Le guide stratégique du RSSI sur la conformité

Barracuda

Le responsable de la sécurité des systèmes d'information (RSSI) est constamment confronté à de nouveaux défis. La cybersécurité relevant désormais du conseil d'administration, le RSSI doit s'adresser à ses membres dans un langage qu'ils comprennent et placer la sécurité au cœur de la stratégie de l'entreprise. Le RSSI doit également maîtriser un sujet qui attire de plus en plus l'attention : la conformité. Alors que seulement 1 à 2 % des RSSI sont formés dans le domaine de la conformité ou de la gouvernance, 85 % déclarent avoir des responsabilités en matière de gouvernance, de conformité et de gestion des risques.

La conformité décrit la capacité d'une organisation à adhérer à certaines directives, règles, réglementations ou politiques. Pour le RSSI, cela concerne les processus, les ressources et l'infrastructure informatiques et la garantie qu'ils sont sécurisés et résilients. La conformité peut faire référence à des règles internes, à des règles établies par des organisations externes avec lesquelles l'entreprise fait affaire (organismes de traitement des paiements ou de normalisation, par exemple) ou à des réglementations établies par la loi. Le non-respect de ces règles peut s'accompagner de lourdes sanctions. Voilà pourquoi il est impératif que les RSSI comprennent les risques réglementaires et la conformité : ils sont de plus en plus importants, de plus en plus complexes, et c'est leur responsabilité.

La conformité va au-delà de la sécurité

La sécurité fait partie intégrante de nombreux cadres réglementaires. Qu'il s'agisse de créer de nouveaux services, d'ouvrir de nouveaux marchés ou d'ajouter de nouvelles fonctionnalités à des services existants, la sécurité doit être considérée par les entreprises comme un élément clé dès le départ, et non comme un complément. L'Union européenne, par exemple, prévoit une série d'amendes en cas de violation du Règlement général sur la protection des données (RGPD).

Cependant, les technologies de sécurité ne garantissent pas à elles seules la conformité. La conformité est une culture, et aucun logiciel ou matériel de sécurité ne peut remplacer une culture de la conformité défaillante, mais il existe un lien. Le RSSI doit réfléchir à la manière dont la sécurité est liée à l'ensemble de l'entreprise, aux clients et à la chaîne d'approvisionnement. Les logiciels et le matériel de sécurité peuvent garantir que les mesures adéquates sont prises, tandis que la formation et l'éducation développent un état d'esprit favorable à la conformité. Les RSSI doivent contribuer à bâtir cette culture avec l'adhésion de la haute direction, en s'assurant que le conseil d'administration est conscient des risques posés par les hackers et la non-conformité.

Pour de nombreuses entreprises, la sécurité doit désormais être constatée, prouvée et auditée par les organismes de réglementation. Quel que soit le risque perçu ou réel, il existe un nombre croissant de règles et de réglementations liées à la sécurité qui doivent être respectées pour rester en activité.

Les sanctions (qu'elles proviennent du Bureau du commissaire à l'information (ICO) ou des organismes de réglementation financière) et les atteintes à la réputation peuvent être sévères.

De plus, la conformité, y compris la capacité de documenter cette conformité, devient plus importante que jamais. Les pressions croissantes obligent les entreprises à atteindre des objectifs environnementaux, sociaux et de gouvernance (ESG), que ce soit de la part des organismes de réglementation, des actionnaires

ou du public, ont donné lieu à de nouvelles politiques internes dans de nombreuses organisations. En plus de cela, les entreprises tendent aujourd'hui à exiger des fournisseurs et autres partenaires commerciaux qu'ils se conforment aux normes de l'entreprise. Une culture de la conformité est un argument de vente pour les partenaires et les clients potentiels. La conformité est un point fort et c'est au RSSI de la promouvoir.

Le RSSI doit faire de la conformité une priorité

Les perspectives de la cybersécurité pour 2024 du Forum économique mondial prévoient une augmentation des cyberinégalités, avec un nombre croissant d'organisations manquant de cyber-résilience. Selon le rapport, cette tendance met en danger l'écosystème cybernétique mondial, car ces organisations vulnérables, si elles sont compromises, pourraient être des passerelles vers d'autres entreprises. C'est pourquoi des politiques d'accès et d'authentification plus rigoureuses, telles que l'accès au réseau de type zero-trust (ZTNA), sont importantes, mais la réglementation l'est tout autant. Le rapport indique que 60 % des dirigeants interrogés s'accordent à dire que les réglementations en matière de cybersécurité et de confidentialité réduisent efficacement les risques pour l'écosystème de leur organisation, contre 21 % en 2022.

