spécifiques que vous rencontrez en tant qu'acteur de la grande distribution, aussi bien au niveau régional qu'international.

Quant à notre collaboration avec les entreprises du groupe NTT et notre réseau de partenaires de confiance, elles nous permettent de combiner des services cloud, managés, de consulting et de sécurité hybrides pour garantir la cyber-résilience de votre entreprise.

Services de sécurité managés

Face à des attaques toujours plus fréquentes et plus sophistiquées, de nombreuses enseignes peinent à gérer tous les aspects de leur cybersécurité

en interne. En faisant de NTT Security votre fournisseur de services de sécurité managés, vous optez pour un spécialiste de réputation mondiale, doté de professionnels chevronnés de la sécurité.

Notre mission : vous offrir des services de surveillance, de gestion et de support, de bout en bout et 24h/24, pour vos données clients et votre infrastructure de sécurité. Notre plateforme mondiale de services de sécurité managés se distingue par ses fonctionnalités de détection des menaces, d'analyses avancées et de Threat Intelligence uniques et adaptées à votre secteur.

Où que vous conduisent vos relations clients, vous pourrez compter sur le soutien d'un leader mondial capable de répondre à tous vos besoins de cybersécurité.

Nos services de sécurité managés vous permettent également de mettre en œuvre les recommandations émises par nos consultants, en toute simplicité. Enfin, nous veillons à ce que vous bénéficiez d'un service de cybersécurité de bout en bout adapté à votre secteur.

Consulting et conformité continue

Répercussions financières et réputationnelles, perte de confiance des clients, violations réglementaires… toute perte de données peut créer une onde de choc considérable. D'où l'importance d'élaborer, d'implémenter et de piloter une stratégie de prévention efficace. C'est précisément là qu'intervient NTT Security.

En moyenne, les distributeurs ont investi presqu'autant dans la prévention d'actes criminels (hors Internet) en 12 semaines qu'ils ne l'on fait tout au long de l'année précédente. Et près de la moitié des personnes interrogées ont observé une hausse des attaques l'an dernier.

Enquête annuelle du British Retail Consortium sur la cybercriminalité

Conseiller de confiance auprès de grands noms du monde entier, NTT Security est parfaitement conscient des exigences des distributeurs en termes de sécurité des données et de réduction des risques. Notre méthodologie éprouvée vous aidera à renforcer la sécurité de vos données clients sensibles, avec à la clé une protection de votre chiffre d'affaires et de votre réputation.

En France, les acteurs du retail doivent se plier à des obligations draconiennes de notification en cas de violation de sécurité. À défaut, toute violation qui se révèlerait une infraction sérieuse au RGPD exposerait l'entreprise concernée à de très lourdes amendes infligées par la CNIL. L'Allemagne a quant à elle adopté une nouvelle loi fédérale sur la protection des données afin de s'aligner sur les exigences du RGPD.

Connaître vos engagements en matière de conformité est une chose, les tenir en est une autre.

En faisant appel aux entreprises du groupe NTT, vous bénéficierez de toute l'expertise des consultants NTT Security, des professionnels à vos côtés pour élaborer vos politiques et processus (gouvernance, risque, conformité) d'un point de vue stratégique et technique.

Vous aurez ainsi toutes les cartes en main pour créer une infrastructure de sécurité dotée des processus, des politiques, de l'architecture et de l'expertise de sécurité qu'il lui faut. L'intervention de consultants externes peut s'avérer très utile pour évoluer vers une stratégie de sécurité complète. Notre méthodologie globale d'entreprise vous aidera à mieux cerner votre degré d'exposition et à prendre des décisions avisées en matière de gestion du risque.

Le rapport Risk:Value 2018 de NTT Security révèle que :

- Seuls 46 % des distributeurs pensent que toutes leurs données critiques sont en sécurité.
- 52 % n'ont mis en place aucune politique de sécurité de l'information.
- Parmi ceux doté d'une telle politique, seulement 37 % pensent que tous leurs collaborateurs en connaissent l'existence.
- L'érosion de la confiance des clients représente le problème n°1 des distributeurs en cas de violation de sécurité.
- 63 % des enseignes désignent les contractuels et les intérimaires comme le maillon faible de leur dispositif de sécurité. Et pour 36 % des personnes interrogées, la menace interne sera le premier facteur de risque de sécurité pour les 12 mois à venir.
- À l'échelle mondiale, seuls 39 % des acteurs du retail disposent d'un plan de réponse à incident (soit le pourcentage le plus faible, tous secteurs confondus).

L'entreprise NTT Security

NTT Security est la branche et centre d'excellence sécurité du groupe NTT. Nous mettons notre expertise au service des entités du groupe NTT en délivrant des solutions métiers résilientes pour accompagner leurs clients dans leur transformation numérique. Forte de ses 10 centres opérationnels de sécurité (SOC), ses 7 centres de R&D et plus de 1 500 experts en sécurité, NTT Security intervient chaque année sur des centaines de milliers d'incidents à travers six continents.

Pour optimiser l'utilisation de nos ressources locales et libérer le potentiel de nos capacités mondiales, nous offrons un ensemble adapté de services de sécurité managés (MSS) mais également de conseil stratégique ou technologique aux entreprises. NTT Security fait partie intégrante du groupe NTT (Nippon Telegraph and Telephone Corporation), l'une des plus grandes entreprises de TIC au monde. Visitez **www.nttsecurity.com/fr-fr** pour en savoir plus sur NTT Security ou **www.ntt.co.jp/index_e.html** pour le groupe NTT.