EBOOK

Qu'est-ce que la directive NIS2 ?

ERCOM
Cyber Solutions by Thales

Qu'est-ce que la directive NIS2 ?

Introduction

L'évolution des sécurités des réseaux et des systèmes d'information est nécessaire à l'échelle européenne, qui montre une hétérogénéité entre les Etats-membres. Au fil des années, nous avons pu constater une évolution significative des cibles, des menaces et de leurs impacts sur la société.

En France, de nouveaux acteurs sont ciblés comme les PME, les ETI et les collectivités territoriales. D'après Capgemini, 79% des entreprises ont subi au moins une violation de données dans le cloud au cours des 18 derniers mois. Il y a **43% des entreprises françaises touchées par une attaque en 2022 contre 54% en 2021**, un chiffre qui est encore trop élevé (*source : CESIN*). Pour donner une estimation, il y a environ **13 fuites de données par jour** (*source : Baromètre 2023 des fuites de données FIC / CNIL*). De plus, d'après le Clusif, **30% des collectivités locales ont déjà été victimes de ransomwares.**

Il faut savoir que les conséquences des ransomwares sont dramatiques pour les cibles. **13 000 vulnérabilités ont été signalées en 2022** d'après NIST. **62% des organisations attaquées** en 2022 par un ransomware **payent la rançon** (*source : Hiscox)* ce qui a de lourdes conséquences financières. La France compte en moyenne seulement **1 personne chargée de la cybersécurité pour 1 500 salariés** (*source : Wavestone)*. La majorité des acteurs du marché n'ont pas les moyens et de ressources suffisantes pour contrer l'ensemble des menaces qui pèsent sur eux et les dommages s'accumulent.

C'est donc dans ce contexte et pour répondre aux menaces croissantes des cyberattaques, que **la Commission Européenne a adopté le remplacement de la directive NIS1 par NIS2 afin de renforcer les exigences en matière de sécurité, introduire des mesures de surveillance et des sanctions plus strictes**, tout en ouvrant le champ d'application. Obligeant ainsi davantage d'entités et de secteurs à prendre des mesures pour accroître le niveau de cybersécurité en Europe à plus long terme.

La directive NIS 2 offre une véritable approche pour améliorer notre réponse commune face aux cyber-risques et à leur augmentation en Europe. Sa mise en œuvre permettra à de nombreuses entités telles que les gouvernements, les institutions gouvernementales et les infrastructures nationales critiques de renforcer leur protection tout en **unifiant globalement le niveau européen de sécurité, le partage d'informations ainsi que la coopération dans la gestion des crises cybernétiques.**

Dans le cadre de la mise en œuvre de la directive NIS 2, **Cyber Solutions by Thales**, dont l'objectif est d'assurer en permanence la sécurité et la résilience des systèmes d'information critiques et des infrastructures industrielles de ses clients, vous propose **une série de livres blancs, rédigés par nos experts en cybersécurité.**

Capitalisant sur notre expertise pour accompagner les stratégies cyber et la conformité aux nouvelles réglementations telles que NIS 1, DORA, PC IDSS... Ainsi que pour aider les clients en termes de certifications de sécurité à travers le monde, nous bénéficions de notre travail conjoint avec les gouvernements, les autorités légales et les Infrastructures Nationales Critiques dans de nombreux domaines d'activités tels que **l'Industrie, l'Energie, l'Espace, la Banque, le Transport, ou encore les programmes de Défense et Souverains,** pour mieux assurer la prise en compte des spécificités de ces prochains défis apportés par NIS 2.

Notre forte présence européenne d'experts en cybernétique et notre portefeuille mondial de services et de solutions permettront de répondre à tous les besoins cybernétiques requis dans le cadre du quatrième pilier de cette nouvelle directive NIS 2, de la gouvernance à la protection, en passant par la cyberdéfense et la résilience.