Un RSSI stratégique doit donc intégrer les outils et processus de sécurité de son organisation aux bonnes pratiques en matière de conformité.

Cela implique la mise en place de systèmes de sécurité robustes (protection des e-mails, firewalls, sauvegardes, par exemple) capables de protéger l'entreprise et de documenter ses activités. Le RSSI doit également chercher à mieux gérer les risques de manière globale, comme le montre le rapport du DSI de Barracuda : Guider votre entreprise face aux cyber-risques.

Pour une bonne conformité, le RSSI doit se tenir informé du paysage réglementaire dans lequel évolue l'entreprise. Une migration vers le cloud à partir d'un datacenter sur site peut sembler sans risque en termes de conformité, mais ce n'est pas forcément le cas. Selon le secteur d'activité, le pays et le type de données hébergées dans le datacenter, le passage à un fournisseur de services sur le cloud peut constituer une violation des lois sur la protection de la vie privée, des réglementations financières ou des restrictions à l'exportation.

L'automatisation des processus métier à l'aide de l'intelligence artificielle (IA) pourrait faciliter la conformité en alertant les équipes sur les risques potentiels ou même en corrigeant les erreurs. Cependant, le fonctionnement de cette IA ou sa façon de traiter les données pourraient créer d'autres obligations, telles que celles prévues par la loi de l'Union européenne sur l'intelligence artificielle.

Il est important de tenir compte du fait que le risque réglementaire peut s'étendre au-delà des frontières. Citons par exemple le RGPD, qui réglemente la confidentialité des données des citoyens de l'UE, la section 500 du NYSDFS de New York, qui réglemente les prestataires de services financiers qui opèrent dans l'État de New York, ou des organismes du secteur tels que le Conseil des normes de sécurité PCI, qui gère les normes de sécurité des paiements à l'échelle mondiale.

Tous établissent des exigences strictes en matière de conformité, et leur non-respect peut entraîner des amendes, des pénalités ou d'autres restrictions. Et nous n'avons cité que trois d'entre eux.

« Un programme de conformité éprouvé fait office de fondation solide pour défendre votre château. Il guide les équipes de sécurité, aide à identifier les lacunes et contribue à l'élaboration d'une feuille de route pour l'avenir. Une bonne fonction de conformité renforce la sécurité de l'ensemble de l'organisation et suscite la confiance des clients et des parties prenantes. Elle contribue à faire de votre entreprise une forteresse prête à affronter la prochaine attaque. »

Riaz Lakhani

CISO, Barracuda

Vers une conformité simplifiée

Un RSSI ne peut pas consacrer tout son temps à la conformité, mais il peut, avec le soutien de sa direction, créer une organisation engagée en faveur de la conformité.

La première étape pour y parvenir est la formation continue. La conformité n'est pas qu'une fonction, c'est un état d'esprit. Elle doit être développée et renforcée par l'ensemble du personnel. Les risques évoluent et la formation doit rester à jour et intéressante.

Outre la formation, l'entreprise doit également procéder régulièrement à des évaluations des risques, ainsi qu'à des audits et des évaluations de la sécurité. Faire des affaires présente toujours un certain risque. Les entreprises avisées gardent une longueur d'avance en identifiant les problèmes et en discutant avec la direction au sujet de la nature des risques et de la manière dont ils peuvent être gérés et mis en conformité. Toutefois, il est important que les évaluations et les audits ne soient pas considérés comme de simples formalités, mais comme des outils permettant d'améliorer la conformité.

Un bon RSSI facilite la mise en conformité en créant une organisation sécurisée. Les outils et processus en place permettent de documenter les activités afin d'assurer la conformité avec l'environnement réglementaire en constante évolution. Cela place également l'entreprise dans une position plus solide pour son succès futur.

Pour en savoir plus sur la manière dont les produits Barracuda peuvent vous aider à atteindre vos objectifs de conformité, veuillez nous contacter.

Barracuda

Barracuda en quelques mots

Rendre le monde plus sûr est notre objectif chez Barracuda. Nous pensons que chaque entreprise doit se doter de solutions cloud-first, faciles à acquérir, à déployer et à utiliser, tout en gardant leur niveau de sécurité. Nous protégeons les e-mails, les réseaux, les données et les applications avec des solutions innovantes et évolutives, qui s'adaptent à la croissance de nos clients. Plus de 200 000 entreprises à travers le monde font confiance à Barracuda pour les protéger – elles restent sereines face aux risques qui sont toujours là – et peuvent se concentrer sur le développement de leur business. Pour en savoir plus, rendez-vous sur fr.barracuda.com.