PECB

When Recognition Matters

L'IMPORTANCE DE LA SÉCURITÉ DE L'INFORMATION DES NOS JOURS

De nos jours, vivre sans accès à l'information d'intérêt, à tout moment et dans chaque lieu à travers d'innombrables types d'appareils, est inconcevable. Cependant, sa sécurité est devenue plus importante que l'accès à l'information même. En fait aujourd'hui la sécurité de l'information gouverne le monde… ! Pourquoi ?

Au moment du réveil, la première chose que nous faisions et de vérifier notre téléphone. Pendant qu'on le connecte à internet, nous recherchons des informations, nous allons dans les réseaux sociaux, les services bancaires, nous effectuons des achats ou d'autres fonctions en ligne. Nous n'éteignons pas les ordinateurs portables où sont enregistrées des données sensibles, comme des documents, des photos personnelles, des courriels, des conversations, des numéros importants et de nombreux autres éléments d'informations.

Puis, sur le chemin du travail, nous sommes accompagnés par des téléphones intelligents et, tout le long de la route, nous essayons de rester connecté, recherchons du wifi, ainsi, nos téléphones peuvent devenir accessibles pour des milliers d'autres personnes qui utilisent le même réseau. Ensuite, peut-être que nous nous arrêtons pour le petit déjeuner, pour acheter un billet de bus, ou payer pour le stationnement, tout au long nous utilisons notre carte de crédit, qui contient également des informations importantes à propos de nous-mêmes.
Une fois arrivé au travail, dans certaines entreprises, où malgré nos informations sensibles qui sont sauvegardées, il y aussi les résultats financiers de l'entreprise, les plans commerciaux confidentiels des années à venir, les secrets commerciaux, la recherche et d'autres informations qui donnent à l'entreprise un avantage concurrentiel.

Tout cela est possible grâce aux grandes améliorations qui ont eu lieu dans le secteur de la technologie, dans les dernières décennies. Pourtant, dernièrement, nous entendons moins parler des innovations concernant le stockage, l'utilisation, les informations traitées par voie électronique et par transmission, que de l'accès non autorisé, des cyber-attaques, du piratage, de la violation de la vie privée etc. Ce phénomène ne réside pas que dans les cas individuels, les sociétés ou les entreprises, ces préoccupations augmentent et les résultats causent des problèmes qui deviennent pertinents au niveau du pays, du gouvernement et des institutions internationales.

Les concepts les plus entendus sont : piratage, virus, vers, cheval de Troie, usurpation d'adresse, le renifleur, le refus de services, le logiciel espion, le logiciel malveillant, les portables malveillants, la crypto virologie etc. Leurs dommages peuvent être terribles, car en profitant des lacunes de la sécurité, les attaquants accèdent à un système informatique à l'insu du propriétaire, rendant le système informatique défectueux et changeant la source /la destination de l'adresse IP pour faire croire qu'elle provient d'une source légitime, mais en réalité, il peut provenir par piratage informatique qui a accès à toutes les infos à travers le réseau sans fil et fait ainsi tomber le réseau ciblé, refuse le service aux utilisateurs légitimes etc.

Pour régler la résistance de ces actions, les agents de la sécurité de l'information ont développé des systèmes pour protéger l'information, avec des concepts tels que : anti-virus, anti-spyware, logiciels, Windows et des applications pare-feu, filtrage du contenu /contrôle parental, les codes de déchiffrement intelligent et les techniques, les méthodes et les conseils pour la sécurité de l'information.

Cette guerre entre les professionnels et les attaquants de la sécurité continue car, en même temps que la technologie assure la sécurité de l'information, elle est également mise en danger. C'est un fait compréhensible, car même si le progrès technologique est réalisé, ces progrès faits par l'homme sont de nouveau en danger car le dommage sera causé par d'autres hommes.

