Directive NIS2

Nouvelles obligations de cybersécurité pour les OSE, OIV et FSN

Sommaire

Introduction à la Directive NIS2

Contexte et évolution

La Directive sur la Sécurité des Réseaux et des Systèmes d'Information, connue sous l'acronyme **NIS 2,** représente une évolution significative de la législation européenne initiale en matière de cybersécurité - la NIS 1 - introduite en 2016.

La révision de cette directive s'imposait alors face à un paysage cybernétique menaçant, en constante évolution, et à l'augmentation exponentielle des risques liés à la digitalisation des services essentiels à travers l'Union européenne.

NIS 2 vise ainsi à **renforcer la résilience des infrastructures critiques et à augmenter le niveau de sécurité à l'échelle de l'Union**. Elle répond à des lacunes identifiées dans la mise en œuvre de la directive précédente, notamment, l'application inégale entre les États membres et le manque de clarté dans plusieurs de ses dispositions.

Importance accrue de la cybersécurité

Dans un contexte où les cyberattaques deviennent plus fréquentes et plus sophistiquées, affectant tant les entreprises privées que les infrastructures publiques, l'UE reconnaît la nécessité d'une approche plus robuste et harmonisée. NIS 2 élargit donc le champ d'application pour inclure un plus grand nombre d'entités, tout en intensifiant les exigences de conformité.

Cette directive marque un tournant, soulignant l'importance stratégique de la cybersécurité, non seulement pour la protection des infrastructures critiques, mais aussi pour **la confiance dans le marché numérique européen**. Elle implique directement les dirigeants des entreprises, renforçant leur responsabilité dans la mise en œuvre des mesures de cybersécurité adéquates.

Statistiques

Coût des cyberattaques : Le coût global des cybercrimes continue d'augmenter, avec une projection atteignant 10,5 trillions de dollars annuel d'ici à 2025. [1]

Impact sur les entreprises : Plus de 75% des attaques ciblées débutent par un email [2], et la récupération d'une attaque par ransomware coûte en moyenne 1,82 million de dollars, hors coût de la rançon. [3]

(1): https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
(2): https://www.roundrobintech.com/email-protection
(3) : https://www.scmagazine.com/resource/report-ransomware-payouts-and-recovery-costs-went-way-up-in-2023

Champ d'application et entités concernées NIS2

Élargissement du périmètre

La directive NIS 2 étend ainsi considérablement la portée de la réglementation précédente, touchant un large éventail de marchés (35 secteurs ciblés) et d'entités. Voici une présentation détaillée des entreprises et des secteurs désormais couverts :

Secteurs essentiels : Comprend les entreprises qui opèrent dans des domaines où une perturbation pourrait avoir des conséquences graves pour la santé, la sécurité ou l'économie. Cela inclut, mais sans s'y limiter, les marchés suivants :

- Énergie (électricité, pétrole, gaz)
- Transports (aérien, ferroviaire, maritime, routier)
- Banque et marchés financiers
- Santé
- Approvisionnement en eau potable et traitement des eaux usées
- Administration publique
- Infrastructure numérique (fournisseurs de services cloud, centres de données)
- Secteur spatial

Secteurs importants : Moins critiques que les secteurs essentiels, mais toujours soumis à des réglementations strictes, notamment :

- Services postaux et de messagerie
- Gestion des déchets
- Fabrication chimique
- Industrie alimentaire
- Fournisseurs de services numériques
- Organismes de recherche

Entités non-européennes : La directive s'applique également aux entités qui ne sont pas basées dans l'UE, mais qui offrent des services au sein de l'Union. Ces entités doivent désigner un représentant dans un État membre où elles opèrent, assurant la conformité avec les normes européennes de sécurité.

Implications pour les entreprises

Toutes les entreprises relevant de ces catégories doivent évaluer et renforcer leurs mesures de cybersécurité pour se conformer aux exigences de la NIS 2. Elles doivent notamment :

- **Mettre en place des procédures robustes de gestion des risques et d'incident.**
- **Assurer une notification rapide et précise des incidents de sécurité selon les protocoles définis par la directive.**

La mise en œuvre de la NIS 2 par ces entreprises renforcera non seulement leur propre sécurité mais contribuera également à la résilience globale de l'espace numérique européen face aux menaces croissantes de cyberattaques.

