LOGPOINT

Mise en conformitéavec la directive NIS2

www.logpoint.com

INTRO

NIS2 est une directive européenne adoptée par le Parlement européen en novembre 2022. Elle vise à protéger les infrastructures critiques au sein de l'UE contre les cybermenaces et à atteindre un même niveau élevé de sécurité dans toute l'UE. NIS2 s'appuie sur la directive NIS de 2016 et comprend des exigences plus strictes en matière de sécurité, d'obligation de reporting et de mise en œuvre pour un plus grand nombre d'entreprises.

La directive européenne NIS2 (Network and Information Security) vise à renforcer la posture de sécurité des organisations pour faire face aux cybermenaces émergentes. Logpoint peut aider votre entreprise à renforcer sa cybersécurité et à se conformer à cette réglementation.

La Directive NIS2 A Renforcé Les Exigences En Matière De Sécurité, Notamment Celles Concernant :

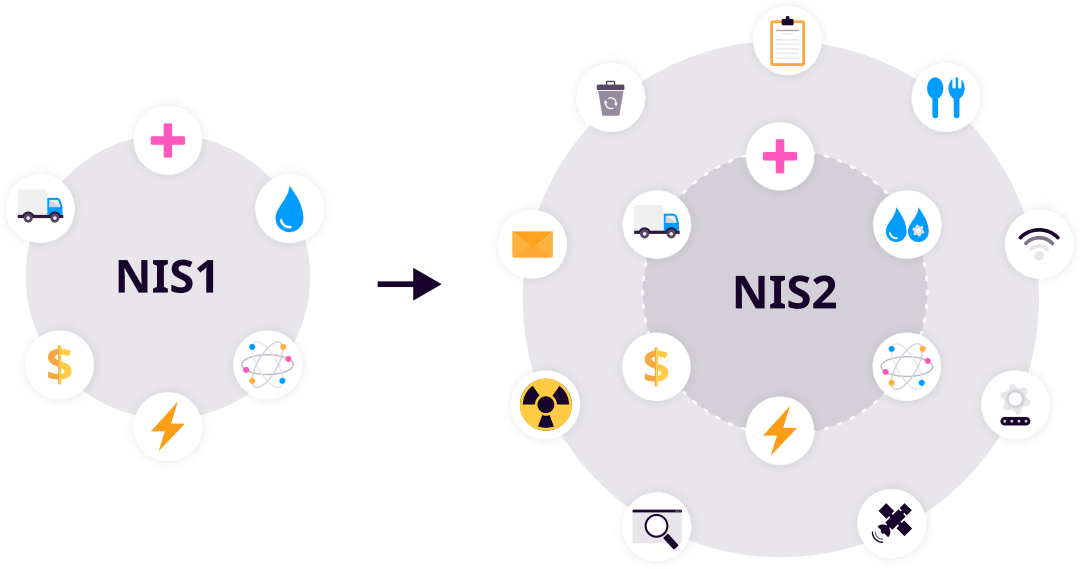
- La réponse aux incidents et la gestion de crise.
- La gestion et la divulgation des vulnérabilités.
- La sécurité de la supply chain.
- Les politiques et procédures pour évaluer l'efficacité de la gestion des risques de cybersécurité.
- Les pratiques élémentaires en matière d'hygiène IT et de formation à la cybersécurité.
- L'utilisation efficace de la cryptographie.
- La sécurité des RH, des politiques de contrôle d'accès et de gestion des actifs/ressources.

Quelles Conséquences En Cas De Non-Conformité Avec La Directive NIS2 ?

Tout comme la directive RGPD, entrée en vigueur en 2018 pour protéger les informations personnelles identifiables (PII), la directive NIS2 introduit des obligations en matière de déclaration et prévoit des sanctions administratives en cas de non-conformité et de non-signalement des incidents. Les sanctions dans le cadre de la directive NIS2 comprennent des obligations de mise en œuvre des recommandations suite à un audit de sécurité et d'alignement de la sécurité sur les exigences du NIS, ainsi que des amendes administratives pouvant aller jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires global d'une organisation. Si vous souhaitez en savoir plus sur les amendes liées à NIS2.

Quand La Directive NIS2 Entrera-T-Elle En Vigueur ?