SOMMAIRE

1. Contexte et évolution de la directive NIS

1.1. Directive NIS1 et ses limites

« NIS » pour Network and Information System Security désigne les mesures et politiques de sécurité des réseaux et des systèmes d'information. La **directive NIS1** a été adoptée par l'Union européenne en 2016 pour **améliorer la sécurité des réseaux et des systèmes d'information en imposant des obligations de sécurité aux opérateurs de services essentiels (OSE)** dans des secteurs tels que l'énergie, les transports, les services bancaires, la santé, etc. Les OSE se doivent de prendre des mesures de sécurité appropriées, détecter les incidents, gérer les risques et notifier les incidents graves aux autorités compétentes. **L'objectif étant de protéger les infrastructures critiques et d'assurer la continuité des services essentiels en cas d'incident de cybersécurité.**

NIS1 était le premier acte législatif majeur à l'échelle européenne portant sur la cybersécurité. L'objectif étant d'**atteindre un niveau élevé et commun de cybersécurité dans tous les Etats-membres**.
Bien que cette directive ait accru les capacités, compétences, réglementations en matière de cybersécurité, sa mise en œuvre s'est avérée difficile et a entraîné une fragmentation à différents niveaux au sein des marchés. C'est ainsi que fin 2020, la Commission Européenne a pris la décision d'**étendre le périmètre et les ambitions de NIS1 avec la mise en vigueur de NIS2 en janvier 2023.** Ainsi, des milliers de nouvelles entités à l'échelle nationale et européenne se retrouvent alors concernées par cette évolution leur permettant de mieux se protéger.

NIS2 est plus prescriptive que NIS1, avec la nécessité de préciser les exigences de sécurité et les mécanismes de régulation. Cette nécessité d'évolution est soutenue par la France et grâce à une prise de conscience collective depuis quelques années pour l'intégration des premiers éléments de base de la cybersécurité et de proportionnalité.

1.2. Objectifs et motivations derrière NIS2

Malgré la mise en place de mesures par NIS1 dans certains secteurs essentiels, le nombre d'attaques ne cessent d'augmenter. Ces derniers mois, les secteurs les plus touchés ont été l'industrie manufacturière, le secteur du conseil et le secteur technologique. De plus, les entreprises en Amérique du Nord, notamment aux Etats-Unis, ont été largement ciblées, ce qui a accentué la nécessité d'une réponse coordonnée à l'échelle internationale.
L'Europe a également été impactée, représentant **25 % du nombre total d'attaques de ransomware**, avec des pays tels que le **Royaume-Uni, l'Allemagne et la France** subissant le plus grand nombre d'attaques. Parmi les groupes de ransomware les plus actifs, LockBit, Play et Cl0p se sont démarqués. (*Source : S21 Sec*)

Face à cette réalité, la directive NIS2 a été conçue pour **renforcer la sécurité et la résilience de l'Union Européenne face aux menaces cybernétiques,** en particulier aux ransomwares. Elle vise à mettre en place des mesures de protection adéquates pour les secteurs clés de l'économie et à promouvoir une coopération internationale plus étroite pour contrer ces attaques croissantes.

L'ANSSI qui est le principal négociateur de la France au niveau européen sur les sujets cyber, se félicite de l'adoption d'une directive qui place l'Union européenne à la pointe de la cybersécurité. La directive NIS2 prévoit **le renforcement des capacités nationales** en matière de cybersécurité et crée **un cadre formel de coopération entre les Etats-membres,** auquel l'ANSSI participe activement. La directive prévoit également de **renforcer la cybersécurité des grands opérateurs de la chaîne d'approvisionnement IT et Numérique**.

Ebook| Qu'est-ce que la directive NIS2

Synthétiquement, la nouvelle directive NIS2 quatre axes :

- La mise en place de mesures de sécurité pour protéger les réseaux et systèmes d'information contre les cybermenaces.
- L'identification et l'évaluation des risques cyber.
- La coopération entre les autorités compétentes en cas d'incident de sécurité à l'échelle européenne. Synthétiquement, la nouvelle directive NIS2 prévoit quatre axes :
- L'alerte des incidents significatifs de cybersécurité auprès du CSIRT (Centre Gouvernemental de veille, d'alerte et de réponse aux attaques informatiques) dans les 24 heures puis par une notification d'incident dans les 72 heures.

