SOLUTION BRIEF

Conformité NIS2

Transformez votre parcours de résilience numérique avec NIS2.

Problème

Les organisations de l'Union européenne font face à un défi sans précédent avec la mise en œuvre de la directive NIS2. Ce cadre de cybersécurité renforcé élargit considérablement à la fois le champ des entités concernées et la complexité des exigences de conformité, créant ainsi des impératifs opérationnels et stratégiques urgents pour les entreprises. La directive introduit des mesures de surveillance plus strictes, des exigences d'exécution et des sanctions plus lourdes.

Les organisations doivent désormais faire face à des obligations nouvelles et complexes en matière de gestion des risques, de signalement des incidents, de sécurité de la chaîne d'approvisionnement, de gouvernance et de partage d'informations. De nombreuses entités peinent à comprendre leur statut de classification, à évaluer leur niveau de sécurité actuel par rapport aux nouvelles exigences et à déterminer les modifications à apporter à leurs programmes de cybersécurité existants. L'élargissement du champ d'application signifie que des milliers d'entreprises supplémentaires doivent désormais s'y conformer, dont beaucoup n'ont jamais été soumises à des réglementations aussi complètes en matière de cybersécurité. Le défi est d'autant plus sérieux qu'il faut assurer la coordination entre de multiples parties prenantes internes et fournisseurs externes, et que les capacités opérationnelles et techniques requises sont considérables. Sans une préparation adéquate et des conseils d'experts, les organisations s'exposent à des pénalités substantielles, à une atteinte à leur réputation et à une interruption de leurs activités.

2 % d'amende sur le chiffre d'affaires global en raison de la non-conformité [1]

Responsabilité personnelle en cas de négligence grave[2]

Principaux avantages

- **Visibilité des risques.**
  Bénéficiez d'une visibilité sans précédent sur les risques humains au sein de votre organisation, compilés en fonction du comportement des utilisateurs et des menaces réelles.
- **Actions adaptatives.**
  Attaquez-vous aux comportements dangereux grâce à des retours en temps opportun et à une formation captivante, dispensée aux bonnes personnes, quand elles en ont besoin.
- **Contrôles proactifs.**
  Limitez les risques humains dans votre environnement de sécurité en anticipant le réglage des contrôles de sécurité pour mieux protéger les utilisateurs.

1 https://nis2directive.eu/nis2-fines/

2 https://www.dlapiper.com/en-us/insights/publications/derisk-newsletter/2024/nis2-directors-personal-liability-for-lack-of-compliance-is-a-warning-message

La solution

Les organisations d'aujourd'hui font face à une pression croissante pour satisfaire aux exigences de la directive NIS2 tout en conservant leur efficacité opérationnelle et en renforçant leur position en matière de sécurité. Mimecast propose une plateforme de sécurité intégrée qui couvre les sept domaines critiques de la conformité NIS2 grâce à une approche unifiée et facile à gérer. Notre solution complète intègre à la fois des contrôles robustes des politiques et des capacités avancées de gestion des incidents, ce qui permet de détecter et de répondre rapidement aux menaces. Nous garantissons la continuité des activités grâce à des solutions fiables de sécurité des e-mails, tout en fournissant les contrôles de sécurité de la chaîne d'approvisionnement nécessaires pour gérer efficacement les risques liés aux tiers. Grâce à une formation captivante de sensibilisation à la sécurité, nous transformons la potentielle vulnérabilité que constituent les employés en une ligne de défense puissante. Notre plateforme permet d'effectuer des tests de sécurité et des audits en continu pour valider l'efficacité des contrôles, tandis qu'un cryptage de qualité professionnelle protège les données sensibles où qu'elles se trouvent. Cette approche intégrée simplifie non seulement la conformité à la norme NIS2, mais apporte une valeur ajoutée mesurable en réduisant les risques, en renforçant la sécurité et en permettant des opérations commerciales sûres et ininterrompues. En s'associant à Mimecast, les organisations acquièrent plus qu'une technologie ; elles gagnent un conseiller de confiance qui s'engage à protéger leurs communications, leurs données et leurs opérations contre les cybermenaces en constante évolution, tout en garantissant la conformité aux exigences de la directive NIS2.

Conformité NIS2 simplifiée : l'avantage de Mimecast

La directive NIS2 renforce le paysage de la cybersécurité de l'UE en s'appuyant sur sept piliers essentiels qui fonctionnent ensemble pour créer une défense globale contre les cybermenaces modernes. Ces piliers interconnectés établissent un cadre de sécurité robuste qui englobe l'analyse des risques et les politiques de sécurité des systèmes, les protocoles de gestion des incidents, les mesures de continuité des activités, les contrôles de la chaîne d'approvisionnement, une formation complète de sensibilisation, des tests et audits de sécurité réguliers, ainsi que des protections cryptographiques fortes. En mettant en œuvre ces sept éléments fondamentaux, les organisations peuvent développer une cyber-résilience durable tout en répondant à des exigences de conformité renforcées, protégeant ainsi leurs actifs et opérations sensibles contre les menaces numériques en constante évolution.

Grâce à notre plateforme de sécurité intégrée, Mimecast offre une protection complète sur les sept piliers du NIS2, transformant les exigences réglementaires en avantages de sécurité pratiques qui protègent les communications de votre organisation, renforcent la conformité et développent une cyber-résilience durable.