Le Parlement européen a adopté la directive NIS2 le 10 novembre 2022. Il s'agit d'une directive européenne que les gouvernements devront transposer dans leur droit national d'ici 21 mois, signifiant ainsi que les entreprises qui opèrent dans l'UE devront se conformer aux exigences d'ici la mi-2024.



LA DIRECTIVE NIS2 S'APPLIQUE-T-ELLE À VOTRE ORGANISATION ?

La directive NIS2 s'appliquera à de nombreuses organisations exploitant des infrastructures critiques, notamment les autorités publiques et les entreprises privées des secteurs suivants :

- Énergie (électricité, pétrole, gaz, chauffage urbain et hydrogène).
- Transports (aérien, ferroviaire, fluvial et routier).
- Banques et infrastructures des marchés financiers.
- Secteur de la santé (notamment les laboratoires et la recherche sur les produits pharmaceutiques ainsi que les dispositifs médicaux).
- Traitement de l'eau potable et des eaux usées.
- Infrastructures numériques (Télécom, DNS, TLD, centres de données, services de confiance, services Cloud).
- Services numériques (moteurs de recherche, marchés en ligne, réseaux sociaux).
- Administration publique.
- Industrie spatiale.
- Service postal et de messagerie.
- Gestion des déchets.
- Produits chimiques (production et distribution).
- Alimentation (production, transformation et distribution).
- Sciences et éducation.

COMMENT LOGPOINT PEUT AIDER À SE CONFORMER À LA DIRECTIVE NIS2 ?

La solution Logpoint Converged SIEM est une plateforme d'opérations de sécurité de bout en bout qui combine SIEM, SOAR, UEBA, une surveillance et une réponse au niveau des agents endpoint, ainsi que la capacité de détecter et de répondre aux menaces au sein des systèmes critiques d'une entreprise. Logpoint réduit le temps de détection et de réponse au niveau de l'ensemble du paysage des menaces à partir d'une interface unifiée.

Logpoint fournit les trois composants essentiels pour une mise en conformité avec la directive NIS2 :

1. Sécurité De La Supply Chain

La directive NIS2 exige que les entreprises prennent en compte les risques de cybersécurité au niveau de la supply chain liée à leurs technologies d'information et de communication. Logpoint prend très au sérieux la cybersécurité et la sécurité de ses logiciels et de ses processus de développement, d'ailleurs notre certification Common Criteria EAL3+ en est la preuve. Cette dernière est la norme de sécurité la plus élevée atteinte par un éditeur SIEM, signifiant ainsi que nos produits sont sécurisés dès leur conception, notamment la manière avec laquelle nous développons, évaluons et protégeons nos logiciels. Logpoint adhère également à la norme ISO 15408 et nous effectuons fréquemment des pentests via des organismes tiers et des audits de sécurité au niveau du secteur, tels que SOC 2 Type II. Logpoint est conforme aux réglementations les plus strictes en matière de protection des données, notamment RGPD, CCPA et Schrems II, qui garantissent le stockage physique des données au sein de l'UE.

2. Reporting

La directive NIS2 exige que les entreprises déclarent dans les 24h les incidents importants. Logpoint collecte les logs de manière centralisée au niveau de votre réseau et infrastructure. Avec des rapports prêts à l'emploi et un enregistrement d'audit de toutes les modifications apportées au système, il est facile de créer et de partager des rapports d'incident complets.

3. Détection, Réponse Etgestion Des Incidents

Après le signalement initial qui doit être réalisé dans les 24h, la directive NIS2 exige la transmission d'un rapport final concernant un incident majeur dans un délai d'un mois. Logpoint dispose d'une gestion de cas intégrée qui combine automatiquement les incidents associés au sein d'un seul et même cas, contribuant ainsi à accélérer les investigations et les réponses. Logpoint ajoute des informations pertinentes issues des renseignements sur les menaces (Threat-intelligence), de l'enrichissement et d'autres investigations pour donner une image complète des évènements ayant eu lieu. Vous pouvez facilement créer des rapports directement à partir de chaque cas.

LES PRINCIPALES ÉTAPES PRATIQUES À SUIVRE

Pour gérer efficacement l'évolution des cyber-risques et se conformer à la directive NIS2, votre conseil d'administration et votre équipe dirigeante doivent définir ou améliorer leur stratégie de cybersécurité à l'aide du guide suivant afin de renforcer la cyber-résilience. Le soutien de la direction générale est essentiel car la directive NIS2 considère celle-ci comme directement responsable de la mise en œuvre et du respect des exigences NIS2.

