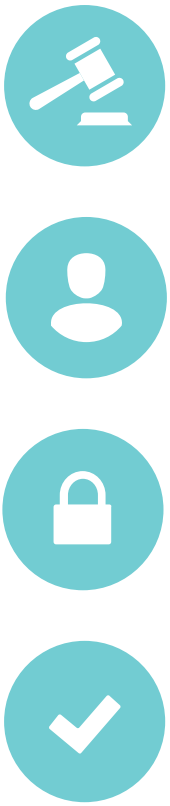
ipswitch

Secure. Control. Perform.

UN GUIDE PROFESSIONNEL IPSWITCH

Guide sur la sécurité et la conformité de l'information pour les professionnels de l'informatique

ipswitch



Introduction

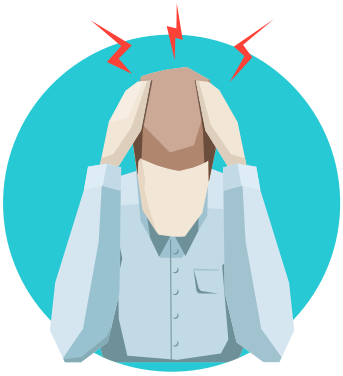
Assurer la sécurité et la conformité des réseaux informatiques est un enjeu suffisant pour faire dresser les cheveux sur la tête de tout informaticien expérimenté.

Votre équipe informatique n'a pas de temps à consacrer à des listes de contrôle complexes pour gérer chaque aspect de la conformité réglementaire. Même si les cadres dirigeants disent parfois que ces listes représentent un mal nécessaire, il est impossible de rester totalement protégé contre les failles de la sécurité.

Pourquoi ? Parce que les vecteurs des attaques des pirates ne cessent de se complexifier. Prenons le cas du ransomware (faux logiciel de décodage et de protection), par exemple. Une attaque de ransomware réussie correspond à une violation de la sécurité, souvent dirigée vers les secteurs de la santé et de la finance.

Grâce à ce livre électronique, vous bénéficierez d'une meilleure visibilité sur ce que les cadres dirigeants et les auditeurs attendent de vous, ainsi que sur les moyens de mieux vous protéger et vous préparer à affronter les menaces externes. Les points suivants sont abordés :

- Conformité aux réglementations et obligations légales
- Comment se préparer à un audit
- Être prêt à réagir à tout incident avec une équipe d'intervention de sécurité



Quelle est votre réponse ?

Si vous êtes un professionnel de l'informatique dans une industrie réglementée, vous devriez vous poser les questions suivantes :

- Mon entreprise fait-elle tout en son pouvoir pour respecter les obligations de conformité ?
- Nos utilisateurs sont-ils capables de détecter les attaques d'hameçonnage ?
- Disposons-nous d'un plan viable pour faire face aux failles de sécurité ?

Si vous avez répondu « non » à l'une de ces questions, pas de panique, vous n'êtes pas seul. La plupart des entreprises ne ménagent pas leurs efforts pour se protéger des menaces extérieures. Respecter les obligations de conformité et être prêt à subir un audit ne signifie pas que vous êtes bien armé pour contrer une attaque d'un pirate déterminé ou d'un employé mécontent.

Un bon début pour limiter les risques consiste à s'assurer que des correctifs sont régulièrement téléchargés sur l'infrastructure informatique pour la protéger des dernières vulnérabilités. Nous vous recommandons de consulter à intervalles réguliers les rapports du système d'évaluation standardisé CVSS (Common Vulnerability Scoring System) ainsi que les bulletins « Patch Tuesday » de Microsoft. Même lorsque ces précautions sont prises, la protection de l'information est une tâche sans répit et ingrate. Les correctifs ne garantissent pas une protection totale à eux seuls. Mais c'est un début.

