Des organismes à l’abri des cyber-attaques grâce à une panoplie de normes sur la sécurité

	*Des organismes à l’abri des cyber-attaques grâce à une panoplie de normes sur la sécurité*

Les cyber-attaques sont l'un des plus grands risques auxquels les organismes sont confrontés. Dans le monde numérique d'aujourd'hui, le besoin de normes et de systèmes pour protéger la sécurité des informations n'a jamais été aussi important. C'est pourquoi la famille de normes ISO/IEC 27000 sur les techniques de sécurité relatives aux technologies de l'information a été mise à jour, afin d'offrir aux organismes cette valeur ajoutée et ce surcroît de confiance.

Il ressort d'une étude mondiale menée par l'ISACA dans 129 pays, que seuls 38 % des organismes interrogés estiment être préparés à une cyber-attaque – même si 83 % d'entre eux sont malgré tout conscients que ce type d'intrusion constitue l'une des trois principales menaces pesant sur les organismes à l'heure actuelle. Compte tenu du volume de données personnelles et sensibles traitées électroniquement, il y a beaucoup à perdre en cas d'atteinte à la sécurité.

Le professeur Edward Humphreys, Animateur du groupe de travail de l'ISO chargé de l'élaboration des normes de systèmes de management de la sécurité des informations (SMSI) souligne que, « Pour garantir la sécurité dans le paysage numérique actuel, tous les organismes, quelle que soit leur taille, devraient mettre en place un cadre de management, à titre de préalable, pour gérer leurs cyber-risques.

La norme ISO/IEC 27001 a été précisément conçue à cette fin. Cette norme fait figure de « langage commun » universel pour apprécier, traiter et gérer les risques de sécurité des informations. »

Les toutes dernières révisions et adjonctions à la famille de normes ISO/IEC 27000 présentées ci-dessous ont été publiées en 2015. Elles font partie de la « boîte à outils » ISO/IEC 27000 destinée à la maîtrise des cyber-risques.

Protéger les informations dans le Cloud (ISO/IEC 27017)

Un nouveau code pratique pour les contrôles de sécurité de l'information pour les services du nuage, ISO/IEC 27017, vient d'être publié. Le nuage, ou Cloud en anglais, est l'une des innovations les plus largement utilisées dans le monde trépidant du commerce et des affaires d'aujourd'hui. À mesure que ce service se généralise, les utilisateurs exigent des garanties quant à la sécurité du stockage et du traitement des données dans le Cloud.

Le marché des services de Cloud, par définition mondial, est caractérisé par la dispersion des fournisseurs sur de vastes secteurs géographiques et par le transfert régulier des données d'un pays à l'autre. Il est donc essentiel de pouvoir s'appuyer sur des directives internationales.

Selon Satoru Yamasaki, l'un des rédacteurs qui a travaillé sur la norme, « ISO/IEC 27017 aidera les fournisseurs de services à trouver un terrain d'entente avec leurs clients quant à l'adéquation des contrôles de sécurité et leurs recommandations de mise en œuvre.

Cette Norme internationale relative aux contrôles de sécurité pour le Cloud facilitera le développement et l'expansion de systèmes informatiques en nuage plus sûrs ».

Ces nouvelles lignes directrices sont le fruit d'une initiative commune des principales organisations élaboratrices de normes internationales – l'IEC, l'ISO, et l'UIT – afin de garantir un rayonnement maximal.

Des solutions intégrées pour les services (ISO/IEC 27013)

Un nombre croissant d'organismes choisissent de combiner leur système de management de la sécurité de l'information (ISO/IEC 27001) et leur système de management des services (ISO/IEC 20000-1). Un système intégré implique que l'organisme peut gérer efficacement la qualité de ses services, les retours d'information de ses clients et résoudre les problèmes tout en préservant la sécurité de ses données.

ISO/IEC 27013 propose une approche systématique pour faciliter l'intégration d'un système de management de la sécurité de l'information avec un système de management des services, ce qui permet de réduire les frais de mise en œuvre et d'éviter les activités à double, dans la mesure où un seul audit, au lieu de deux, est nécessaire pour l'obtention de la certification.

Communications intersectorielles et interorganisationnelles (ISO/IEC 27010)

Comment des organismes qui s'échangent des informations peuvent-ils s'assurer que leurs données sont protégées ? ISO/IEC 27010 est un complément sectoriel à la boîte à outils ISO/IEC 27000, qui établit des lignes directrices pour l'introduction, la mise en œuvre, la mise à jour et l'amélioration de la sécurité de l'information des communications intersectorielles et interorganisationnelles. Elle comprend des principes généraux sur les moyens à mettre en œuvre pour respecter les exigences spécifiées, en s'appuyant sur des méthodes de messagerie et d'autres techniques établies. Cette norme devrait encourager l'essor de communautés de partage d'informations à l'échelle mondiale.

Comme l'explique M. Mike Nash, l'un des rédacteurs de la norme, « ISO/IEC 27010 permet fondamentalement d'adapter et d'appliquer ISO/IEC 27001 et ISO/IEC 27002 aux communications entre organismes. La mise en place de cette norme leur apporte un surcroît de confiance dans le fait que les informations qu'ils partagent avec un autre organisme ne seront pas divulguées involontairement. » Cette norme est particulièrement pertinente pour la protection d'une infrastructure nationale cruciale, lorsque le partage sécurisé d'informations sensibles est primordial. Elle est aussi largement utilisée par les équipes chargées de réagir en cas d'incidents liés à la sécurité.

Détection et prévention des cyber-attaques (ISO/IEC 27039)

Comment un organisme peut-il détecter et prévenir une cyber-intrusion dans son réseau, ses systèmes ou ses applications ? Au vu des meilleures pratiques en la matière, un organisme devrait être capable de savoir si, quand et comment une intrusion est susceptible de se produire. Il devrait également être prêt à identifier quelle faille a été exploitée et quels contrôles devraient être mis en place pour que ce type d'incident ne se réitère pas. Il peut, pour ce faire, recourir à un système de détection et de prévention d'intrusion (IDPS).

ISO/IEC 27039 établit les lignes directrices relatives à la préparation et à la mise en place d'un IDPS, et couvre des aspects essentiels tels que la sélection, le déploiement et les opérations. Cette norme est particulièrement utile sur le marché actuel où un nombre important de produits et services IDPS basés sur différentes technologies et approches sont proposés, qu'ils soient commercialisés ou disponibles en source ouverte. ISO/IEC 27039 permet de guider les organismes tout au long du processus.

Audit et certification (ISO/IEC 27006)

De plus en plus d'organismes s'en remettent aux audits de certification par tierce partie pour démontrer qu'ils ont mis en place un système de management de la sécurité de l'information (SMSI) fiable, en conformité avec les exigences d'ISO/IEC 27001. ISO/IEC 27006 établit les exigences que les organismes procédant à l'audit et à la certification doivent remplir pour être accrédités, afin d'être en mesure d'offrir des services de certification selon ISO/IEC 27001.

« ISO/IEC 27006 est une référence en matière d'accréditation pour les organismes de certification qui proposent des services relatifs à ISO/IEC 27001 » explique M. Humphreys, qui ajoute que « cet aspect est important car l'accréditation des organismes de certification est un gage de confiance supplémentaire dans le processus d'audit, qui renforce la crédibilité du certificat qu'ils octroient ».

Réagissez à cet article

Source : *Des organismes à l'abri des cyber-attaques grâce à une boîte à outils de normes sur la sécurité (2015-12-17) – ISO*