Kiteworks

Whitepaper

Maîtriser les réglementations NIS-2, DORA et autres - Mettre en place une stratégie gagnante de mise en conformité

l'introduction

Les professionnels de l'informatique et de la sécurité doivent à la fois faciliter la collaboration multiplateforme et assurer l'intégrité et la confidentialité des données de l'entreprise. De plus, les menaces informatiques sont de plus en plus complexes. Rien qu'en 2023, l'Office fédéral de la police criminelle allemande (BKA) a enregistré une augmentation significative du nombre et de la qualité des cas de cybercriminalité. Et d'après BITKOM (association pour l'industrie allemande des technologies de l'information et de la communication), les pertes financières dues à la cybercriminalité s'élèvent à 205,9 milliards d'euros.

Réponse aux cybermenaces en Europe

Ces chiffres soulignent le besoin urgent d'avoir une norme commune pour renforcer la sécurité informatique et lutter contre les cyberattaques. En réponse, l'Union européenne a introduit de nouvelles réglementations dans le cadre de sa « Décennie numérique ». Le but : s'assurer que les organisations publiques et privées soient mieux équipées pour faire face à la menace cybernétique croissante. Parmi les nouvelles réglementations, citons :

NIS-2 (directive sur la sécurité des réseaux et de l'information) : vise à renforcer la cybersécurité dans l'UE avec des mesures renforcées et des obligations de signalement. Concerne les opérateurs de services essentiels et critiques et les fournisseurs de services numériques. Elle garantit que les États membres de l'UE prennent des mesures de sécurité appropriées et signalent les incidents de sécurité.

DORA (Loi sur la résilience opérationnelle numérique) : vise à garantir que les entités financières disposent de la résilience numérique nécessaire ; capacité à réagir en cas de cyberattaques et continuité de l'activité même en cas de graves perturbations informatiques.

Loi sur la cyber-résilience : vise à harmoniser et à améliorer les exigences de sécurité pour les produits contenant des éléments numériques. Cette législation importante de l'UE a pour but d'établir des règles communes de cybersécurité tout au long du cycle de vie des produits numériques. Pour améliorer la résilience globale du matériel et des logiciels mis sur le marché européen.

Ces nouvelles mesures compliquent sérieusement la tâche des entreprises, en particulier à cause de la pénurie de compétences et de ressources IT. Les problèmes de non-conformité peuvent entraîner des sanctions importantes (allant de simples amendes à des poursuites judiciaires), nuire à l'image de marque et accroître la vulnérabilité aux cyberattaques. Soit des pertes de données et des pertes financières non négligeables.

Pour répondre aux exigences réglementaires, rien de tel qu'une approche globale et cohérente.

La conformité est un sujet de préoccupation majeure pour les entreprises, quelle que soit leur taille, qui requiert du temps et la participation de tous les collaborateurs. Une stratégie de conformité bien structurée et adaptée aux besoins des utilisateurs est la clé de la réussite.

Les clés d'une stratégie réussie

Le déploiement d'une stratégie de conformité n'est pas une opération ponctuelle, mais un processus continu dont le pilotage doit être centralisé et adapté en permanence. Elle nécessite un investissement temps et humain de tous les collaborateurs.

Pour réussir, il faut se concentrer sur les trois grands piliers : **Protéger, Suivre et Contrôler**.

Protéger les données sensibles, suivre les flux de données en toute transparence et réaliser des contrôles poussés permet d'instaurer durablement une culture de la conformité règlementaire au sein de l'entreprise.

Le plus dur est de réussir à mettre en œuvre ces principes de bonnes pratiques. Dans le passé, on utilisait plein d'outils et de systèmes de communication pour faciliter les échanges de contenus sensibles au sein d'une organisation. Finalement, cela a conduit à des solutions isolées et autonomes et à de l'informatique parallèle. Alors exit les mesures de sécurité cohérentes et le suivi du contenu.

Avec les nouvelles réglementations, en revanche, il faut être capable de prouver aux autorités compétentes que toutes les mesures de sécurité sont en place et efficaces. Que l'on a un système de gouvernance approprié pour garantir l'intégrité et la sécurité des données, et que l'on crée un environnement de travail sûr pour l'ensemble des collaborateurs.

Les données sensibles contre les accès non autorisés, le vol de données ou l'utilisation abusive, via des mesures de sécurité robustes comme le chiffrement, les pare-feux et les protocoles de sécurité.