Implications pour les entités non-européennes

La directive NIS 2 étend également ses exigences aux entités qui ne sont pas établies dans l'Union européenne, mais qui offrent des services au sein de l'UE. Voici les implications claires pour ces entités non-européennes :

- **Obligation de désigner un représentant dans l'UE :**
  Les entités non-européennes qui fournissent des services dans l'Union doivent désigner un représentant légal dans l'un des États membres où elles opèrent. Ce représentant agira comme point de contact avec les autorités de régulation locales et sera responsable de la conformité avec la directive NIS 2.

- **Juridiction des États membres :**
  En cas de non-conformité, les entités non-européennes sont soumises à la juridiction de l'État membre où elles ont désigné leur représentant. Cela signifie que les sanctions et les mesures correctives peuvent être appliquées conformément à la législation de cet État membre.

- **Conformité réglementaire obligatoire :**
  Comme les entités basées dans l'UE, ces organisations doivent se conformer à toutes les exigences de sécurité et de rapport d'incidents stipulées par la NIS 2. Cela inclut l'adoption de mesures de sécurité robustes, la mise en œuvre de procédures de gestion des incidents et la notification rapide des incidents aux autorités compétentes.

- **Impact sur les opérations commerciales :**
  Les entités non-européennes doivent évaluer l'impact de ces exigences sur leurs opérations commerciales et ajuster leurs stratégies en conséquence. Elles peuvent nécessiter des modifications dans leurs politiques de sécurité, leurs systèmes informatiques et leurs procédures opérationnelles.

Obligations légales et mesures de conformité

Répercussions pour la gestion interne et la conformité

La mise en œuvre de la directive NIS 2 impose aux entités concernées de revisiter et renforcer leurs stratégies de cybersécurité internes pour assurer la conformité :

- **Évaluation des risques :** Chaque entité doit effectuer une évaluation complète des risques de sécurité informatique auxquels elle est exposée. Cela comprend l'identification des vulnérabilités dans leurs systèmes et infrastructures et l'évaluation de leur potentiel d'impact sur les opérations.
- **Sécurisation de la chaîne d'approvisionnement contractuelle :** chaque entité doit garantir que la sécurité de l'information est maintenue sur toute la chaîne d'approvisionnement. Tous les partenaires, sous-traitants et fournisseurs doivent aussi respecter les normes de sécurité fixées.
- **Mise en place de mesures de sécurité :** Sur la base de cette évaluation, les entreprises doivent développer ou améliorer des mesures de sécurité pour prévenir, détecter et répondre efficacement aux incidents de cybersécurité. Cela peut inclure la mise à jour des logiciels, le renforcement des protocoles d'accès et l'amélioration des systèmes de surveillance et de réponse aux incidents.

Parmi les mesures incontournables, nous retrouvons les PSSI (Politiques d'analyse des risques et de Sécurité des Systèmes d'Information), les PCA, les PRA, les solutions d'authentification à plusieurs facteurs ou encore **l'adoption d'outils de communication sécurisés** (Voir point 8).

- **Formation et sensibilisation :** Il est crucial de former le personnel à reconnaître les signes d'attaques potentielles et à réagir correctement en cas d'incident. La sensibilisation continue à la sécurité doit être une priorité, pour tous les niveaux de l'organisation.
- **Procédures de notification des incidents :** NIS 2 requiert que les incidents de sécurité soient signalés aux autorités compétentes dans des délais très courts. Les entreprises doivent donc mettre en place des procédures claires et efficaces pour la notification rapide des incidents, ce qui inclut la préparation des rapports détaillés et l'interaction avec les autorités réglementaires.
- **Révision des politiques internes :** Les politiques internes de sécurité et de gestion des risques doivent être régulièrement révisées et mises à jour pour rester en conformité avec les exigences de la NIS 2. Cela garantit non seulement la conformité réglementaire, mais aussi l'alignement avec les meilleures pratiques de l'industrie.