Vous trouverez ci-dessous six actions que vous devez mener à bien afin de préparer au mieux votre entreprise à être en conformité avec la directive NIS2 :

Évaluation De La Maturité

Évaluez si la directive NIS2 s'applique à votre entreprise et quelles sont les implications d'une mise en conformité de votre organisation avec celle-ci, soit en interne, soit par l'intermédiaire d'un consultant externe. L'évaluation de la maturité montre ce que votre entreprise devra mettre en œuvre ou bien les domaines à améliorer pour répondre aux exigences. L'évaluation permettra d'établir clairement également tous les investissements ou compétences dont votre entreprise aura besoin pour réussir sa mise en conformité.

Identification Des Actifs/Ressources Critiques

La directive NIS2 cherche à protéger les infrastructures critiques, la supply chain sur laquelle reposent ces dernières ainsi que d'autres fonctions sociétales importantes. Cette dernière classe les actifs critiques en deux catégories :

- **Entités essentielles :** énergie, transports, santé, eau, espace,administration publique, infrastructures numériques, marchés bancaires etfinanciers.
- **Entités importantes :** services postaux, secteur manufacturier, production alimentaire, entre autres.

Il est important d'identifier les actifs opérationnels critiques au niveau des processus, des personnes, des technologies ainsi que les fournisseurs de votre entreprise, tels que ceux soumis à l'influence potentielle d'un pays hors zone UE ou bien d'acteurs sponsorisés par des États.

Mise En Œuvre D'un SIEM Ou D'un Framework De Cyber-Gestion

La directive NIS2 exige que les entreprises mettent en œuvre un ISMS (Information Security Management System) pour la cybersécurité et la sécurité de l'information en général. En plus d'un ISMS, un SIEM, comme celui proposé par Logpoint, fournit une gestion centralisée des logs et la capacité de détecter et de répondre aux incidents, garantissant ainsi que vous répondrez aux exigences qui imposent que Logpoint adhère aux normes en matière de sécurité de l'information, notamment la norme ISO27001, afin d'assurer la sécurité des actifs informationnels.

Évaluation Des Risques Et Mise En Œuvre Des Mesures De Mitigation

La directive NIS2 nécessite une approche basée sur les risques en matière de cybersécurité et de sécurité de l'information, signifiant ainsi que votre entreprise doit décrire un processus de risque, s'y conformer et identifier des mesures préventives afin de réduire les risques potentiels. À l'aide d'un framework de gestion de la sécurité de l'information tel que la norme ISO27001, vous devez évaluer les risques de tous les actifs critiques, notamment au niveau de votre supply chain et de vos fournisseurs.

Déclaration Au CSIRT

La directive NIS2 exige que les entreprises signalent les incidents aux CSIRT (Computer Security Incident Response Team) régionaux dans les 24h. Les entreprises doivent continuellement fournir des mises à jour de la situation et signaler toute compromission. L'objectif de cette obligation déclarative est d'augmenter les cyber-capacités à travers l'Europe.

Répétez Cette Démarche Encore Et Encore

L'un des principaux points de la directive NIS2 est que les entreprises doivent mettre en œuvre un processus de risque et l'optimiser en permanence, comme c'est le cas avec les normes en matière de gestion de la sécurité de l'information (par exemple la norme ISO27001). Le cyber-paysage est en constante évolution, tout comme les risques. Les entreprises doivent évaluer régulièrement leurs politiques et procédures de cybersécurité pour maintenir leur posture de sécurité à jour.

À PROPOS DE LOGPOINT

Logpoint est le créateur d'une plateforme d'opérations de cybersécurité fiable et innovante, permettant aux entreprises du monde entier d'évoluer et se développer dans un monde constitué de menaces en constante évolution. En combinant une technologie sophistiquée et une compréhension approfondie des défis de ses clients, Logpoint renforce les capacités des équipes de sécurité tout en les aidant à lutter contre les menaces actuelles et futures. Logpoint propose les technologies de sécurité SIEM, UEBA, SOAR et SAP convergées dans une plateforme complète qui détecte efficacement les menaces, minimise les faux positifs, priorise les risques de manière autonome, répond aux incidents et bien plus encore. Basée à Copenhague, au Danemark, et possédant des bureaux dans le monde entier, Logpoint est une entreprise multinationale, multiculturelle et inclusive.

www.logpoint.com