Fiche technique

Simplifier la conformité de la sécurité des identités NIS2 avec la gestion des accès à privilèges de nouvelle génération

Votre organisation est-elle prête pour la directive NIS2 ?

La directive NIS2 (directive (UE) 2022/2555) entre en vigueur en octobre 2024. La directive NIS2 étend le champ d'application de son prédécesseur, la directive sur les réseaux et les systèmes d'information, pour couvrir un plus large éventail de secteurs et de types d'organisations en raison de la dépendance croissante à l'égard des technologies numériques et de l'augmentation de cybermenaces. La directive vise à renforcer la sécurité des réseaux et des systèmes d'information au sein de l'UE, en garantissant un niveau commun élevé de cybersécurité. En révisant la directive, les États membres de l'UE visent à mieux défendre les secteurs industriels critiques contre les attaques par ransomware, les vulnérabilités de la chaîne d'approvisionnement et plus encore.

Le NIS2 couvre davantage de secteurs industriels que la directive initiale, et les exigences s'appliquent non seulement aux organisations et à leurs employés directs, mais également aux sous-traitants et aux fournisseurs de services qui les soutiennent.

Industries NIS	Étendues Industries NIS2	
• **Banque** • **Infrastructure numérique** • **Fournisseurs de services numériques** • **Financial Market Infrastructure** • **Énergie** • **Soins de santé** • **Transport** • **Approvisionnement en eau**	• Produits chimiques • Fournisseurs de services numériques (marchés en ligne, moteurs de recherche, plateformes de réseaux sociaux) • Producteurs, transformateurs et distributeurs d'aliments • Santé (appareils médicaux critiques, Pharma, R&D) • Services postaux et de messagerie	• Administration publique • Espace • Eaux usées • Fabrication de produits critiques (ordinateurs, appareils électroniques, appareils médicaux, automobiles) • Fournisseurs de réseaux ou de services de communications électroniques publics

Le non-respect des règles peut être coûteux et dangereux

Si une organisation ne respecte pas les obligations de conformité définies dans la directive NIS2, elle s'expose à plusieurs conséquences, qui visent à garantir que les entités prennent au sérieux leurs obligations en matière de cybersécurité. La nature et la gravité de ces conséquences peuvent varier en fonction de la législation nationale spécifique de chaque État membre de l'UE, puisque les États membres sont responsables de la transposition des directives de l'UE dans leur droit national. Cependant, la directive NIS2 fournit un cadre pour ces sanctions, visant à une approche harmonisée dans l'ensemble de l'UE. Les conséquences potentielles comprennent :

- Amendes pécuniaires
- Paiements de pénalités périodiques
- Ordre de prendre des mesures spécifiques
- Avis publics et atteinte à la réputation
- Restrictions opérationnelles
- Responsabilité pour les dommages

L'application de ces conséquences est assurée par les autorités nationales désignées par chaque État membre de l'UE.

Éliminer la difficulté de la conformité NIS2 avec KeeperPAM

Les organisations de l'Union européenne peuvent s'appuyer sur la solution de gestion des accès à privilèges de nouvelle génération (PAM) de Keeper pour se conformer facilement et à moindre coût à la directive NIS2. En offrant des contrôles d'accès basés sur les rôles (RBAC) granulaires, Keeper permet aux administrateurs informatiques de gérer l'accès aux comptes à privilèges à travers l'organisation, en s'assurant que les utilisateurs n'ont que les autorisations nécessaires pour remplir leurs rôles.Des capacités avancées de rapports fournissent des informations claires sur les activités des comptes à privilèges, facilitant la surveillance continue et simplifiant l'audit requis pour la conformité à la norme NIS2. Keeper permet également aux organisations de toutes tailles d'appliquer les meilleures pratiques en matière de cybersécurité, y compris l'utilisation de mots de passe forts et uniques et l'authentification multifacteur (MFA). Au cœur de la solution de Keeper se trouve son modèle de chiffrement Zero-Knowledge, qui garantit que les données sensibles sont protégées par une sécurité de pointe, ce qui en fait un choix idéal pour les organisations de l'UE qui souhaitent respecter les normes NIS2 tout en améliorant leur position globale en matière de cybersécurité.