Mettre en œuvre des procédures de suivi des transferts de données sensibles au sein de l'entreprise et avec des fournisseurs tiers. En enregistrant les flux de données, par exemple dans des journaux d'audit, il est possible de détecter les lacunes à un stade précoce et de prendre les bonnes décisions pour y remédier.

Mettre en œuvre des mécanismes de contrôle des données sensibles, qu'elles soient en transit ou au repos.

La base d'une stratégie de conformité efficace

Centraliser et unifier les systèmes de communication est une démarche qui a fait ses preuves pour améliorer la conformité règlementaire. Pour cela, il faut se doter d'une infrastructure IT robuste et mettre en place un réseau de contenu privé (PCN) central. Une fois l'environnement de travail protégé, les fichiers sensibles sont stockés, partagés et utilisés pour collaborer en toute sécurité. Cette mesure de gouvernance pose les bases saines d'une stratégie de conformité efficace.

L'infrastructure IT choisie doit fournir trois composantes essentielles :

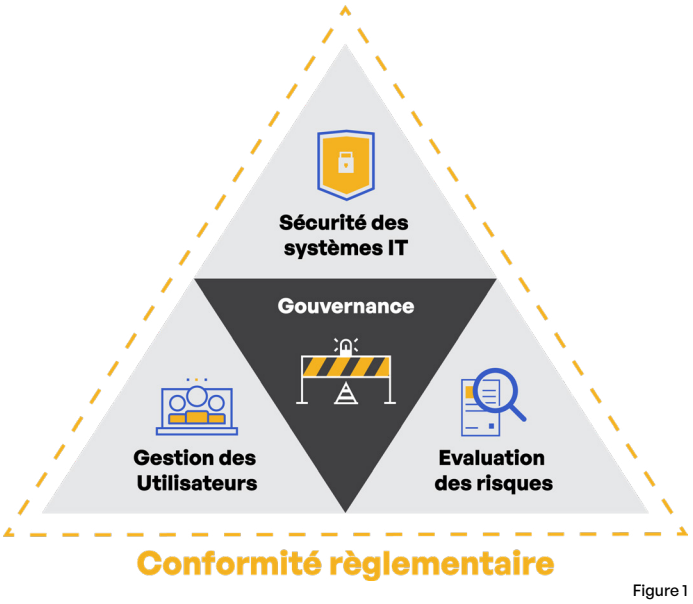

Figure 1

Sécurité des systèmes IT

Le module « Sécurité des systèmes informatiques » englobe toutes les mesures et process qui contribuent à protéger l'environnement IT contre les accès non autorisés, les pertes de données et les cyberattaques. En vertu du premier pilier « PROTÉGER », ce module consiste à instaurer des protocoles de sécurité robustes, des mécanismes de chiffrement et des contrôles d'accès. Le but étant de garantir l'intégrité, la confidentialité et la disponibilité des données.

Un réseau de contenu privé facilite et accélère considérablement la démarche. Doté de fonctionnalités de sécurité avancées (double chiffrement, mécanismes de protection multicouches avec suppression proactive des données inactives, architecture zéro trust), un PCN aide à sécuriser les systèmes informatiques de manière générale. Il protège contre les menaces, assure la confidentialité des données et permet l'échange sécurisé d'informations (via des liens de partage par exemple).

Évaluation des risques

Le module « Évaluation des risques » englobe l'identification, l'évaluation et la hiérarchisation systématiques des risques susceptibles d'affecter l'infrastructure IT d'une organisation. En vertu du deuxième pilier « SUIVRE », ce module consiste à surveiller et évaluer en continu les menaces et les vulnérabilités. Le but étant de prendre des mesures appropriées d'atténuation des risques et de comprendre la probabilité de l'impact potentiel des incidents.

Un réseau de contenu privé aide à identifier plus rapidement les vulnérabilités et à les corriger avant qu'elles ne surviennent. Parmi ses fonctionnalités de sécurité avancées, des reportings personnalisables permettent d'analyser les risques en détail et d'identifier les menaces spécifiques. Des journaux d'audit complets permettent de repérer rapidement les lacunes et d'assurer le suivi détaillé des activités et des modifications au sein des systèmes informatiques.