En bref

L'extension du périmètre de la directive NIS 2 est une réponse adaptée à notre ère numérique, où la sécurité des informations et des réseaux est plus critique que jamais. En imposant des normes strictes et en élargissant la portée de la réglementation, l'UE vise à renforcer la résilience de son espace numérique et à instaurer une culture de sécurité robuste pour toutes les entités opérant sur son territoire. Les entreprises doivent non seulement ajuster leurs pratiques en conséquence, mais aussi préparer leurs équipes à répondre efficacement aux exigences accrues. Elles doivent ainsi assurer la sécurité des données et des infrastructures, qui se retrouvent désormais au cœur de la société contemporaine.

Protocoles de notification et de réponse aux incidents

La directive NIS 2 renforce considérablement les exigences en matière de notification et de gestion des incidents de cybersécurité pour les entités concernées. Rentrons dans le détail de ces protocoles :

Notification des incidents

- **Délais de notification :** Les entités doivent notifier les incidents de sécurité aux autorités compétentes dès que possible après leur découverte. La directive spécifie généralement un délai maximal de 24 heures pour une notification préliminaire, suivi d'un rapport complet dans un délai spécifié, souvent de 72 heures, dépendant de la gravité de l'incident.
- **Contenu de la notification :** La notification initiale doit inclure des informations de base sur la nature et l'étendue de l'incident, ainsi que les mesures immédiates prises en réponse à ces événements. Le rapport complet devrait fournir une analyse détaillée de l'incident, y compris les vecteurs d'attaque, les systèmes affectés, les données compromises et les mesures correctives appliquées pour prévenir de futurs incidents.

Réponse aux incidents

- **Planification de la réponse :** Chaque entité doit avoir un plan de réponse aux incidents établi et prêt à être déployé. Ce plan doit détailler les étapes à suivre pour identifier, contenir, éradiquer et récupérer de l'incident, tout en minimisant les impacts opérationnels et en préservant les preuves pour une enquête ultérieure.
- **Exigences de suivi :** Après la résolution de l'incident, les entités sont tenues de soumettre un rapport de suivi détaillant les leçons apprises et les ajustements apportés aux politiques et procédures de sécurité. Ce suivi est crucial pour éviter la récurrence des incidents et améliorer continuellement les pratiques de sécurité.

Collaboration avec les autorités

- **Échange d'informations :** La directive encourage les entités à partager activement des informations sur les menaces et les vulnérabilités avec les autorités et les autres entités concernées. Cet échange d'informations aide à construire une compréhension collective des menaces en cours et à renforcer les mesures de sécurité à travers l'industrie.
- **Assistance des autorités :** En cas de besoin, les autorités compétentes peuvent fournir une assistance technique ou consultative aux entités pour gérer les incidents de sécurité. Cette assistance peut inclure des conseils sur la mitigation des menaces, des audits de sécurité ou des formations spécifiques.

Ces protocoles de notification et de réponse aux incidents sont essentiels non seulement pour la conformité réglementaire, mais aussi pour la capacité des entités à réagir efficacement aux incidents de sécurité, minimisant ainsi les dommages et renforçant la confiance dans l'écosystème numérique global.

En bref

Ces nouvelles obligations légales et mesures de conformité imposées par la directive NIS 2 visent à créer un environnement numérique plus sûr et plus résilient au sein de l'Union européenne. En mettant en place des mécanismes robustes de gestion des risques et de réponse aux incidents, ainsi que des protocoles de notification rigoureux, les entités concernées contribueront à la sécurité de leurs propres opérations ainsi qu'à celle de l'ensemble de l'économie numérique européenne

Statistiques

Vitesse et fréquence des cyberattaques : Environ 45% des cas traités par l'Unité 42 de Palo Alto Networks en 2023 ont impliqué l'exfiltration de données en moins d'un jour après la compromission. (1)

Coût des attaques par ransomware : Le coût moyen d'une attaque par ransomware était de 4,54 millions de dollars en 2023 (2), avec des coûts de récupération moyens s'élevant à 1,82 million de dollars, excluant le paiement de la rançon. (3)

Efficacité des réponses aux ransomwares : Seulement 8% des entreprises qui paient une rançon récupèrent toutes leurs données. (4)