Conformité aux réglementations et obligations légales

Les législateurs connaissent depuis longtemps les risques associés à des transferts de données mal gérés. Leurs attentes augmentent dans la même proportion que les sanctions qu'ils imposent. La conformité est essentielle, quel que soit l'environnement d'entreprise (des grands groupes internationaux aux PME). À l'heure actuelle, les auditeurs interprètent les normes avec plus de cohérence et d'exigence aussi, en s'appuyant sur un ensemble de meilleures pratiques toujours plus important. Anticiper les questions que l'on vous posera au cours d'un audit, avant le début de l'audit, constitue votre meilleure carte.

De nombreuses entreprises des secteurs de la santé et de la finance ont leurs propres équipes d'audit internes chargées de préparer la venue des auditeurs de l'extérieur. Si vous cherchez à constituer un groupe interne, envisagez de recruter à la fois des auditeurs expérimentés, des juristes et des responsables informatiques (ou un éventuel sous-groupe). À tout le moins, les équipes internes doivent disposer des connaissances et ressources nécessaires pour mener des audits des pratiques en cours et identifier les carences et potentielles faiblesses.

ISO/CEI 27001/2

Les entreprises s'intéressent de plus en plus à la norme internationale ISO/CEI 27001, largement reconnue par les autorités administratives et le monde des affaires.

La section A.13.2 de la norme ISO/CEI 27001 est dédiée au transfert d'informations, et a pour objectif déclaré de garantir la protection des données transférées au sein d'une entreprise et/ou dans le cadre d'échanges avec des parties prenantes extérieures.

Plutôt qu'une spécification, cette norme est une pratique exemplaire qui peut être interprétée de manière à s'adapter aux besoins spécifiques et à l'environnement à risque de chaque entreprise. Toutefois, l'obligation de référencer la norme connexe plus complète ISO/CEI 27002 sous-tend cette interprétation.

Normes de sécurité des données des cartes bancaires (PCI DSS)

La norme PCI DSS est une exigence de conformité internationale que doivent respecter toutes les entreprises qui traitent, stockent, transmettent ou accèdent aux données de détenteurs d'une carte de crédit (s'applique aux principaux émetteurs de cartes de crédit).

Elle exige l'application de contrôles de sécurité très stricts visant à protéger les données des détenteurs de cartes de crédit, avec notamment la mise en place d'un environnement sécurisé. Cette norme est stipulée par contrat et fait souvent l'objet d'audits et de tests menés par des consultants et des prestataires agréés dans le domaine de la sécurité.

Si votre entreprise stocke des données financières telles que les numéros de carte de crédit, vous devez respecter la norme PCI.

Règlement général sur la protection des données

Les entreprises qui conservent des informations personnellement identifiables doivent adhérer à un large ensemble de réglementations existantes sur la protection des informations ; en parallèle, de nouvelles réglementations plus exigeantes sont en cours d'introduction dans des zones telles que l'Union européenne, les États-Unis et la Chine.

La Commission européenne a unifié la réglementation sur la protection des données au sein de l'Union européenne, sous l'égide du Règlement général sur la protection des données. S'agissant d'un règlement plutôt qu'une directive, il est immédiatement applicable à tous les états membres. Pas de panique cependant, le Règlement relatif à la protection des données n'entrera pas en vigueur avant le 25 mai 2018. Mais un conseil, n'attendez pas la dernière minute pour vous préparer.

La mise en œuvre du Règlement de l'UE ne représente pas le seul bouleversement à gérer ; le « Brexit » (sortie du Royaume-Uni de l'Union européenne) implique que les entreprises transférant et stockant des données au Royaume-Uni devront à la fois respecter les normes anglaises, tout en se conformant au Règlement sur la protection des données de l'UE.

Le Règlement est incisif, dans le sens où il exige la confidentialité par nature, ainsi que le droit de suppression, la notification des violations de sécurité, et la portabilité des données lorsqu'un patient ou un client souhaite obtenir une copie de ses données (un dossier médical, par exemple). Le non-respect de ce règlement a de graves répercussions, la sanction encourue pouvant représenter jusqu'à 5 % du chiffre d'affaires annuel d'une entreprise.

