Conformité à la directive NIS2 en 7 étapes : le guide essentiel

Le cadre de travail « Network and Information Security 2.0 », plus connu sous le nom de directive NIS2, marque un progrès important dans la législation de l'Union européenne en termes de cybersécurité. Elle est entrée en vigueur le 16 janvier 2023 pour remplacer la précédente directive (UE) 2016/1148. Les États membres ont jusqu'au 17 octobre 2024 pour intégrer ces mesures à leurs lois nationales, qui devront être mises en œuvre à partir du 17 janvier 2025.

L'objectif de la directive NIS2 est d'améliorer le niveau de cybersécurité général dans l'Union, en réponse à l'augmentation des menaces liées à la numérisation et aux cyberattaques toujours plus nombreuses. Elle introduit un ensemble d'améliorations conçues pour créer une solide structure de gestion de cybercrise, harmoniser les exigences de sécurité et de signalement. Un plus large éventail d'entités et de secteurs sont désormais tenus d'améliorer leurs mesures de cybersécurité. Elle met en outre l'accent sur la sécurité au sein des chaînes d'approvisionnement, la gestion des vulnérabilités, l'infrastructure principale d'Internet, et les bonnes pratiques numériques dans les stratégies nationales.

Cette directive confie de nouvelles missions essentielles à l'Agence de l'Union européenne pour la cybersécurité (ENISA). Celle-ci est notamment chargée de développer un registre européen des vulnérabilités, d'encadrer le réseau CyCLONe (European Cyber Crises Liaison Organisation Network) et de publier un rapport annuel sur la cybersécurité. Cette portée élargie de la directive NIS2 ainsi que ces mesures plus strictes sont conçues pour améliorer considérablement la cybersécurité dans toute l'Europe.

Ce guide explore les nouvelles exigences et obligations en vertu de la directive NIS2, décrit les sept étapes essentielles pour s'y conformer, ainsi que ce qu'AvePoint peut faire pour aider votre organisation à s'adapter à ces normes clés.

Directive NIS2 : nouvelles exigences et obligations

La directive NIS2 introduit plusieurs changements importants pour renforcer la cybersécurité au sein de l'Union européenne. Pour les entreprises, comprendre ces changements et les mettre en œuvre est essentiel afin d'assurer leur conformité et de consolider leur approche de la cybersécurité. Nous aborderons les modifications majeures dans quatre domaines essentiels : la gestion des risques, la continuité des opérations, les obligations de signalement, et la responsabilité des entreprises. Chaque domaine présente les nouvelles exigences et obligations, en détaillant leur objet et leur raison d'être.

01 Gestion des risques

Objet : les organisations sont tenues d'effectuer régulièrement des évaluations des risques de leurs systèmes d'information et de leur réseau. Elles doivent mettre en œuvre des mesures de sécurité sur les plans techniques et organisationnels pour gérer efficacement les risques identifiés. Cela implique de développer des procédures et des politiques exhaustives pour l'évaluation des risques, la sécurité des systèmes d'information, et des process pour faire face aux vulnérabilités et les divulguer.

Raison : l'objectif est de limiter les cyberrisques en encourageant une gestion proactive des incidents, en renforçant la sécurité de la chaîne d'approvisionnement et celle des réseaux, ainsi qu'en améliorant le chiffrement et la régulation des accès. En adoptant une approche systématique et approfondie de l'analyse des risques, les organisations peuvent grandement améliorer leur résilience globale face aux cybermenaces.

02 Continuité des opérations

Objet : les organisations sont tenues d'avoir un plan détaillé pour garantir la poursuite des activités en cas de cyberincident majeur. Ce plan doit prévoir la restauration des systèmes et des données, des procédures d'urgence, ainsi que la mise en place d'une équipe de gestion de crise. Les organisations doivent également développer et garder à jour de solides plans de reprise en cas de catastrophe et pour la continuité des opérations.

Raison : ces mesures sont cruciales pour assurer le fonctionnement continu des opérations et de services essentiels lors des incidents et interruptions. Elles englobent la gestion des sauvegardes, les procédures de restauration et des protocoles de gestion et de communication efficaces en temps de crise. Le tout permet aux activités critiques de continuer en limitant au mieux le temps d'indisponibilité.

03 Obligations de signalement

Objet : les organisations œuvrant dans des secteurs importants, voire essentiels, sont tenues d'implémenter des processus pour signaler rapidement les incidents de sécurité pouvant sérieusement affecter leurs services ou leurs clients. Ces organisations travaillent dans des domaines essentiels tels que la santé, l'énergie ou les transports, et sont soumises à une supervision proactive. Les secteurs importants comprennent l'alimentation, la gestion des déchets et l'industrie, entre autres. Ceux-ci sont surveillés après le signalement d'un incident ou d'une non-conformité. La directive NIS2 impose des délais impartis pour le signalement, notamment une « alerte rapide » sous 24 heures.

