Tribune de Genève

24 heures

La «confiance» et la «sécurité» ne devraient jamais être considérées uniquement comme des options

ISACA, l'Association internationale pour la gouvernance des systèmes d'information, soutient les entreprises dans la lutte contre les cyberattaques.

INTERVIEW **SMA**

Internet est un outil essentiel pour la plupart des entreprises. Malheureusement, il n'offre pas que des opportunités, mais crée également des vulnérabilités potentielles facilitant les cyberattaques, en particulier envers les petites et moyennes entreprises (PME). ISACA aide les entreprises à lutter contre cette tendance. Jeff Primus, expert en sécurité et membre du comité directeur du chapitre ISACA Suisse et Lead ISACA Suisse romande, nous en dit davantage à ce sujet.

Aujourd'hui personne ne conteste l'importance de la cybersécurité. Selon vous, Jeff Primus, que signifie exactement la notion de «cybersécurité» pour les PME?
Tout d'abord, nous devons examiner le contexte dans lequel évoluent actuellement les entreprises. Amplifiées par l'accélération des changements mondiaux, les cybermenaces se diffusent rapidement et ont un impact considérable dans le monde entier, avec un effet majeur sur la Suisse, plateforme clé d'échange d'information. Dans un tel contexte, les PME se doivent d'être prêtes à faire face à des perturbations majeures de leurs systèmes d'information résultant de cyberattaques. L'incapacité à activer les solutions préparées pour ce type de scénarios, susceptible d'affecter la livraison des produits et services, peut avoir des conséquences majeures sur la survie des entreprises. La discipline de «gouvernance de la cybersécurité» ne cesse donc de gagner en importance.

En quoi consiste la gouvernance de la cybersécurité?
Elle met l'accent sur la définition d'objectifs, de mesures, de rôles et de responsabilités afin d'aider à protéger les systèmes d'information, de manière à maximiser leur valeur ajoutée tout en réduisant les risques. Par exemple, dans le contexte de la pandémie de coronavirus, le télétravail est devenu la pratique la plus largement adoptée pour assurer la continuité des opérations. Les entreprises ouvrent par conséquent plus de «portes» afin de permettre le flux d'informations entre le centre de données de l'entreprise et les employés en télétravail. Ces «portes» contribuent à une hausse de la fréquence des cyberattaques qui exploitent les vulnérabilités ainsi crées. Ces attaques, remettent en question les bases de la sécurité et de la vie privée en termes de confidentialité, de protection des données, d'intégrité et de continuité des opérations. La gouvernance de la cybersécurité apporte aux entreprises un ensemble d'outils permettant de gérer l'ensemble de ces aspects.

La gouvernance de la cybersécurité devient donc l'une des bases de la continuité des opérations. Quel rôle joue la protection des données?
Selon les statistiques officielles 2019 publiées par le gouvernement suisse, 99% du pouvoir économique est basé sur les PME, ce qui fait que la majorité des entreprises sont vulnérables face aux cyberattaques. Dans le contexte de la pandémie, la convergence de la sécurité de l'information, de la protection des données et de la continuité des opérations devient un aspect incontournable pour réduire l'impact financier, opérationnel, juridique et réputationnel des cybermenaces. L'une des conditions essentielles pour la réussite d'une gouvernance convergente consiste à appliquer des cadres et des certifications bien établis comme COBIT, ISO 27001, etc. Le problème: l'implémentation de ces cadres peut s'avérer très exigeante en matière de main-d'œuvre et de coûts. Elle est à la portée des grandes entreprises, mais pas de la plupart des structures plus modestes.

La solution?
Elle repose sur une «approche d'implémentation légère». En divisant des grands cadres en parties plus petites et plus faciles à mettre en œuvre, les PME peuvent choisir un sous-ensemble de mesures qui répond le mieux à leurs besoins. Dans l'idéal, les entreprises devraient adopter la «sécurité» et la «protection des données» dès la conception pour les inscrire dans l'ADN du système d'information. Cela signifie que ces deux facteurs essentiels devraient être pris en compte dès le début du développement des applications et de l'acquisition des infrastructures. Pourtant, une des plus graves erreurs commises par de nombreuses organisations consiste à mettre en place des concepts sans incorporer ces facteurs, qui ne sont ajoutés que plus tard, comme s'il s'agissait d'options.

L'application COVID du gouvernement a relancé le débat sur la question du partage des données des utilisateurs avec les organisations. Comment peut-on gagner la confiance des utilisateurs?
Suite à des événements comme le vol des données de Swisscom en 2018, les citoyens hésitent à faire confiance aux organisations, ce qui explique la nécessité pour les entreprises de cultiver la «confiance dès la conception». Comment peuvent-elles y parvenir? En intégrant les mesures de sécurité et de protection de données tout au long du cycle de vie des applications. En appliquant ces pratiques, les applications comme SwissCovid seront plus largement adoptées. Le nouveau cursus d'ISACA permet de se former à ce type d'implémentation: «Ingénieur certifié en solutions de protection des données».