Loi Sarbanes-Oxley (SOX)

Dans un monde qui a subi l'impact de l'affaire Enron, la transparence est vitale pour les entreprises du secteur de la finance, alors que les éléments fluctuants sont nombreux. Un des facteurs importants de la conformité réglementaire, notamment par rapport à la loi Sarbanes-Oxley, consiste à savoir en permanence où sont vos données stratégiques : au repos et en transit.

Prenons l'exemple fictif d'un délit d'initiés : un employé sans scrupules communique à un ami de Wall Street des informations sur les bénéfices de son entreprise montrant une rentabilité négative deux jours avant la publication des résultats. Quels contrôles votre équipe informatique a-t-elle mis en place pour identifier et limiter les risques pour la sécurité de ce type ? Comment appliquer ces contrôles sans générer de goulets d'étranglement qui entraînent des tâches manuelles fastidieuses ?

Les entreprises qui rendent comptent à la Securities and Exchange Commission (SEC) des États-Unis doivent respecter la loi Sarbanes-Oxley. La loi vise à protéger les investisseurs en améliorant la précision et la fiabilité de la communication d'informations sur et par les entreprises. Elle rend le président-directeur général et le directeur financier personnellement responsables de l'évaluation de l'efficacité des contrôles internes régissant le reporting financier.

Les conséquences de la non-observation des règles peuvent être de lourdes amendes et des peines d'emprisonnement. Leur évaluation doit être contrôlée par un cabinet d'audit indépendant. Bien qu'aucune liste de contrôles prescrits ne soit disponible, la sécurité et l'intégrité des systèmes de reporting financier sont des composants essentiels d'une évaluation aux termes de la loi Sarbanes-Oxley. Elle englobe tous les contrôles permettant de garantir que les applications fonctionnent correctement. Il existe des lois de ce type dans beaucoup d'autres pays, dont l'Australie, le Canada, la France, l'Allemagne, l'Italie, les Pays-Bas, l'Afrique du Sud, la Turquie et le Japon.

Règles de Bâle II et III

L'accord de Bâle est le dispositif international destiné aux institutions bancaires et financières. Entre autres consignes, il stipule que les banques doivent minimiser les risques opérationnels, tels que les fraudes, les pannes de système et les intrusions non autorisées, et établir des règles de gestion de l'information, des procédures et des contrôles dans un cadre formel.

Le nouvel accord Bâle III introduit un mécanisme d'évaluation et de mesure des risques plus évolué, ainsi que des règles actualisées sur la gouvernance d'entreprise et des normes de reporting.

Les sanctions pour non-respect de la conformité peuvent entraîner des amendes allant jusqu'à 10 % du chiffre d'affaires d'une entreprise et le retrait de la licence bancaire.

Health Insurance Portability and Accountability Act (HIPAA)

Les établissements de santé respectent la loi HIPAA (loi américaine sur l'assurance maladie) pour un certain nombre de raisons, notamment pour se prémunir contre les poursuites du gouvernement fédéral américain ou des poursuites au civil intentées par des patients. La loi HIPAA exige la mise en place d'un large ensemble de protections administratives, physiques et techniques. Il s'agit de procédures formelles, de responsabilités, de formations, de plans d'urgence et d'audits internes visant à protéger les données numériques confidentielles des patients. Les données de santé protégées sont constituées de toutes les informations relatives à l'état de santé, à la fourniture de soins de santé ou au paiement de soins, pouvant être reliées à un individu en particulier.

Le non-respect de la loi HIPAA peut être sanctionné par des amendes pouvant atteindre 1,5 million de dollars par an, assorties de peines d'emprisonnement d'une durée maximale de 10 ans pour des violations intentionnelles.