Raison : la rapidité de signalement va de pair avec la rapidité de réaction et de restauration pour limiter les effets d'un incident. Les autorités peuvent ainsi surveiller les incidents de cybersécurité et agir en conséquence, améliorant la réponse collective aux cybermenaces. Cette rapidité permet en outre de mieux partager les informations et une meilleure coordination entre les parties prenantes, ce qui augmente la résilience en cybersécurité dans toute l'Union européenne.

04 Responsabilité de l'entreprise

Objet : la directive NIS2 exige que la direction des entreprises supervise et approuve les mesures de cybersécurité de l'organisation, mais aussi qu'elle y soit formée. Les dirigeants doivent activement prendre en compte les cyberrisques, car les brèches peuvent mener à des pertes pour la direction, y compris des prises de responsabilité et l'interdiction temporaire d'occuper des postes de management.

Raison : les organisations se doivent de protéger la confiance du public. La directive NIS2 impose que la direction des entreprises s'implique, afin de garantir que les dirigeants adoptent une approche proactive des risques de cybersécurité. En leur incombant cette responsabilité, la directive les encourage à mener par l'exemple, tout en soulignant l'importance de la cybersécurité aux plus hauts niveaux hiérarchiques des entreprises.

Consolidez votre cyberrésilience avec la directive NIS 2.0

Les nouvelles exigences et obligations de la directive NIS2 ont pour but de renforcer la cyberrésilience de l'Europe face aux menaces actuelles et futures. En respectant ces changements en matière de gestion des risques, de continuité des opérations, d'obligations de signalement et de responsabilité des entreprises, les organisations peuvent éviter des pertes, renforcer leur approche de la cybersécurité, et améliorer la confiance de leurs clients. La mise en œuvre de ces mesures est cruciale pour se conformer à la directive NIS2, mais aussi pour construire de meilleurs remparts contre des cybermenaces en constante évolution.

Votre démarche de conformité à la directive NIS2 : le guide essentiel en 7 étapes

Si vous souhaitez respecter la directive NIS2, votre organisation doit adopter une approche systématique et structurée pour améliorer sa cybersécurité. Ce guide souligne les principales étapes à suivre, ainsi que ce qu'AvePoint peut faire pour vous aider à répondre à ces exigences.

01 Implémentez des politiques de sécurité des systèmes d'information et d'analyse des risques

Vos obligations : développez et mettez en œuvre des politiques approfondies en matière de sécurité des systèmes d'information et d'analyse des risques. Vous devez notamment avoir des process détaillés pour identifier, évaluer et limiter les risques. Il vous faut aussi établir des lignes directrices claires pour gérer les vulnérabilités et la sécurité des systèmes d'information.

Comment AvePoint vous aide : AvePoint Policies automatise l'application des politiques liées à Microsoft 365, garantissant que les politiques de votre organisation sont toujours respectées et que les violations sont surveillées et corrigées. Cette automatisation assure la conformité en vérifiant continuellement le bon respect des politiques et en réalisant les ajustements nécessaires.

02 Évaluez souvent vos mesures de sécurité

Vos obligations : évaluez régulièrement l'efficacité de vos mesures de sécurité et modifiez-les en conséquence. Examinez et actualisez vos protocoles de sécurité pour contrer les nouvelles menaces et vulnérabilités.

Comment AvePoint vous aide : vous pouvez générer des rapports édifiants grâce aux outils d'AvePoint et surveiller en permanence l'efficacité de vos mesures de sécurité. AvePoint Policies et AvePoint Insights vous fournissent des évaluations approfondies et des rapports détaillés, vous permettant d'identifier les points à améliorer pour que vos mesures de sécurité restent aussi efficaces.

03 Mettez en place des process de gestion d'incident

Vos obligations : mettez en place des procédures de détection, de réaction et de gestion face aux incidents. Ces procédures doivent comprendre la surveillance en direct, des protocoles de réponse aux incidents, ainsi que des analyses après chaque incident pour empêcher qu'ils se reproduisent.

Comment AvePoint vous aide : AvePoint propose une surveillance et des alertes en temps réel en cas d'incident, vous permettant de détecter rapidement les menaces de cybersécurité pour y réagir efficacement. La fonction de détection de rançongiciel assistée par IA d'AvePoint Cloud Backup identifie les activités inhabituelles qui pourraient indiquer une compromission ou une attaque par rançongiciel. Elle en informe immédiatement votre admin et fournit une analyse détaillée pour que votre organisation puisse rapidement réagir et limiter les conséquences de l'incident. AvePoint Policies prend les devants face aux menaces internes en appliquant des règles automatisées en matière d'accès, de paramètres et de configurations.