Exploitation des vulnérabilités logicielles : L'exploitation des vulnérabilités de logiciels et d'API a été responsable de 38,60% des points d'accès initiaux par les attaquants en 2023, en hausse par rapport à l'année précédente. (5)

(1) : https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report
(2) : https://www.ibm.com/reports/data-breach
(3) : https://www.scmagazine.com/resource/report-ransomware-payouts-and-recovery-costs-went-way-up-in-2023
(4) : https://www.sophos.com/en-us/press/press-releases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-more-than-doubling-in-a-year
(5) : https://unit42.paloaltonetworks.com/unit42-incident-response-report-2024-threat-guide/

Sanctions et responsabilités

Cadre des sanctions en cas de non-conformité

La directive NIS 2 a mis en place un cadre rigoureux de sanctions pour assurer l'application efficace de ses mesures de sécurité. Ce cadre vise à encourager une conformité stricte et à décourager toute négligence éventuelle. Voici les principales sanctions que les entités pourraient encourir en cas de non-respect des normes établies :

- **Amendes financières :** Les entités qui ne respectent pas les exigences peuvent se voir infliger des amendes allant jusqu'à 10 millions d'euros ou 2% du total de leur chiffre d'affaires annuel mondial pour les entités essentielles. Pour les entités importantes, les amendes peuvent atteindre jusqu'à 7 millions d'euros ou 1,4% du chiffre d'affaires global, selon le montant le plus élevé.
- **Sanctions administratives :** Outre les amendes, les autorités peuvent imposer des avertissements publics, des injonctions de mise en conformité, et des interdictions ou restrictions temporaires d'opération.
- **Mesures correctives obligatoires :** Les entités peuvent être obligées de prendre des mesures spécifiques pour rectifier les manquements constatés, ce qui peut inclure des audits de sécurité supplémentaires, des formations accrues pour le personnel et la révision des politiques de sécurité existantes.

Responsabilités spécifiques des dirigeants

NIS 2 met l'accent sur la responsabilité des dirigeants et des conseils d'administration, soulignant leur rôle crucial dans la mise en œuvre des pratiques de cybersécurité :

- **Responsabilité directe :** Les dirigeants ont la responsabilité de veiller à ce que leur organisation respecte les exigences de la directive. Cela inclut l'approbation des politiques de sécurité, la supervision de leur mise en œuvre effective et la capacité à déployer les ressources nécessaires.
- **Formation et sensibilisation :** Les dirigeants doivent également s'assurer que leur personnel soit correctement formé et conscient des risques de cybersécurité. Cela implique des formations régulières et des mises à jour sur les meilleures pratiques de sécurité.

En bref

Le renforcement des sanctions et la clarification des responsabilités sous NIS 2 sont des mesures essentielles pour assurer une cybersécurité efficace au sein de l'UE. Ces initiatives visent non seulement à protéger les infrastructures critiques, mais aussi à promouvoir une culture de la sécurité à tous les niveaux des organisations concernées. La directive induit que la cybersécurité n'est pas seulement une question technique, mais aussi une question de gouvernance d'entreprise, nécessitant un engagement fort de la part des leaders organisationnels.

Statistiques

Amendes significatives pour violations de données : Des amendes considérables ont été imposées pour des violations majeures de données. Par exemple, Home Depot a dû faire face à des coûts dépassant 200 millions de dollars suite à un incident de sécurité qui a affecté ses systèmes de paiement. De même, Capital One a réglé un recours collectif pour 190 millions de dollars à la suite d'une brèche de données affectant plus de 100 millions de personnes. (1)

Pénalités pour pour non-conformité au RGPD : Depuis l'application du RGPD, des amendes totalisant environ 4,68 milliards d'euros ont été imposées pour divers manquements à la protection des données personnelles. (2)

Le cas Zoom : Zoom a été condamné à une amende de 85 millions de dollars pour de fausses déclarations concernant le chiffrement et la protection des données partagées avec des services tiers (Enzuzo). (1)