Comment fonctionne ISACA et en quoi ses services sont-ils utiles aux entreprises?
Actif en Suisse depuis plus de 30 ans, ISACA est un réseau d'experts qui souhaitent se perfectionner dans des domaines comme la gouvernance & l'audit des systèmes d'information, la cybersécurité et la gestion des risques. D'un côté, ISACA promeut le partage de connaissances et, de l'autre, elle fournit des formations et des certifications approfondies. Ces dernières sont des outils précieux pour les professionnels qui souhaitent renforcer leur expertise technique et organisationnelle.

Comment votre entreprise, ACTAGIS, aide-t-elle ses clients à mettre en pratique les principes d'ISACA?
ACTAGIS, partenaire officiel et exclusif du chapitre suisse d'ISACA en Suisse romande, propose des services de conseil et de formation. Actifs sur le marché depuis plus de 25 ans, dans la gouvernance des systèmes d'information et des domaines de cybersécurité, les consultants d'ACTAGIS offrent leur expertise aux entreprises et aux organisations afin de créer plus de valeur en réduisant les risques et les dépenses.

Plus d'informations sur *www.isaca.com* et *www.actagis.com*

Certifications

(Certified Information Systems Auditor)
CISA est la référence en matière d'audit, de contrôle, de surveillance et d'évaluation des systèmes d'information d'une organisation. Il s'agit de la certification la plus ancienne et réputée. Elle est particulièrement prisée par les auditeurs informatiques et souvent exigée à certains niveaux hiérarchiques.

(Certified in the Governance of Enterprise IT)
CGEIT, destinée aux fonctions de gouvernance de systèmes d'information, est la seule certification capable d'apporter les compétences nécessaires pour évaluer, concevoir, mettre en œuvre et gérer des systèmes de gouvernance alignés sur les objectifs de l'entreprise.

(Certified in Risk and Information Systems Control)
CRISC est destinée aux experts de la gestion du risque et apporte une expertise en matière d'identification et de gestion des risques informatiques pour les entreprises et d'implémentation et de maintenance de mesures de contrôle des systèmes d'information visant à atténuer ces risques.

(Certified Information Security Manager)
CISM apporte une expertise en gouvernance de la sécurité de l'information, du développement et de la gestion de programme, de la gestion des incidents et de la gestion des risques. Elle est destinée aux cadres qui travaillent dans le domaine de la sécurité de l'information.

Cybersecurity Nexus (CSX)
CSX-P est conçue pour les professionnels de la sécurité qui souhaitent approfondir leur expertise dans des environnements de cyberlaboratoire. Elle reste la première et la seule certification qui évalue un panel de compétences de cybersécurité reconnues au niveau mondial et couvrant cinq fonctions de sécurité: Identification, Protection, Détection, Intervention et Rétablissement.

(Certified Data Privacy Solutions Engineer)
CDPSE permet aux professionnels de la branche l'implémentation de la protection des données dès la conception des systèmes, réseaux et applications informatiques tout en intégrant les mesures adaptées aux environnements nouveaux et existants.

(Control Objectives for Information and Related Technologies)
COBIT est un outil utilisé dans le monde entier pour la gestion et l'audit des systèmes d'information. Il convient aux personnes impliquées dans les missions d'architecture et de gouvernance.

À propos de

Jeff Primus
Fondateur & CEO I Consultant Senior
Formateur officiel et accrédité ISACA, BCI, PECB

CGEIT, CRISC, CISA, CISSP, SABSA-SCF, MBCI
ISO 27001 LA+LI, 22301 LA+LI, 27005 RM, 20000 LI, 9001 LI+LA, COBIT 5
CDPSE et Délégué certifié à la protection des données - RGPD

Il possède plus de 25 ans d'expérience dans le domaine de la gouvernance des systèmes d'information, de la sécurité et de la continuité des activités, et dirige des équipes de consultants qui participent à des missions critiques pour les entreprises.

En tant qu'expert, Jeff Primus implémente des systèmes de gestion de la sécurité, de protection des données et de continuité des activités conformes aux normes ISO 27001, RGPD, ISO 22301 pour des organismes du secteur public, des entreprises multinationales et des PME en Suisse et en Europe. Il enseigne en tant que maître de conférences à l'Université Paris-Sorbonne, à l'Université de Genève et à HES-SO-Valais. Il a également écrit de nombreux articles consacrés à la sécurité

À propos d'ISACA

ISACA est l'association internationale qui réunit les spécialistes des domaines de la gouvernance et de l'audit des systèmes d'information, de la cybersécurité et de la gestion des risques. Fondée en 1969, cette organisation compte désormais plus de 140 000 membres. Le chapitre suisse a été fondé en 1988 avec le statut d'association et compte aujourd'hui plus de 1 500 membres.

Pour plus d'informations, visitez **www.isaca.ch**

30 YEARS ISACA® Switzerland Chapter