2. Principales modifications apportées par NIS2

2.1. Extension du champ d'application

La directive NIS 2 offre une vraie démarche d'amélioration face au risque Cyber. Sa mise en œuvre permettra à de nombreuses entités de renforcer leur protection. Cela représentera également une occasion de **mobiliser largement le secteur économique national et le secteur public.**

De plus, elle encourage les Etats membres à renforcer leur coopération en matière de gestion des crises cybernétiques, en établissant **un cadre officiel pour le réseau CyCLONe, qui réunit l'ANSSI et ses homologues européens.**

Le nombre d'organisations concernées par NIS2 sera multiplié par dix. On peut souligner l'extension du périmètre de manière générale autour de **35 secteurs** d'activités au lieu de 19 dans NIS1.

La directive couvrira également l'**administration publique** des Etats-membres, les collectivités territoriales et l'inclusion d'une grande partie des acteurs de la chaîne d'approvisionnement IT & Numérique. Pour chaque secteur, des « types d'entités » ont été identifiés pour détourer le périmètre, ce qui correspond à des activités métiers définis sur la base de :

- La définition précise issues de réglementations déjà existantes.
- La classification européenne des activités NACE (NAF en France).
- La définition ad hoc.

L'autre critère de sélection est **la taille de l'entité.** De manière générale, on identifie les critères et seuils des entités de taille moyenne, intermédiaire ou grande avec un nombre d'employés **supérieur ou égal à 50** ou un **chiffre d'affaires/bilan annuel supérieur ou égal à 10 millions d'euros.**

En d'autres termes, toute entreprise respectant ces critères sera concernée par la directive NIS2.

Cependant, il existe **des exceptions**. La France aura la possibilité d'**intégrer unitairement,** et à la marge des entités ne respectant pas les critères sur la base d'une analyse de risque nationale. La France aura également la possibilité d'**exclure unitairement des entités** au regard de la clause de défense et de sécurité nationale prévues par la directive.

Il existe des opérateurs où ce critère de taille ne s'applique pas :

- Les fournisseurs de communications électroniques publics.
- Les fournisseurs de services de communications électroniques accessibles au public.
- Les fournisseurs de registre de domaine de premier niveau.
- Les fournisseurs de services de système de noms de domaine.
- Les prestataires de services de confiance.

Au sein de ce périmètre, **il existe des entités essentielles et des entités importantes**. Les entités essentielles et les entités importantes font référence à des catégories spécifiques d'organisations soumises à des exigences particulières en matière de cybersécurité.

L'objectif de cette distinction entre entités essentielles et entités importantes est d'adapter les mesures de cybersécurité en fonction de l'importance stratégique et de l'impact potentiel pour ces organisations, une cyberattaque.

Les entités essentielles sont considérées comme étant d'une importance critique, tandis que les entités importantes jouent un rôle significatif mais moins vital dans l'économie et la société.

2.2. Distinction entre entités essentielles et entités impotantes

D'une part, **les entités essentielles** correspondent aux entités de taille moyenne, intermédiaire et grandes faisant partie **des secteurs tels que l'énergie, les transports, la santé, les services bancaires et financiers, etc.** (Annexe 1 de la directive)
Certains critères et seuils ont été mis en place afin de savoir si une entreprise peut être considérée comme essentielle, tels que :

- Le nombre d'employés supérieur ou égal à 250

Ou

- Un chiffre d'affaires supérieur ou égal à 50 millions d'euros

Ou

- Un bilan supérieur ou égal à 43 millions d'euros

Sont également considérées entités essentielles :

- Les prestataires de services de confiance qualifiés et les registres de noms de domaines de premier niveau ainsi que les fournisseurs de services DNS, quelle que soit leur taille.
- Les fournisseurs de réseaux publics de communications électroniques publics ou de services de communication électronique accessibles au public qui constituent des entreprises de taille moyenne.
- Toute entité soumise à la directive Résilience des Entités Critiques (REC).
- Toute entité désignée Opérateur de Service Essentiel au titre de NIS 1.
- Certaines entités désignées unitairement par la France au regard de certains critères spécifiques, à la marge et concernant l'Annexe 2 de la directive.