(1) : https://www.enzuzo.com/blog/biggest-data-breach-fines
(2) : https://blogs.dlapiper.com/advocatus/files/2024/01/DLA-Piper-GDPR-fines-and-Data-Breach-Report-2024.pdf#:~:text=URL%3A%20https%3A%2F%2Fblogs.dlapiper.com%2Fadvocatus%2Ffiles%2F2024%2F01%2FDLA

Ressources et soutiens disponibles pour les entités concernées

Pour faciliter l'adoption et l'application de la directive NIS 2, diverses ressources sont mises à disposition des entreprises par l'Union européenne et d'autres organismes. Ces aides visent à assurer que toutes les entités concernées, quelle que soit leur taille, puissent répondre efficacement aux exigences réglementaires :

- **Guidelines et documentation :** L'Agence européenne pour la cybersécurité (ENISA) propose des lignes directrices détaillées, des rapports techniques et des documents de recommandations pratiques pour aider les organisations à comprendre et à mettre en œuvre les exigences de la directive NIS 2. Ces ressources couvrent divers aspects de la cybersécurité, des évaluations de risques à la gestion des incidents.
- **Programmes de formation et sensibilisation :** Des programmes de formation sont fréquemment organisés par des autorités nationales ou des organismes européens pour éduquer les employés des entreprises sur les meilleures pratiques de sécurité et les spécificités de la directive NIS 2.
- **Assistance technique :** Des consultants en cybersécurité ou des spécialistes peuvent être disponibles pour fournir un soutien technique direct aux entreprises. Ce soutien peut inclure l'aide à l'implémentation des technologies de sécurité, l'audit de systèmes existants et l'assistance durant les processus de notification et de gestion des incidents.
- **Aides financières :** Pour les petites et moyennes entreprises (PME), des subventions ou des aides financières sont proposées pour aider à couvrir les coûts associés à la mise en conformité avec la directive. Ces aides financières permettent aux PME de renforcer leurs infrastructures de sécurité sans compromettre leur viabilité financière.
- **Forums et réseaux de partage :** Des plateformes de collaboration et des forums en ligne sont souvent organisés pour permettre aux entreprises de partager des expériences, des conseils et des solutions concernant la mise en œuvre de la directive NIS 2.

Détails sur les aides financières et subventions disponibles pour les PME concernant la cybersécurité dans le cadre de la directive NIS 2

Programme Digital Europe : Ce programme propose des financements visant à renforcer les capacités de cybersécurité des PME européennes. Plusieurs appels à propositions sont disponibles avec un budget total de 84 millions d'euros pour soutenir les technologies avancées, la mise en œuvre des législations de l'UE sur la cybersécurité et la transition européenne vers la cryptographie post-quantique. Les domaines spécifiques incluent l'application de l'IA dans les centres d'opérations de sécurité et le renforcement des capacités des PME en ligne.

Horizon Europe : C'est le programme phare de l'UE pour la recherche et l'innovation, avec un budget substantiel consacré à la cybersécurité. Il offre aux PME la possibilité de participer à des projets de recherche et d'innovation qui abordent les défis mondiaux, y compris la cybersécurité, en visant à renforcer la compétitivité et la croissance de l'UE.

Connecting Europe Facility (CEF) : Ce programme soutient le développement d'infrastructures numériques. Il vise à améliorer les réseaux de transport, d'énergie et numériques à travers l'Europe, incluant des financements pour des projets de cybersécurité.

De l'échelle Européenne

Impact sur la cyber-sécurité

La directive NIS 2 représente une avancée majeure dans l'approche européenne face aux enjeux de cybersécurité, avec un impact significatif sur la sécurité et la résilience numériques à travers toute la zone. Cette directive contribue à établir un environnement numérique plus sûr pour tous les citoyens et entreprises de l'UE.

- **Renforcement des infrastructures critiques :** La directive vise principalement à assurer la protection des infrastructures essentielles qui, si elles étaient perturbées ou atteintes, pourraient avoir des répercussions majeures sur la santé, la sécurité, ou le bien-être économique des citoyens de l'UE. En exigeant que ces infrastructures adoptent des mesures de cybersécurité robustes, la NIS 2 aide à prévenir les interruptions de service et à minimiser les dommages en cas d'attaque.
- **Harmonisation des normes de sécurité :** En imposant des exigences uniformes de sécurité et de rapport d'incidents à travers tous les États membres, la directive facilite une meilleure coordination et une réponse plus rapide aux menaces cyber sécuritaires, notamment au niveau transfrontalier.
- **Amélioration continue de la gestion des risques :** La directive encourage les entités régulées à adopter une approche proactive dans la gestion des risques de cybersécurité. Cela inclut la mise en place de systèmes avancés pour la détection des menaces, la mise en œuvre de défenses adaptées et la préparation aux incidents.