En intégrant les données de sécurité de l'ensemble de l'environnement IT dans un SIEM, vous pourrez surveiller les incidents de sécurité de manière centralisée et recevoir des alertes automatiques en cas de non-conformité ou de risques pour la sécurité. Cela vous aidera à détecter les menaces et les attaques, à hiérarchiser les risques et à corriger les vulnérabilités en temps voulu.

Figure 1 - Les trois composantes d'une stratégie de conformité réussie

User Management

Le module « User management » englobe tous les mesures et process qui contribuent à l'administration des comptes utilisateurs et aux droits d'accès à l'infrastructure IT. En vertu du troisième pilier « CONTRÔLER », ce module consiste à surveiller et à gérer les droits d'accès, ainsi qu'à former régulièrement tout le personnel aux enjeux de sécurité.

Un réseau de contenu privé empêche les accès non autorisés en utilisant des méthodes d'authentification sécurisées. Ainsi, seuls les utilisateurs habilités ont accès aux données sensibles. Même des identifiants de connexion volés (par exemple suite à une attaque par phishing) ne seraient pas exploitables. L'attribution de droits en fonction des rôles utilisateurs restreint encore plus l'accès aux données sensibles, puisqu'ils sont attribués en fonction des besoins de l'utilisateur (lecture/modification/suppression).

Un réseau de contenu privé fournit également un environnement de travail et un lieu de stockage sécurisé pour les données sensibles qui peuvent être consultées en temps réel depuis n'importe où. En offrant plus de flexibilité et d'efficacité aux utilisateurs, il s'intègre facilement dans la vie quotidienne.

Par ailleurs, des formations et communications régulières sensibilisent les utilisateurs aux questions de sécurité et garantissent le respect des exigences réglementaires.

Instaurer une véritable culture de la conformité

La combinaison des trois modules (Sécurité des systèmes IT, Évaluation des risques et User management) jette les bases d'une stratégie efficace en matière de respect des règles de sécurité. Choisir un fournisseur de services IT fiable épargne aux équipes IT le problème de la pénurie de compétences techniques. Un réseau de contenu privé améliore de manière significative la sécurité et l'efficacité des infrastructures informatiques sur le long terme, dans le respect des exigences légales et réglementaires.
Attention, il ne suffit pas de réunir ces éléments pour instaurer une culture de la conformité durable et performante. Il faut évidemment communiquer les uns avec les autres lorsque vous définissez votre stratégie. En effet, il s'agit de prendre les bonnes décisions et d'utiliser les bonnes fonctionnalités. Mais la seule façon d'intégrer la conformité dans la culture d'entreprise est de favoriser le dialogue. Soyez présent dans les différents services et parlez de conformité règlementaire et de tous les sujets annexes (prévention du « shadow IT » ou réduction des doublons par exemple).

Pour garantir le succès à long terme, vous devez revoir régulièrement votre politique de conformité. Examinez l'ensemble du processus, la manière dont les politiques et les procédures ont été communiquées et intégrées dans votre organisation, et évaluez objectivement leur intérêt et leur efficacité. La communication et l'engagement continus de toutes les parties prenantes, en particulier des cadres, sont décisifs. Ils servent de modèles et contribuent activement au respect et à l'engagement de leurs équipes. Ce faisant, ils soulignent l'importance de ces mesures dans l'ensemble de l'organisation.

Kiteworks

Kiteworks, un réseau de contenu privé et un partenaire de confiance

Le réseau de contenu privé de Kiteworks est votre meilleur allié pour satisfaire aux nombreuses exigences règlementaires et gagner en sécurité IT. Certifié ISO 27 001, 27 017 et 27 018, il garantit un niveau élevé de protection des données, et offre une base solide pour le contrôle total et l'intégrité des données sensibles de votre entreprise. Véritable partenaire, Kiteworks vous aide à répondre aux exigences règlementaires grâce à des mécanismes de sécurité appropriés (PROTÉGER), des outils de reportings pour surveiller et détecter rapidement les vulnérabilités (SUIVRE), et des contrôles de cyberhygiène appropriés (CONTRÔLER).

Venez tester Kiteworks ! L'essai est gratuit et sans engagement. Vous pouvez également nous contacter pour obtenir plus d'informations sur nos offres.

Essayez notre démo gratuite!

Commencer

Vous souhaitez en savoir plus sur Compliance.

En savoir plus

Kiteworks

Juin 2024

www.kiteworks.com