Le non-respect de la loi HIPAA peut être sanctionné par des amendes pouvant atteindre 1,5 million de DOLLARS par an.

Comment se préparer à un audit

Le meilleur moyen de se préparer et de se tenir prêt pour un audit est d'organiser une répétition générale en bonne et due forme. Vous souhaiterez peut-être confier votre propre audit interne à un auditeur certifié. Les équipes informatiques pourront ainsi devenir totalement opérationnelles à la lumière des problèmes à traiter détectés dans le cadre de la procédure. Généralement, les audits internes sont gérés par les membres d'une équipe dédiée à la conformité, constituée notamment de cadres dirigeants tels que le responsable de la conformité, le responsable de la sécurité, ou même le PDG s'il s'agit d'une petite entreprise. Ces responsables sont souvent les gardiens de la documentation qui prouve que votre entreprise a fait de son mieux pour respecter les obligations de conformité.

Il est important de retenir que, dans tous les cas de figure d'un audit, un membre de l'équipe informatique doit y assister pour répondre à toutes les questions éventuelles. C'est pourquoi il est crucial de mandater un auditeur interne afin de vérifier que le département informatique a tout sous contrôle avant la tenue d'un véritable audit. Il est même possible d'engager un prestataire tiers pour auditer votre entreprise.

Être prêt à réagir à tout incident avec une équipe d'intervention de sécurité

À mesure que la réglementation prend de l'ampleur, la protection des données ne peut rester l'affaire d'un seul individu ou d'une seule équipe. De nombreux pans de l'entreprise sont partie prenante dans les obligations de conformité. Une pratique exemplaire consiste à mettre en place une équipe d'intervention de sécurité composée de spécialistes de la conformité, de la sécurité et des technologies, ainsi que de responsables de tous les services. Cette équipe sera la plus qualifiée pour former les utilisateurs à éviter d'être à l'origine de violations de la sécurité.

UNE LISTE DES MEMBRES DE L'ÉQUIPE DE SÉCURITÉ

Voici une liste de collaborateurs de l'entreprise que vous devriez considérer pour intégrer l'équipe d'intervention de sécurité :

Tous les membres de l'équipe dirigeante

Ils devraient tous en faire partie. Souvent un processus de riposte en matière de sécurité peut être issu d'un document existant sur la communication de crise. Et si quelqu'un doit être poursuivi, ce sera probablement votre PDG. La plupart des cadres supérieurs font l'objet d'attaques de hameçonnage extrêmement ciblées. En clair, pour bien se préparer, il faut commencer par la tête.

L'équipe informatique

Il n'est pas étonnant que ce groupe doive maîtriser parfaitement les outils informatiques et soit informé sur toutes les dernières attaques et vulnérabilités en ligne. Comme indiqué précédemment, il est important de rester au fait des rapports tels que celui du CVSS, et de former l'utilisateur final à reconnaître les méthodes d'ingénierie sociale.

Choisissez un membre de votre équipe informatique capable de communiquer efficacement avec des personnes ayant beaucoup moins de compétences techniques. Ce communicant doit être en mesure de délivrer une représentation claire et précise de la politique, des procédures et des décisions de l'entreprise. Tout comme le PDG, le directeur informatique peut se retrouver sur la sellette si une violation de la sécurité entraîne des complications juridiques.

Responsables de la conformité et de la sécurité

Votre directeur de la conformité ou de la sécurité est responsable de la création de tous les protocoles d'entreprise en lien avec la conformité aux réglementations. De fait, il est membre de l'équipe d'intervention de sécurité, qu'il l'ait choisi ou non. Il est également le gardien de la documentation qui prouve que votre entreprise a fait tout le nécessaire pour respecter les obligations de conformité même si des cybercriminels s'introduisent dans votre réseau.