En consolidant ces aspects, la directive NIS 2 augmente non seulement la sécurité des réseaux et des informations à l'échelle de l'UE, mais elle renforce également la confiance dans le marché numérique européen, essentielle pour le développement économique et l'innovation dans la région.

Coopération et coordination entre États membres

La directive NIS 2 met également l'accent sur l'amélioration de la coopération et de la coordination entre les États membres :

- **Échanges d'informations et meilleures pratiques :** La mise en place de groupes de coopération permet aux États membres de partager des informations sur les menaces et les vulnérabilités, ainsi que des meilleures pratiques en matière de cybersécurité.
- **Réponse coordonnée aux incidents :** La directive encourage une réponse coordonnée aux incidents de cybersécurité à l'échelle de l'UE, permettant ainsi une gestion plus efficace des crises aux implications transfrontalières.
- **Rôles définis pour les autorités nationales :** Les autorités nationales de cybersécurité jouent un rôle central dans la supervision de la mise en œuvre de la NIS2, garantissant que les directives soient appliquées de manière cohérente et efficace.

Le rôle de l’ENISA

L’Agence européenne pour la cybersécurité (ENISA) joue un rôle clé pour identifier et partager les meilleures pratiques en matière de cybersécurité. ENISA aide à traduire les obligations légales en exigences techniques et conseille les États membres sur l’amélioration des mesures de sécurité en accord avec la législation de l’UE, y compris la directive NIS 2.

En bref

En conclusion, la directive NIS 2 est une étape significative vers la création d’un espace numérique européen plus sécurisé et résilient. Par ses exigences étendues, ses mesures de renforcement de la coopération et son approche harmonisée de la cybersécurité, elle vise à protéger les économies et les sociétés européennes contre les risques de cybersécurité de plus en plus complexes. L’engagement actif des États membres et des entités concernées est essentiel pour atteindre les objectifs ambitieux de cette directive et renforcer la posture de l’Union dans son ensemble.

Interactions avec d’autres politiques de l’UE

La directive NIS 2 ne fonctionne pas de manière isolée mais interagit étroitement avec d’autres réglementations et politiques européennes. Le but ? Créer un cadre cohérent et robuste en matière de cybersécurité. Ces interactions assurent que les mesures prises dans le cadre de la NIS 2 soient complémentaires et renforcent les autres aspects de la réglementation européenne.

Interaction avec le RGPD

L’un des points d’intersection les plus significatifs est avec le Règlement Général sur la Protection des Données (RGPD), qui régit la protection des données personnelles au sein de l’UE. La NIS 2 et le RGPD se complètent, la première imposant des exigences de sécurité pour les réseaux et les systèmes d’information, alignant ainsi les objectifs de sécurité et de protection de la vie privée.

Coordination avec la Directive eIDAS

La NIS 2 travaille également en synergie avec la Directive eIDAS, qui concerne les services d’identification électronique et de confiance pour les transactions. Ensemble, ces directives soutiennent l’intégrité et la sécurité des services en ligne et des transactions numériques à travers l’Europe, renforçant ainsi la confiance dans l’économie numérique.

Complémentarité avec la Directive DORA

En outre, la NIS 2 complète la Directive sur la Résilience Opérationnelle Numérique (DORA), destinée spécifiquement aux secteurs financiers. Tandis que DORA se concentre sur la cybersécurité dans le secteur financier, la NIS 2 apporte une couverture plus large, assurant que les infrastructures utilisées par ces institutions financières, ainsi que d’autres secteurs, soient également protégées.

