Résoudre les problèmes de mise en œuvre des normes avec un SGSI mondial

Il existe une multitude de normes ou de cadres de sécurité de l'information destinés à aider les entreprises à sécuriser leurs données et leurs opérations. La mise en œuvre de ces normes implique de lire non seulement les exigences des normes elles-mêmes, mais aussi les guides de mise en œuvre qui les accompagnent et une myriade de documents en ligne concernant les défis à relever. Cela devient plus difficile si une entreprise doit s'aligner sur plus d'une norme en raison de son empreinte mondiale. La solution est un système global de gestion de la sécurité de l'information (SGSI) qui répond à une combinaison d'exigences provenant de plusieurs normes.

SARANTOS KEFALAS | CISA, CISM, CCSP, CISSP, ISO 27001 LI

Directeur risque et conformité de la sécurité de l'information du Groupe Infosec chez Webhelp et responsable du maintien de son système de gestion de la sécurité de l'information (SGSI) au niveau mondial. Auparavant, il a occupé des fonctions d'audit et de conseil chez PricewaterhouseCoopers (PwC) en Grèce et au Royaume-Uni, travaillant sur la sécurité de l'information et la cybersécurité, principalement dans le secteur des services financiers, du transport maritime et des télécommunications. Il affiche plus de 10 ans d'expérience dans le domaine de la sécurité de l'information, notamment dans la formation et l'encadrement de jeunes professionnels et d'étudiants. M. Kefalas est membre de l'ISACA® et d'autres organisations professionnelles.

SGSI

Le SGSI a été introduit par l'Organisation internationale de normalisation/Commission électrotechnique internationale (ISO/IEC) 27001, qui stipule que :

> *[L]'établissement et la mise en œuvre du système de gestion de la sécurité de l'information d'une organisation sont influencés par les besoins et les objectifs de l'organisation, les exigences en matière de sécurité, les processus organisationnels utilisés, ainsi que par la taille et la structure de l'organisation.*[1]

Cela signifie que, pour une entreprise mondiale, le SGSI doit couvrir toutes les exigences internes et externes au niveau mondial et au niveau local, tout en veillant à ce qu'il couvre également les opérations critiques et qu'il suive la structure de gouvernance de l'entreprise.

L'alignement du SGSI d'une entreprise internationale sur plusieurs normes et la certification de la conformité à ces normes sont devenus nécessaires parce que les entreprises ont des parties intéressées dans le monde entier, chacune d'entre elles pouvant reconnaître des cadres de sécurité différents. Les exigences légales et réglementaires de chaque pays peuvent également imposer à une entreprise de s'aligner sur une combinaison de normes, rendant les obstacles locaux inévitables.

Lorsqu'une entreprise fait l'effort de s'aligner sur des normes mondialement reconnues et qu'elle peut le prouver, la confiance des tiers s'en trouve renforcée, ce qui peut déboucher sur un accroissement de ses activités. Comme le souligne Ivan Milenkovic, Responsable de la sécurité de l'information du groupe (GCISO) de Webhelp, « la mise en œuvre d'un SGSI présente de multiples avantages : Il constitue une « invitation à la fête » avec les clients, représente la base du langage commun et témoigne de la volonté d'améliorer constamment la culture d'entreprise. D'une part, les clients comprennent ce qu'ils obtiennent ; d'autre part, nous brisons le cercle vicieux des questionnaires et des audits. »

Mise en œuvre d'un SGSI mondial

Une fois que les exigences globales d'une entreprise en matière de SGSI ont été identifiées, que les normes ont été sélectionnées, qu'une équipe d'experts a été engagée et que la direction de l'entreprise est d'accord, la mise en œuvre peut commencer.

Dans la plupart des cas, sinon tous, il existe plus d'une façon de mettre en œuvre une mesure (c'est-à-dire un contrôle) pour atteindre un objectif de sécurité. Les exigences standard ont toujours un objectif ultime de sécurité à atteindre, quel que soit leur degré de prescription. C'est pourquoi il est judicieux d'élaborer un ensemble de mesures de référence adaptées à l'entreprise et pouvant couvrir des objectifs relevant de plusieurs normes. Si cette base est accompagnée d'un moyen de mise en correspondance avec chaque norme, ainsi que d'une justification de la raison et de la manière dont les mesures de base répondent aux exigences de la norme, cela permet de s'assurer que rien n'a été oublié.

Certification d'un SGSI mondial

Une fois que la base du SGSI mondial a été mise en œuvre, l'étape suivante est la certification. Le SGSI ne peut généralement être certifié que pour une seule norme à la fois et, dans la plupart des cas, pour un seul pays à la fois. Bien que le SGSI réponde à un certain nombre d'exigences, il faut démontrer qu'il est conforme à chaque norme spécifique. Pour cela, il faut des experts en sécurité de l'information ayant une connaissance pratique des normes pertinentes, qui peuvent lancer un programme avec une feuille de route qui comprend :

- Stratégie de l'entreprise
- Exigences du client
- Objectifs de sécurité de l'information
- Spécificités du pays
- Autres exigences de conformité interne

Ces exigences doivent être équilibrées et respectées dans des délais précis. Des changements inattendus peuvent également survenir au cours du processus de certification, notamment :

- Nouvelles exigences de la part de clients potentiels ou existants
- Extension du champ d'application en raison de la croissance de l'entreprise dans de nouveaux pays ou de nouveaux sites dans des pays existants
- Acquisition d'une entreprise à inclure dans le périmètre de certification
- Nouvelles réglementations dans un ou plusieurs pays
- Indisponibilité imprévue des ressources
- Nouvelles versions d'une norme

> Les auditeurs doivent être utilisés comme des facilitateurs et leurs conseils doivent être pris comme s'ils étaient des consultants.