Rationaliser la conformité NIS2

Aux exigences	Solution
Paragraphe 49: Politiques de cyberhygiène	**Mettre en place des politiques de cyberhygiène solides avec la gestion des mots de passe et l'accès selon le principe de moindre privilège.** Le gestionnaire de mots de passe d'entreprise de Keeper, leader sur le marché, crée, stocke et gère des mots de passe complexes et uniques pour chaque utilisateur. Les contrôles d'accès basés sur les rôles (RBAC) permettent aux administrateurs de gérer avec précision les autorisations des utilisateurs, en veillant à ce que les individus n'aient accès qu'aux ressources nécessaires à leurs fonctions, afin de garantir le principe de moindre privilège dans l'ensemble de l'organisation.
Paragraphe 54: Ransomware	**Défendre les données et les systèmes contre les ransomwares.** Keeper impose l'utilisation de mots de passe forts et uniques ainsi que la MFA pour chaque utilisateur et chaque appareil au sein d'une organisation.KeeperPAM centralise les secrets dans un coffre-fort sécurisé et peut être configuré pour effectuer une rotation automatique des identifiants. Keeper fournit également une infrastructure à distance sécurisée et un accès aux bases de données sans exposer les identifiants. Des rapports détaillés, des alertes en temps réel et la surveillance du dark Web permettent aux organisations de détecter rapidement les identifiants faibles ou compromis afin d'atténuer les menaces potentielles.
Paragraphe 62: Informations en temps utile sur les vulnérabilités	**Avoir accès à des informations correctes et opportunes sur les vulnérabilités et établir une procédure appropriée pour prendre des mesures d'atténuation.** Le tableau de bord des risques complet de Keeper fournit aux administrateurs un aperçu instantané de l'activité des utilisateurs et de l'état général de la sécurité, y compris les mots de passe faibles ou réutilisés ou les identifiants qui ont été trouvés sur le dark Web.
Paragraphe 85: Sécurité de la chaîne d'approvisionnement	**Gérer la sécurité de la chaîne d'approvisionnement et les relations avec les fournisseurs.** Keeper Secrets Manager fournit une solution cloud-based entièrement gérée pour stocker, accéder et effectuer la rotation des secrets, éliminant la distribution incontrôlée des informations confidentielles au sein de votre environnement. Il s'agit notamment des mots de passe, des clés API, des clés de mots de passe de bases de données, des certificats et d'autres données sensibles.
Paragraphe 89: Pratiques de cyberhygiène pour les utilisateurs	**Mettre en place des pratiques de cyberhygiène solides, depuis les principes Zero-Trust jusqu'à la gestion de l'identité et de l'accès.** Keeper gère les autorisations d'accès et surveille l'activité de tous les utilisateurs d'une organisation grâce à une combinaison de RBAC, de stockage sécurisé des identifiants, de gestion des sessions, d'intégration MFA, d'audits et de rapports détaillés. Keeper centralise la gestion des comptes à privilèges pour un contrôle d'accès efficace, utilise le RBAC pour s'assurer que les utilisateurs n'ont accès qu'à ce dont ils ont besoin pour leur rôle, stocke en toute sécurité les identifiants dans des coffres-forts chiffrés, surveille et enregistre les sessions pour la sécurité et la conformité, améliore la sécurité avec la MFA, et fournit des pistes d'audit complètes pour toutes les actions des utilisateurs à privilèges.
Paragraphe 98: Chiffrement de bout en bout pour les fournisseurs de communications publiques	**Tirer parti du chiffrement de bout en bout pour renforcer la sécurité.** Keeper est un fournisseur de sécurité Zero-Knowledge. Le Zero-Knowledge est une architecture de système qui garantit les plus hauts niveaux de sécurité et de confidentialité. Le chiffrement et le déchiffrement des données s'effectuent toujours localement sur l'appareil de l'utilisateur. Keeper est la plateforme de sécurité des mots de passe la plus sûre, certifiée, testée et auditée au monde. Keeper possède la plus longue conformité SOC2 et certification ISO27001 du secteur et se conforme aux normes de l'UE et des États-Unis. Le cadre de protection des données UE–États-Unis, l'extension britannique de ce dernier et le cadre de protection des données Suisse-États-Unis, tels qu'ils ont été définis par le ministère américain du commerce.
Paragraphe 102: Signalement d'incidents obligatoire	**Les incidents doivent être signalés dans les 24 heures suivant la notification.** Le module avancé de rapports et d'alertes de Keeper notifie les administrateurs des événements avec plus de 200 types d'événements pour des rapports personnalisés avec des intégrations pour envoyer les notifications vers Slack, Teams, e-mail et beaucoup d'autres solutions de messagerie préférées via webhook.