Management de la sécurité de l'information

La protection de l'information ou la sécurité assurée n'est pas seulement un problème de la technologie. Maintenant une plus grande importance est apportée aux actions, aux plans, aux politiques, aux sensibilisations des entreprises, des organismes ou des personnes engagés dans la protection de l'information. «La sécurité de l'information ne constitue plus un problème des TI, c'est un problème de l'entreprise. »

Les systèmes de management entiers dans les organismes et les entreprises sont maintenant en train d'apporter une attention considérable aux politiques, aux objectifs prouvés, aux audits d'auto piratage, aux formations et aux activités de sensibilisation.

En outre, la conformité avec les exigences légales et réglementaires pour la sécurité et la vie privée est devenue un facteur important afin d'assurer la sécurité de l'information. L'une des principales exigences en cela est l'appréciation du risque et son évaluation. Les questions relatives à l'information des clients et du personnel, la sécurité de l'information et les actions privées sont devenues l'un des sujets les plus importants. Pour démontrer le respect envers les clients et atteindre une crédibilité concernant la sécurité de l'information, les organismes doivent assurer les clients que leur information est en sécurité.

Toutefois, tenir compte de ces caractéristiques, ces règles, ces stratégies et ces meilleures pratiques dans un système de management n'est pas une tâche facile, mais beaucoup de normes sont devenues un langage commun parmi les utilisateurs de l'information. Une des plus importantes est l'Organisation Internationale de la normalisation qui possède un certain nombre de normes sur la façon de gérer la sécurité de l'information.

Les plus importantes sont : ISO/IEC 27001 Système de Management de la Sécurité de l'Information, ISO/IEC 15408, Critères d'évaluation pour la sécurité des TI, ISO/IEC 13335, Management de la sécurité des TI pour le contrôle de la sécurité technique, ISO 29100 Cadre privé, ISO 80001 Management du risque des réseaux des TI contenant les dispositifs médicaux etc.

Un grand nombre de normes ISO, concernant la sécurité de l'information et une fois de plus à prouver l'importance de ce sujet.

Conclusion

L'information est devenue l'atout le plus important dont une personne, un organisme ou une société a besoin et sa sécurité est celle qui nous rend plus compétent dans ce que nous faisons, c'est pourquoi la sécurité de l'information sera toujours le but premier.

Pour atteindre un niveau élevé de la sécurité de l'information, un organisme doit assurer la coopération de tous les genres de niveaux y compris l'utilisation de l'information qui signifie la réunification de toutes les parties à l'intérieur et à l'extérieur de l'organisme. De plus, dans les systèmes de la sécurité de l'information la sécurité doit faire partie de l'implication continue sur le plus haut niveau de la gestion organisationnelle dans sa conception, sa planification et sa mise en œuvre. Par conséquent, les conformités de la sécurité de l'information doivent faire partie des responsabilités quotidiennes et le personnel certifié est plus que nécessaire.

Le PECB (Professional Evaluation and Certification Board) est un organisme de certification du personnel pour une large gamme de normes professionnelles. Il offre des services de formation et de certification ISO 27001, ISO 29100 et ISO 20000 pour les professionnels qui souhaitent soutenir un organisme dans la mise en œuvre de ces systèmes de management.

Les formations ISO et professionnelles organisées par le PECB sont :
• Certified Lead Implementer (5 jours)
• Certified Lead Auditor (5 jours)
• Certified Foundation (2 jours)
• ISO Introduction (1 jour)

Lead Auditor, Lead Implementer et Master sont les programmes de certification accrédités par l'ANSI ISO/IEC 17024.

Rreze Halili est la gestionnaire du produit de la technologie, de la sécurité et de la continuité (TSC) au PECB. Elle est chargée du développement et du maintien des cours de formation de la TSC.
Pour toute question n'hésitez pas à la contacter à l'adresse : tsc@pecb.com.

Pour plus d'informations veuillez visiter le site : http://pecb.com/site/renderPage?param=139