Support à travers le Digital Europe Programme

Le Programme Europe Numérique, qui promeut le déploiement et l’utilisation des technologies numériques, soutient la mise en œuvre de la NIS 2 en finançant des projets qui améliorent les compétences numériques et la cybersécurité. Ce programme aide à bâtir l’infrastructure et les compétences nécessaires pour répondre aux exigences de la NIS 2 et des autres directives associées.

Sécuriser la collaboration

Avec l'entrée en vigueur de la directive NIS2, la sécurisation des interactions et des données est devenue une priorité absolue pour toutes les entreprises européennes. **De ce fait, la question de la collaboration - et la sélection des bons outils - devient vitale.**

Une plateforme collaborative ne doit plus seulement faciliter la communication et la gestion de projet - elle doit également se conformer aux normes et aux réglementations qui régissent le quotidien de ses utilisateurs.

Wimi & NIS 2

La suite collaborative Wimi se positionne ainsi comme un partenaire stratégique pour la conformité à NIS2.

Made in France :
Fondée à Paris en 2010, Wimi est une société 100% indépendante et 100% Européenne.

Souveraineté des données :
Les données des clients Wimi sont exclusivement hébergées sur des infrastructures propriétaires et physiques, en France métropolitaine.

SecNumCloud :
Wimi suit les meilleures pratiques de sécurité dictées par l'ANSSI au-travers du référentiel SecNumCloud.

Certification Cloud de Confiance :
Wimi aspire à devenir la première suite collaborative à obtenir la certification Cloud de Confiance.

SecNumCloud & Wimi, à quoi s'attendre ?

Organisation de la sécurité

- RSSI, Politique de sécurité
- Gestion des risques
- Processus, documentation, mises à jour
- Gestion des actifs

Sécurité des ressources humaines

- Contrats, vérification
- Chartes
- Contrôle d'accès
- Gestion des identités

Les engagements sur la sécurité

- Plan d'Assurance Sécurité
- Audit
- Informations
- PCA / PRA

Les processus sécurité de l'éditeur de logiciel

- Accès aux environnements de production
- Sauvegardes, restauration
- Détection automatique d'anomalies d'usage
- Gestion des incidents de sécurité

Sécurité du logiciel (code)

- Cryptologie
- Tests d'intrusion réguliers
- Fonctionnalités de sécurité
- Formation continue des développeurs

Sécurité de l'hébergement (Serveurs)

- Sécurité physique et environnementale
- Centralisation des logs machines
- Cloisonnement des données client
- Analyse et corrélation des événements

Les solutions de sécurité Wimi

Wimi MFA : l'authentification renforcée

Wimi MFA, ou Multi Factor Authentication, est une application d'authentification forte développée par Wimi, disponible sur iOS et Android. Les méthodes incluent :

- Codes temporaires à 6 chiffres
- Empreinte digitale
- Reconnaissance faciale

Cette solution minimise les risques d'usurpation d'identité et de vol de mots de passe, assurant ainsi une identification sûre, sans nécessiter d'équipement supplémentaire.

Wimi Tattoo : sécurité avancée pour documents sensibles

Wimi Tattoo est une fonctionnalité intégrée dans la suite collaborative Wimi, spécialement conçue pour sécuriser le partage de documents sensibles. Utilisant une technologie de watermarking unique, Wimi Tattoo permet de tracer l'origine des fuites potentielles tout en préservant l'intégrité des documents. Voici ses principales caractéristiques :

- **Imperceptibilité :** préserve la confidentialité sans altérer les documents.
- **Sécuritaire :** augmente la sécurité par la responsabilisation des utilisateurs.
- **Versatilité et adaptabilité :** s'intègre harmonieusement tout en supportant divers formats de documents.
- **Résilience :** maintient l'authenticité des documents même après manipulations.
- **Économie :** permet une détection rapide des violations, réduisant ainsi les coûts associés à la gestion des risques.

Chiffrement de bout-en-bout

Wimi offre un chiffrement de bout-en-bout (E2EE) pour les espaces de travail contenant des données sensibles, utilisant des technologies cryptographiques certifiées par l'ANSSI. Cette fonctionnalité assure une protection contre divers risques tels que le vol de données, les intrusions et les vols d'appareils.