Cela peut sembler une entreprise impossible, mais ce n'est pas le cas.

La certification dans un nouveau pays où l'entreprise opère est beaucoup plus facile (en supposant qu'il existe des ressources locales en matière de sécurité de l'information) si elle dispose d'un plan décrivant les étapes nécessaires pour obtenir la certification pour chaque norme en utilisant la base de référence élaborée précédemment. Pour garantir l'efficacité, le plan d'action devrait comprendre les éléments suivants :

- Les étapes de la certification exprimées en langage clair, y compris les mesures à prendre pour mettre en œuvre le référentiel.
- L'estimation de l'effort nécessaire pour la mise en œuvre de chaque étape.
- Le propriétaire prévu.
- Des ressources internes utiles, telles que des politiques, des normes, des procédures, des cadres ou des modèles élaborés à l'échelle mondiale et permettant une normalisation dans différents pays.

À ce stade, l'entreprise devrait disposer d'une base de référence qui couvre toutes les normes pertinentes et d'un plan d'action pour obtenir la certification pour chacune de ces normes.

Choisir un organisme de certification et des auditeurs de certification

Une entreprise internationale doit choisir un organisme de certification mondial capable de prendre en charge tous les pays dans lesquels elle souhaite obtenir une certification. L'auditeur principal chargé du compte d'une entreprise doit examiner la base de référence et le plan d'action pour la certification concernée afin de confirmer l'acceptation de l'approche choisie, avant même le début de l'audit.

Les auditeurs de certification jouent un rôle extrêmement important. L'expérience a montré que chaque auditeur est différent. Bien que tous les représentants locaux de l'organisme de certification respectent les mêmes exigences et lignes directrices, ils peuvent se concentrer sur des domaines différents

en fonction de leur expérience. Il est probable que certaines questions identifiées dans un pays en raison de l'attention particulière portée par un auditeur existent également dans d'autres pays, même si elles n'ont pas été mentionnées. Ceci est extrêmement utile pour améliorer la posture de sécurité globale d'une entreprise et pour obtenir le soutien nécessaire au changement. Les auditeurs doivent être utilisés comme des facilitateurs et leurs conseils doivent être pris comme s'ils étaient des consultants. L'ouverture et l'honnêteté des deux parties peuvent être la clé d'une certification réussie.

Pour la plupart des entreprises, il est plus difficile de maintenir le SGSI certifié et la base de référence correspondante que de les développer au départ.

Enfin, il faut être conscient des éventuelles barrières linguistiques avec les auditeurs locaux. Déterminez à l'avance si l'auditeur désigné parle couramment la langue officielle de l'entreprise et quelle langue sera utilisée pour chaque pays afin d'assurer le bon déroulement de l'audit.

La certification est-elle synonyme de sécurité ?

L'obtention de la certification d'un SGSI global signifie beaucoup de choses, mais cela ne signifie pas que la sécurité de l'entreprise ne peut pas être violée. Cela signifie que certaines opérations de l'entreprise suivent une approche cohérente et normalisée, ce qui permet de mettre en place des mesures de prévention et de détection plus efficaces et plus matures en matière de sécurité de l'information. Cela signifie que les facteurs de risque et les incidents liés à la sécurité de l'information peuvent être identifiés plus rapidement et traités selon des lignes directrices globales conformes aux bonnes pratiques. Toutefois, des améliorations sont toujours possibles, comme en témoignent les conclusions de l'audit de certification.

La certification rend-elle l'entreprise plus sûre ? Indirectement, oui. Toutefois, il faut se plonger dans les détails d'un rapport d'audit de certification pour comprendre quelles mesures préventives et curatives permettent d'améliorer le niveau de sécurité.

Maintenir un SGSI mondial

La certification d'un SGSI n'est pas un exercice unique. Pour la plupart des entreprises, il est plus difficile de maintenir le SGSI certifié et la base de référence correspondante que de les développer au départ. Des efforts continus sont nécessaires pour s'en assurer :

- Strict respect des exigences normatives.
- Gestion des menaces pesant sur la sécurité de l'information.
- Les processus de sécurité de l'information sont intégrés et les exceptions potentielles sont documentées, contrôlées et attestées périodiquement.
- Les performances du SGSI sont évaluées et font l'objet d'un rapport.
- Tous les employés (internes et externes) sont formés.
- La documentation est revue et mise à jour.
- La posture de sécurité est améliorée.

Conclusion

Se conformer aux exigences internes et externes en matière de sécurité de l'information pour une entreprise mondiale n'est pas une mince affaire. Pour qu'un système de sécurité de l'information fonctionne au mieux, il faut du temps et des ressources humaines et technologiques. Pour que la conformité soit efficace et effective, toutes ces exigences doivent être combinées, des bases de référence doivent être établies et un SGSI global doit être développé. L'introduction de plans d'action peut s'avérer très utile pour garantir la certification du SGSI en fonction de normes et de cadres mondialement acceptés, de sorte que l'entreprise montre aux parties intéressées qu'elle prend la sécurité de l'information au sérieux et qu'elle se conforme à leurs exigences multidimensionnelles.

Bibliographie

1 Organisation internationale de normalisation (ISO)/Commission électrotechnique internationale (IEC), ISO/IEC 27001:2013 *Technologies de l'information-Techniques de sécurité-Systèmes de gestion de la sécurité de l'information-Exigences, 2ème*nd *Édition*, Suisse, 2013, *https://www.iso.org/obp/ui/iso:std:iso-icc:27001:ed-2:v1:en*