De l'autre part, **les entités importantes** sont des organisations qui, bien qu'elles ne fournissent pas de services essentiels, **jouent un rôle significatif dans l'économie et la société.**

Les entités importantes peuvent appartenir à différents secteurs d'activité et sont également **soumises à des exigences de sécurité renforcée**, bien que moins strictes que celles imposées aux entités essentielles.

Toute autre entité du périmètre (Annexe 1 et 2 de la directive et taille moyenne et plus) qui n'est pas essentielle au regard des critères et cas précédemment exposés sera **par défaut importante.**

Annexe 1 de la Directive :

01. Energie
02. Transports
03. Secteur bancaire
04. Infrastructures des marchés financiers
05. Santé
06. Eau potable
07. Eaux usées
08. Infrastructure numérique
09. Gestion des services TIC
10. Administration publique
11. Espace

Annexe 2 de la Directive :

01. Services postaux et d'expédition
02. Gestion des déchets
03. Fabrication, production et distribution de produits chimiques
04. Production, transformation et distribution de denrées alimentaires

Voici un schéma récapitulatif simplifié de la règle de base :

Taille entité	Nombre d'employés	Chiffre d'affaires (Millions d'euros)	Bilan annuel (Millions d'euros)	Annexe 1	Annexe 2
INTERMEDIAIRE & GRANDE	x > 250	y > 50	z > 43	ENTITES ESSENTIELLES	ENTITES IMPORTANTES
MOYENNE	50 > x > 250	10 > y > 50	10 > z > 43	ENTITES IMPORTANTES	ENTITES IMPORTANTES
MICRO & PETITE	x < 50	y < 10	z < 10	NON CONCERNÉES	NON CONCERNÉES

Source : ANSSI

En conséquence, la directive NIS2 impose des **exigences spécifiques de sécurité et de gestion des risques pour les entités essentielles et les entités importantes**, afin de renforcer leur protection contre les cybersmenaces. Cela vise à **assurer la résilience des services essentiels et à prévenir les incidents de sécurité susceptible d'avoir un impact majeur sur l'économie et la société dans l'Union européenne.**

3. Impacts de la directive NIS2

3.1. Renforcement des obligations et régulations en matière de cybersécurité

Certaines exigences de la nouvelle directive seront d'application directe et d'autres devraient être soumises à un délai de mise en conformité. Néanmoins, **cette mise en conformité aura des impacts sur toutes les entités concernées et les régulateurs.**

Car la directive NIS2 implique également **le renforcement du rôle de régulateur**, pour la France, il s'agit de l'ANSSI, prévoyant une **supervision du périmètre et la remontée d'information à la Commission Européenne** ainsi que la précision de ses actions de régulation.

Il existe plusieurs obligations majeures issues de cette directive en lien avec le régulateur. Tout d'abord **la notification à l'ANSSI**. La France envisage de mettre en place un mécanisme permettant aux entités de se notifier auprès de l'ANSSI pour leur communiquer les informations de contact et de mises à jour des mesures cyber.

La déclaration de l'ANSSI sur les incidents majeurs de NIS1 sera conservée, mais en ajoutant plusieurs étapes comprenant **la notification, le rapport d'avancement et le rapport final.**

Au regard de l'ANSSI, il est important en tant que régulateur de **conserver une mission d'accompagnement tout en intégrant la capacité de sanction et en renforçant l'activité de contrôle**. Le but étant d'adapter l'accompagnement aux nouvelles entités régulées et de développer des services numériques ainsi que des relais locaux et industriels.

Au-delà de son rôle de régulateur, l'ANSSI se doit de respecter les grands principes directeurs lors de la transposition nationale. Par exemple, les délais de transposition nationale seront fixés par l'Union Européenne, avec une participation aux travaux d'harmonisation européenne.
Il y aura également la création d'un dispositif qui ait un réel impact sur la sécurisation des entités et la co-construction avec les secteurs concernés. Les derniers principes sont de s'assurer de **la prise en compte de la diversité des situations des entités et d'informer les futurs écosystèmes régulés tout au long de la transposition dans le droit national.**

Les acteurs du numérique ne seront pas soumis aux mêmes exigences relatives aux mesures de sécurité transposées à l'échelle européenne. Ils seront soumis à un acte d'exécution publié par la Commission européenne au plus tard le 17 octobre 2024 qui précisera les mesures à appliquer.