Antivirus

Wimi intègre un antivirus puissant sur son infrastructure SecNumCloud, assurant une analyse immédiate des fichiers dès leur dépôt sur la plateforme. En cas de détection de risque, le fichier est automatiquement mis en quarantaine et l'utilisateur est immédiatement averti.

Wimi Armoured: Écosystème de Défense Européen

Wimi Armoured est une solution avancée conçue pour répondre aux exigences spécifiques de l'écosystème de défense européen. Elle intègre le chiffrement de bout-en-bout (end-to-end), assure l'accessibilité au niveau de classification DR, et est déployée sur des serveurs tactiques en mode EDGE pour une sécurité maximale et une performance adaptée aux environnements exigeants.

Note de synthèse

Supervision et application renforcées

La directive NIS 2 confie aux autorités nationales de cybersécurité des responsabilités accrues pour garantir le respect des normes de sécurité à travers l'Union européenne. Ces autorités disposent désormais de pouvoirs étendus pour effectuer des audits réguliers, inspecter les mesures de sécurité en place, et imposer des sanctions en cas de non-conformité. Les sanctions peuvent inclure des amendes substantielles, destinées à encourager une mise en conformité rapide et sérieuse avec les règles de cybersécurité.

Harmonisation et coopération européenne

Un aspect clé de la directive NIS 2 est l'harmonisation des procédures de notification et de réponse aux incidents à travers les États membres, facilitant ainsi une coordination et une gestion des crises plus efficaces. La directive promeut une coopération accrue entre les États membres, notamment par le partage des informations sur les menaces et les meilleures pratiques de cybersécurité. Cette approche collaborative renforce la sécurité collective et permet une réponse plus cohérente aux incidents à l'échelle européenne.

Extension de la portée à de nouveaux secteurs

La directive NIS 2 élargit son application à des secteurs précédemment moins réglementés en matière de cybersécurité, tels que le secteur de la santé et les services numériques, qui incluent les fournisseurs de services cloud et les plateformes numériques. Ces secteurs jouent un rôle crucial dans l'économie numérique et sont désormais tenus de mettre en œuvre des mesures de sécurité avancées et de signaler les incidents de sécurité de manière rigoureuse. L'impact de cette extension est significatif ; elle augmente la résilience globale de l'UE face aux cyberattaques et aligne les pratiques de sécurité à travers de nouveaux domaines économiques et sociaux essentiels.

Vision stratégique

La directive NIS 2 est conçue non seulement pour répondre aux menaces actuelles, mais aussi pour anticiper les défis futurs dans un monde numérique en constante évolution. Elle représente les efforts de l'UE pour maintenir et améliorer sa compétitivité économique et sa sécurité nationale dans le paysage numérique global.

Engagement continu

Pour atteindre ces objectifs, un engagement continu des États membres, des entreprises et des institutions à tous les niveaux sera crucial. La mise en œuvre effective de la NIS 2 nécessitera une collaboration étroite, un partage d'informations en temps réel et un investissement continu dans les technologies de cybersécurité.

Vers un avenir plus sûr

En conclusion, la directive NIS 2 est une avancée significative vers la création d'un espace numérique sécurisé et résilient en Europe. Elle incarne la réponse proactive de l'UE aux menaces cybernétiques, en s'assurant que toutes les entités concernées soient préparées non seulement à se défendre, mais aussi à anticiper et à répondre efficacement aux incidents de cybersécurité. L'avenir de la cybersécurité européenne, sous l'égide de la NIS 2, promet d'être plus sécurisé, résilient et adapté aux défis du XXIe siècle.

Wimi est la suite collaborative qui rassemble tout ce dont votre organisation a besoin en matière de collaboration, de gestion documentaire avancée, de gestion de projets et de communication pour fluidifier le travail de vos équipes et la relation avec vos partenaires externes ou clients. Wimi est la 1ère suite collaborative souveraine à viser une qualification SecNumCloud et Cloud de Confiance en 2024/2025.

112, Rue Réaumur, Paris, Île-de-France 75002

01.76.44.01.97

www.wimi-teamwork.com/fr/

Wimi.solutions

@wimi_solutions

@Wimi_solutions

@WimiTV