Les entités visées qui subissent une infraction affectant plus de 500 résidents d'un État ou d'une juridiction sont non seulement tenues de notifier les individus concernés, mais également d'avertir les principaux médias desservant l'État ou la juridiction. Les entités visées utiliseront probablement la voie du communiqué de presse pour notifier les médias appropriés desservant la zone concernée. Tout comme une notification à titre individuel, cette notification aux médias doit être fournie dans un délai raisonnable et, dans tous les cas, dans les 60 jours suivant la découverte d'une faille. Elle doit comprendre les informations nécessaires pour une notification individuelle.

– HIPAA, obligation de notifier les violations de données

Produit

Si vous êtes dans le commerce interentreprises (B2B), vous travaillez très probablement avec une équipe de produit car vous vendez des produits/services. L'équipe de produit bénéficie d'une expérience pratique de la technologie utilisée au sein d'une entreprise. Compte tenu du développement de la culture DevOps actuellement, les équipes de produit et informatiques doivent collaborer lorsqu'un problème survient. En fonction de l'origine d'une violation ou d'un point de défaillance de la conformité, ce sera très probablement l'équipe informatique ou l'équipe de produit qui mettra en œuvre une solution.

Marketing

Toutes les équipes d'intervention ont besoin d'un communicant expérimenté dans l'entreprise. Ces experts en relations publiques sont des gestionnaires de crise professionnels salariés du groupe chargés de contrôler tous les flux d'informations dirigés vers le monde extérieur. De nombreuses normes, dont la loi HIPAA, exigent qu'une entreprise victime d'une violation de la sécurité diffuse l'information via un communiqué de presse si plus de 500 personnes sont impactées. En ce qui concerne les failles moins graves, une notification aux personnes qui en sont affectées constitue le minimum.

La responsabilité de la sécurité et de la conformité incombe à tout le monde

Chaque membre d'une équipe intervention de sécurité doit être en mesure de comprendre son rôle et ses responsabilités par rapport à une norme donnée. Votre entreprise doit avoir établi un plan prévoyant les modalités d'un audit ou les mesures à prendre en cas de violation de la sécurité.

Savoir réagir vite et de manière efficace peut faire toute la différence au niveau du bilan de votre entreprise. C'est pourquoi il est essentiel d'organiser deux fois par an des audits internes et des exercices d'entraînement pratique. Une bonne préparation est absolument essentielle. Lorsque vous êtes victime d'une violation de la sécurité, vous n'avez simplement pas le temps d'apprendre sur le tas.

À propos d'Ipswitch

On compte aujourd'hui sur des équipes informatiques travaillant d'arrache-pied pour gérer la complexité croissante des environnements et garantir des temps d'indisponibilité proches de zéro. L'ensemble d'outils d'administration réseau Ipswitch aide ces équipes à réussir leur tâche en facilitant le contrôle sécurisé des transactions, des applications et de l'infrastructure d'entreprise. Les logiciels Ipswitch sont puissants, flexibles et faciles à tester, acheter et utiliser. Ils mettent en valeur le travail des équipes en garantissant de hauts niveaux de performance et de sécurité en continu dans les environnements de cloud, virtuels et réseau. Les logiciels de surveillance unifiée des infrastructures et des applications Ipswitch offrent une visibilité de bout en bout, sont extrêmement souples et se déploient simplement. Les solutions gérées de transfert de fichiers et de protection de l'information permettent de sécuriser et d'automatiser des transactions et des transferts de fichiers en toute conformité pour des millions d'utilisateurs. Ipswitch fonctionne sur plus de 150 000 réseaux dans 168 pays. Son siège social est situé à Lexington, dans le Massachusetts, et l'entreprise dispose de bureaux aux États-Unis, en Europe, en Asie et en Amérique latine.

Pour de plus amples renseignements, consultez le site www.ipswitch.com, ou venez nous rejoindre sur LinkedIn et Twitter.

ipswitch

Téléchargez votre version d'ÉVALUATION GRATUITE d'Ipswitch MOVEit ›