Kiteworks

RAPPORT DE CONFORMITÉ

Kiteworks et la directive NIS 2 réduisent les risques informatiques

Organisation de service essentiel et de vente en ligne : se conformer à la norme NIS 2 et sécuriser votre contenu

L'UE a proposé la directive NIS 2, un cadre réglementaire européen pour la gestion des risques liés aux technologies de l'information et de la communication (TIC) et des cybermenaces dans les services essentiels et la vente en ligne. Kiteworks simplifie les choses grâce à sa plateforme unique qui protège et gère les communications de contenu en toute transparence, afin d'aider les entreprises à démontrer leur conformité à la norme NIS 2.

Le projet de réglementation exigerait des entités financières qu'elles assurent la sécurité de leurs systèmes et réseaux TIC et qu'elles signalent les incidents majeurs aux autorités compétentes. La directive prévoit également une approche coordonnée à l'échelle de l'UE en matière de cybersécurité et de réponse aux incidents, les autorités nationales compétentes étant chargées de la surveillance et de l'application de la loi. NIS 2 s'appliquera aux organisations de l'UE comptant plus de 50 salariés et dont le chiffre d'affaires annuel dépasse 10 millions de dollars, ainsi qu'à toute organisation précédemment concernée par la directive NIS. Kiteworks et un Réseau de Contenu Privé compatible avec Kiteworks, déployé sur site, dans le cloud ou en hybride, vous aideront à être conforme en ce qui concerne les fichiers sensibles et les e-mails que vous communiquez à l'intérieur et à l'extérieur de l'entreprise. Voici comment :

Assurer la conformité grâce aux politiques de sécurité des systèmes d'information

Kiteworks permet aux clients de standardiser les politiques de sécurité pour la messagerie électronique, le partage de fichiers, la téléphonie mobile, le MFT, le SFTP, etc., et d'appliquer des contrôles granulaires pour protéger la confidentialité des données. Les administrateurs ont la possibilité d'attribuer des autorisations basées sur les rôles aux utilisateurs externes, conformément à la norme NIS 2 qui s'applique de manière cohérente à tous les canaux de communication.

Gérer les incidents avec efficacité

La détection des anomalies permet d'avoir une vision immédiate des accès non autorisés. La technologie de l'IA détecte les événements suspects comme une éventuelle exfiltration, et envoie une alerte par e-mail et dans les journaux d'audit. Grâce aux journaux d'audit immuables de la plateforme, les organisations sont en mesure de détecter les attaques plus rapidement et de conserver la chaîne de preuves nécessaire aux investigations futures. Cela permet un signalement obligatoire efficace de toute violation de données à l'équipe de réponse aux incidents de sécurité informatique (CSIRT) ou, si nécessaire, à l'Agence de l'Union européenne pour la cybersécurité (ENISA) en temps utile, conformément à la directive.

Assurer la continuité de l'activité grâce à la reprise après sinistre intégrée de Kiteworks

L'interface de suivi conviviale permet de conserver des enregistrements détaillés de toutes les activités et données techniques. Les journaux d'audit remplissent alors deux fonctions : permettre à l'organisation d'enquêter sur les violations de données, et fournir des preuves de conformité lors des audits. En cas de violation, l'organisation est capable d'identifier exactement les données exfiltrées et de travailler immédiatement à la récupération après sinistre pour poursuivre ses activités quotidiennes en conformité..

Gérer les vulnérabilités lors du développement et de la maintenance

Kiteworks applique un cycle de vie strict de développement de logiciels sécurisés comprenant des examens approfondis du code de sécurité, des tests de piratage réguliers et un programme de récompenses pour assurer la protection de vos données. Un pare-feu réseau et un WAF intégrés, un accès zéro trust et la surface d'attaque réduite contribuent à réduire considérablement les risques de sécurité. Kiteworks gère également les mises à jour pour les clients qui ont été testés pour la compatibilité du correctif avec d'autres composants du système, ce qui permet d'apporter rapidement des corrections au système d'exploitation, aux bases de données et aux bibliothèques open source.

Définir et appliquer les bonnes pratiques en matière d'hygiène informatique

L'ISO a reconnu que Kiteworks protégeait efficacement tous les contenus sensibles contre les risques informatiques (ISO 27001), y compris lorsqu'il était déployé en tant que service en cloud (ISO 27017), et qu'il protégeait votre organisation contre les fuites préjudiciables d'informations personnelles identifiables (ISO 27018). En outre, Kiteworks dispose d'une bibliothèque de certifications de conformité, y compris la conformité SOC 2 et la certification SOC 2. Ces certifications, ainsi que l'architecture à locataire unique et le renforcement multicouche, valident la capacité de Kiteworks à atténuer les risques liés au contenu avec le système de gestion du contenu et à maintenir les bonnes pratiques d'hygiène informatique conformément à NIS 2.

Protéger le contenu grâce au chiffrement

Assurer le chiffrement des fichiers et des volumes de tout le contenu au repos (avec le chiffrement AES-256) et le chiffrement TLS en transit pour le protéger contre l'accès non autorisé, l'altération des données et les logiciels malveillants. Le chiffrement flexible permet aux clients d'utiliser le chiffrement de bout en bout de Kiteworks et de faire le lien avec des partenaires qui utilisent différentes normes telles que OpenPGP, S/MIME et TLS. La messagerie sécurisée de Kiteworks prévoit le chiffrement et des contrôles de sécurité uniformes grâce à une passerelle de protection des e-mails qui garantit que seuls les utilisateurs authentifiés peuvent lire les messages.

Établir des politiques de contrôle d'accès et de gestion des actifs

Les administrateurs de Kiteworks déploient des contrôles granulaires pour protéger les contenus sensibles et appliquer les politiques de conformité. Ainsi, les dirigeants d'entreprise peuvent gérer facilement les contenus, dossiers, invitations et contrôles d'accès afin de garantir la conformité de tous les contenus à la norme NIS 2. Le contrôle d'accès peut aussi être géré à l'aide du geofencing, de l'app enablement, du filtrage des types de fichiers et du contrôle de la redirection d'e-mails.

Vérification des utilisateurs avec l'authentification multifactorielle

Appliquez des politiques granulaires MFA et SSO en fonction des rôles et des emplacements en utilisant RADIUS, SAML 2.0, Kerberos, des applications d'authentification, PIV/CAC ou encore SMS.