04 Élaborez des plans de reprise en cas de catastrophe et pour la continuité des opérations

Vos obligations : mettez en place de solides plans de reprise en cas de catastrophe et pour la continuité des opérations. Vérifiez que des procédures de restauration et de récupération sont en place et fonctionnent. Examinez régulièrement la pertinence de ces politiques et de la documentation qui s'y rapporte. Cela implique de garder des sauvegardes sécurisées à jour de vos données et systèmes cruciaux.

Comment AvePoint vous aide : AvePoint Cloud Backup Express (en anglais) restaure les données de SaaS 20 fois plus vite que les sauvegardes cloud traditionnelles. Ce service utilise le stockage de Microsoft 365 Backup pour protéger les informations sensibles sur Exchange Online, OneDrive, SharePoint Online, Teams et Microsoft 365 Groups plus rapidement et à plus grande échelle.

05 Implémentez des politiques de chiffrement et de cryptographie

Vos obligations : utilisez la cryptographie et le chiffrement pour protéger les données sensibles. Cela implique de mettre en œuvre des protocoles de chiffrement avancé pour protéger les données statiques ou en mouvement, ainsi que de manipuler vos clés de chiffrement en toute sécurité.

Comment AvePoint vous aide : grâce à AvePoint Cloud Backup, les sauvegardes de données sont chiffrées, qu'elles soient stockées ou en train d'être transférées. Vos données critiques sont ainsi protégées de tout accès non autorisé. Vous pouvez faire confiance à AvePoint Cloud Backup pour préserver vos données grâce à des pratiques de chiffrement avancé.

06 Gérez les accès et les permissions des utilisateurs

Vos obligations : gérez et régulez les accès et permissions de chaque utilisateur concernant les données sensibles. Implémentez des politiques de contrôle d'accès strictes, examinez régulièrement les permissions des utilisateurs, et vérifiez que les informations critiques ne sont accessibles qu'aux membres autorisés.

Comment AvePoint vous aide : les politiques et les ajustements automatiques d'AvePoint vous aident à surveiller et réguler les accès, empêchant les modifications non autorisées et garantissant le respect des politiques d'accès. AvePoint Policies s'intègre parfaitement avec AvePoint Insights pour réguler les accès et vérifier les permissions régulièrement, assurant une gestion appropriée des données sensibles.

07 Mettez en place un système de rapports de conformité

Vos obligations : tenez des registres détaillés sur vos activités en lien avec la conformité et les mesures de sécurité. Documentez toutes les actions visant à respecter les exigences NIS2, et gardez-les à disposition pour les audits et les rapports réglementaires.

Comment AvePoint vous aide : les outils d'AvePoint vous permettent d'établir des rapports et une documentation claire pour vos activités de conformité, en respectant les exigences d'audit et la tenue de registres réglementaire. AvePoint Insights propose des rapports détaillés comprenant toutes les données nécessaires pour prouver simplement votre conformité aux normes réglementaires.

Protégez vos données grâce à AvePoint

Pour améliorer la résilience en cybersécurité de votre organisation tout en adhérant aux dernières normes réglementaires, se conformer à la directive NIS2 est crucial. En prenant systématiquement en compte des domaines essentiels comme la gestion des risques, la continuité des opérations, les obligations de signalement et la responsabilité des entreprises, vous pouvez préserver votre organisation face à l'évolution des cybermenaces.

Leader mondial pour la gouvernance, la gestion et la sécurité des données, AvePoint propose des solutions exhaustives pour vous accompagner dans votre démarche de conformité. De l'application automatique des politiques aux solides pratiques de sauvegarde et de chiffrement, en passant par la surveillance en direct des incidents, les outils et les services de pointe d'AvePoint permettent de préparer votre entreprise aux strictes exigences de la directive NIS2.

En mettant à profit l'expertise et les technologies d'AvePoint, vous avancez dans votre démarche de conformité tout en améliorant votre approche globale de la cybersécurité, en renforçant la confiance de vos parties prenantes, et en consolidant votre avantage compétitif. Vous associer à AvePoint revient à investir pour un avenir dans lequel vos données sont protégées, vos opérations sont résilientes, et votre organisation est prête à affronter les défis de l'ère du numérique.

AvePoint s'engage à offrir le meilleur à ses clients en matière de sécurité et de confidentialité des données. Avec des certifications comme ISO 27701, ISO 27001 et ISO 27017, ainsi que les certifications SOC2 Type II et CSA STAR de niveau 2, vous pouvez faire confiance à AvePoint pour protéger vos données et garantir le respect des réglementations.

AvePoint France

Startway Immeuble Le Crossing 24, 32 Boulevard Gallieni | 92130 Issy-les-Moulineaux

www.avepoint.com/fr | +33 (1) 70 61 02 17 | SalesFR@avepoint.com

AvePoint