Risques cachés dans la nouvelle cyberguerre, une protection grâce à la version 2013 de la norme ISO/CEI 27001

Qu'on le veuille ou non, l'information est devenue un bien essentiel dans le monde interconnecté et en pleine mutation qui est le nôtre. Il est urgent de protéger notre cyberespace, et cette question exige une attention immédiate et constante.

1. Les entreprises n'ont d'autre choix que de se protéger.

Les risques cachés menacent les entreprises et souvent, il suffit de prendre les bonnes mesures de sécurité pour décourager les pirates les plus zélés. Ces recommandations de sécurité pour s'en prémunir, ce retrouve dans la norme ISO/CEI 27001, qui constitue notre première ligne de défense.

Les cybercriminels demeurent un fléau pour les gouvernements et les entreprises du monde entier. Ils améliorent leur ciblage et leur savoir-faire et les menaces sont à la hausse. Le problème appelle une solution internationale. La norme ISO/CEI 27001, synonyme de sécurité de l'information, apporte un cadre de gestion pour l'évaluation et le traitement des risques, cyber-orientés ou non, qui peuvent porter préjudice aux entreprises et aux gouvernements, voire endommager la trame de l'infrastructure nationale d'un pays. Elle a connu un succès remarquable dans le monde économique, en apportant une protection et des avantages aux organisations dans tous les secteurs, indépendamment de la taille et de la nature de leurs activités.

À l'heure où les cybercriminels accentuent leur pression sur les petites et grandes entreprises, les incidents de sécurité de l'information augmentent. Une étude approfondie du Department for Business, Innovation & Skills du Royaume-Uni a mis en évidence l'ampleur des menaces. L'étude – Enquête 2013 sur les violations de la sécurité de l'information (The 2013 Information Security Breaches Survey) – révèle que *les attaques contre les petites entreprises dans ce pays ont augmenté de 10 % en un an, leur coûtant jusqu'à 6 % de leur chiffre d'affaires.*

Surpris ? On le serait à moins, mais il y a plus. Les menaces sur la sécurité dans l'environnement mobile évoluent très rapidement. Les pirates informatiques mobiles sont à l'affût, coopérant avec les cybercriminels pour transmettre des informations professionnelles et privées volées. Qui plus est, ces menaces sont de plus en plus intelligentes et ciblent les appareils mobiles. Selon les rapports de CNN Hong Kong et NQ Mobile, la croissance spectaculaire des logiciels malveillants mobiles s'intensifie, avec une augmentation estimée à 163 %. Un chiffre stupéfiant.

Les voleurs d'identité ont également le vent en poupe, suggère l'enquête annuelle publiée en 2013 par la firme Javelin Strategy & Research. En 2012, le nombre des victimes de vols d'identité avait augmenté de plus d'un million (montant le plus élevé depuis 2009) et les fraudeurs avaient fait main basse sur plus de 21 milliards de dollars, le montant le plus élevé depuis 2009.

Les organisations sont toujours plus nombreuses à exploiter les possibilités qui s'offrent en ligne pour promouvoir leur entreprise et consolider leur position sur le marché grâce aux appareils mobiles et aux applications associées, sans oublier les sites de réseautage social.

Ce faisant, ces entreprises amplifient le nombre et la sophistication des menaces dont elles font l'objet. Aujourd'hui, les entreprises n'ont d'autre choix que de se protéger en mettant en œuvre la norme ISO/CEI 27001.

2. Témoignages

2.1. Entre boom et débâcle

La cybersécurité n'est pas seulement un défi informatique, elle est essentielle pour le fonctionnement de toute entreprise.

Selon Prinya Hom-anek, président d'ACIS (Thaïlande), on ne saurait trop souligner les avantages d'un cadre de gestion des risques : « Pour s'attaquer au problème, nous devons disposer non seulement de solutions techniques plus robustes, mais aussi de solutions de gestion pour améliorer les processus permettant de gérer les risques sur la confidentialité, l'intégrité et la disponibilité des informations et, surtout, pour mieux sensibiliser le personnel et les usagers et les rendre plus aptes à assurer cette protection ».Il ajoute : « ISO/CEI 27001 [...] nous a aidés à améliorer nos défenses contre les cyberattaques et donc la sécurité dans les services offerts à nos clients, qui nous font ainsi davantage confiance en tant que partenaire commercial sûr. »

Les attaques pénalisent beaucoup les marchés en ligne en compromettant les transactions électroniques et en infligeant des dégâts coûteux.

Pour José Renato Hopf, de Getnet, fournisseur de solutions technologiques gérées et de services commerciaux pour les transactions électroniques en Amérique latine, il est important pour les entreprises de conserver de l'avance dans le jeu de la cybersécurité : « Getnet a décidé de mettre en œuvre un système de management de sécurité de l'information (SMSI) efficace, fondé sur la norme ISO 27001:2013, pour protéger son centre de données situé à Campo Bom, Rio Grande do Sul (Brésil), contre les menaces et les vulnérabilités, et préserver la confidentialité, l'intégrité et la disponibilité de ses informations. Offrant les meilleures pratiques de sécurité de l'information [...], ISO 27001:2013 augmentera la confiance de nos clients, partenaires et autres parties intéressées. »

2.2. Un facilitateur de marché

Les organisations qui gèrent leurs risques de sécurité de l'information à travers la certification ISO/CEI 27001 marquent des points sur le marché.

Tony Plummer, de Stralfors UK (Royaume-Uni), explique comment cette norme établit la crédibilité et permet à l'entreprise de se différencier de ses concurrents. « Pour la grande majorité des clients existants et potentiels, la certification ISO/CEI 27001 est un prérequis. Pour le dire simplement, notre qualification ISO/CEI 27001 nous confère un droit d'entrée. Nous en voulons pour preuve le fait que la certification est obligatoire pour les organisations qui, comme Stralfors, impriment ou personnalisent les chèques. Elle a manifestement amélioré notre approche de tous les aspects de la sécurité informatique et de la sécurité

physique. De plus, elle facilite la sensibilisation du personnel et la sélection et la gestion des fournisseurs. »

3. Une arme de choix

Utilisée au niveau international depuis 2005, ISO/CEI 27001 a aidé des milliers d'organisations à renforcer leur sécurité de l'information. Cette norme de système de management très appréciée, récemment mise à jour, est maintenant disponible dans une version nouvelle et améliorée : ISO/CEI 27001:2013. Cette deuxième édition prend en compte l'expérience des utilisateurs et l'amélioration des contrôles de sécurité pour l'environnement informatique d'aujourd'hui, menacé par le vol d'identité, les risques liés aux appareils mobiles et d'autres vulnérabilités en ligne. Elle est alignée sur d'autres normes de systèmes de management.

ISO/CEI 27001 est désormais synonyme de sécurité de l'information. Elle a connu un succès remarquable dans le monde économique, en apportant une protection et des avantages aux organisations dans tous les secteurs, indépendamment de la taille et de la nature de l'entreprise. Les entreprises interrogées ci-dessus ne sont que la pointe de l'iceberg. Des milliers d'organisations dans le monde utilisent la norme ISO/CEI 27001 pour gérer leurs risques de sécurité de l'information. Dans un monde de plus en plus en proie aux cyberattaques et autres menaces, le contraire serait impensable.

R. Cox
PME Cert SA

Source : iso.org
Suite sur les normes 27000 dans la prochaine revue