Politique

NIS2 impose des contrôles de sécurité complets pour les systèmes de messagerie électronique, exigeant des organisations qu'elles mettent en œuvre le cryptage, des mécanismes d'authentification sécurisés et une protection sophistiquée contre les menaces. Notamment en ce qui concerne la protection des systèmes critiques susceptibles d'être infiltrés par une attaque par e-mail. Les organisations doivent déployer des mesures de sécurité des e-mails à plusieurs niveaux, notamment des fonctionnalités d'évaluation continue de la sécurité afin de se protéger contre l'évolution des menaces liées aux e-mails, telles que le phishing et les attaques par compromission de messagerie professionnelle (BEC).

Incydr offre des capacités complètes de protection des données et de gestion des risques conformes aux exigences de la directive NIS2. Grâce à la surveillance en temps réel et à la détection avancée des menaces, Incydr donne une visibilité continue sur les mouvements de données de votre environnement numérique, ce qui vous aide à identifier les risques potentiels et à y répondre avant qu'ils ne dégénèrent en incidents graves.

Réponse aux incidents

Les capacités complètes de réponse aux incidents de Mimecast offrent des fonctionnalités de sécurité et de conformité robustes dont votre organisation a besoin pour satisfaire aux exigences de la directive NIS2. Notre suite de solutions intégrées comprend Analysis and Response, Internal Email Protect et Mimecast Email Incident Response (MEIR), offrant une surveillance continue des menaces et une correction rapide sur vos canaux de messagerie. MEIR simplifie vos opérations de sécurité en associant triage automatisé et validation humaine experte, réduisant ainsi considérablement la charge de travail de vos équipes de sécurité tout en conservant la précision. Grâce à une intégration fluide avec les plateformes d'orchestration, nous automatisons les workflows de réponse pour la suppression des menaces, les mises à jour des politiques et la documentation, assurant ainsi une gestion cohérente et efficace des menaces.

En offrant une visibilité complète sur les mouvements de données et les menaces potentielles, Incydr vous aide à satisfaire aux exigences strictes de la directive en matière de signalement des incidents. Notre système intégré de gestion des cas simplifie la conformité en consolidant les fonctions de sécurité qui nécessitent traditionnellement plusieurs outils, permettant ainsi à votre équipe de sécurité de se concentrer sur des initiatives stratégiques plutôt que sur la gestion de processus de signalement complexes.

Continuité

La continuité garantit un accès ininterrompu aux communications pendant les pannes planifiées et non planifiées. Il est pris en charge par des centres de données géographiquement dispersés et bénéficie d'un accord de niveau de service (SLA) de 100 % de disponibilité. Sync and Recover permet de rétablir rapidement les opérations suite à une perte de données accidentelle ou à des actions malveillantes. Cette solution s'attaque spécifiquement aux menaces basées sur les e-mails, comme les ransomwares, en offrant une récupération rapide et granulaire des boîtes mail, des calendriers et des tâches, avec des politiques de conservation configurables.

Chaîne d'approvisionnement

La protection avancée contre les attaques par compromission des e-mails professionnels (BEC) constitue votre défense essentielle contre les attaques sophistiquées de la chaîne d'approvisionnement, en s'appuyant sur l'apprentissage automatique et le traitement du langage naturel pour analyser les modèles de communication et bloquer les activités frauduleuses avant qu'elles n'affectent les opérations de votre entreprise. Nous renforçons cette protection grâce au chiffrement Transport Layer Security (TLS) et au protocole DANE (DNS-based Authentication of Named Entities) basé sur le DNS, qui veillent à ce que vos transmissions par e-mail restent sécurisées et authentifiées tout au long de leur parcours.

Formation

Mimecast Engage transforme les vulnérabilités de sécurité potentielles en forces organisationnelles grâce à une formation ciblée et à une évaluation des risques. Les capacités de gestion des risques humains fournissent des informations détaillées sur les comportements des employés et les profils de risque englobant vos outils de sécurité, et proposent une formation personnalisée de sensibilisation à la sécurité qui s'adapte aux menaces émergentes.

Cryptographie

Le protocole de sécurité Transport Layer Security (TLS 1.2 et 1.3) assure le chiffrement automatique de vos communications en transit. Nous renforçons cette protection grâce au protocole DANE (DNS-based Authentication of Named Entities) basé sur le DNS, qui s'appuie sur le DNSSEC pour vérifier l'authenticité des serveurs de messagerie et prévenir les attaques de type HDM (homme du milieu). Pour les organisations qui ont besoin d'une sécurité maximale, nous prenons en charge les normes PGP et OpenPGP avec une gestion intuitive des clés, ce qui permet un véritable chiffrement de bout en bout sans alourdir le travail de votre équipe informatique.

En outre, nos outils sont conçus pour répondre à vos exigences en matière d'audit, de journalisation intégrée et de partage des menaces, ce qui permet aux organisations de respecter et de maintenir la conformité. En collaborant avec Mimecast, les organisations peuvent aborder en toute confiance la conformité NIS2 tout en renforçant leur résilience opérationnelle numérique globale.

propos de Mimecast

Sécurisez les risques humains grâce à une plateforme unifiée.

La plateforme connectée de gestion des risques humains de Mimecast empêche les menaces sophistiquées qui exploitent l'erreur humaine. En obtenant une visibilité sur les risques humains dans votre environnement de collaboration, vous pouvez protéger votre organisation, sauvegarder les données importantes et impliquer activement les employés pour réduire les risques et améliorer la productivité.