Certains délais de mise en conformité sont fixés par la directive et d'autres sont laissés à l'appréciation des Etats-membres. Les délais non fixés par la directive feront partie des sujets instruits lors des consultations avec l'écosystème des futures entités régulées.

3.2. Changements majeurs dans les obligations et les pratiques cyber

L'introduction de la directive NIS2, entraîne des changements majeurs dans les obligations et les pratiques en matière de cybersécurité.

Pour les RSSI (Responsables de la Sécurité des Systèmes d'Information) et les directeurs techniques, la directive **NIS2 impose de nouvelles responsabilités**. Les RSSI doivent veiller au respect des nouvelles obligations de sécurité, notamment en mettant en place des mesures appropriées pour protéger les réseaux et systèmes d'information contre les cybermenaces.

De plus, ils doivent se conformer aux exigences de notification des incidents, en signalant les incidents significatifs dans les délais prévus. **Les RSSI doivent maintenir une communication étroite avec les autorités compétentes** désignées par la directive NIS2, telles que l'ANSSI en France, afin de coopérer efficacement en cas d'incident de sécurité.

Les directeurs techniques, quant à eux, s**ont chargés de superviser le développement et la mise en œuvre de solutions technologiques conforme aux nouvelles réglementations.** Ils doivent s'assurer que l'infrastructure technologique de leur organisation est en conformité avec les exigences de sécurité renforcées. Ils ont également pour **rôle de soutenir les stratégies de cybersécurité de l'organisation en collaborant avec les RSSI et d'autres parties prenantes.**

Les organisations concernées par la directive NIS2 ont de nouvelles obligations à respecter. Elles doivent mettre en place des mesures de sécurité adéquates pour protéger leurs réseaux et systèmes d'information contre les cybers menaces.

Cela implique l'identification et l'évaluation régulières des risques liés à la cybersécurité. Les organisations doivent coopérer pleinement avec les autorités compétentes en cas d'incident de sécurité, en fournissant les informations nécessaires et en contribuant aux enquêtes.

De plus, elles doivent **notifier les incidents significatifs de cybersécurité dans les délais prescrits, en effectuant une alerte initiale auprès du CSIRT** (Centre Gouvernemental de veille, d'alerte et de réponse aux attaques informatiques) dans les 24 heures suivant la découverte de l'incident, puis en fournissant une notification d'incident détaillée dans les 72 heures. Ces obligations visent à améliorer la détection, la réponse et la gestion des incidents de cybersécurité.

3.3. Sanctions administratives et financières

La directive NIS2 prévoit des sanctions en cas de non-respect des obligations. Les sanctions peuvent prendre différentes formes, telles que **des amendes administratives dont le montant peut atteindre 10 millions d'euros ou 2% du chiffre d'affaires total annuel de l'organisation.**

Les sanctions peuvent également inclure **des sanctions pénales ou des mesures de réparation**. Les Etats membres sont chargés de veiller à ce que les sanctions soient efficaces, proportionnées et dissuasives.

Pour se préparer à la directive NIS2, les entreprises et les administrations doivent prendre plusieurs mesures. Tout d'abord, elles doivent s'assurer de respecter les obligations de la directive NIS1 en attendant la transposition de la directive NIS2 en droit national. Les entités déjà concernées par la NIS1 doivent poursuivre leurs efforts de conformité et s'assurer de maintenir un niveau de sécurité adéquat.

De plus, il est essentiel d'entamer dès maintenant une démarche proactive pour améliorer la sécurité informatique. Cela peut inclure l'évaluation du niveau de maturité en matière de cybersécurité, l'identification des lacunes et la mise en place de mesures correctives. Les entreprises peuvent également bénéficier de l'expertise de prestataires qualifiés pour les accompagner dans leur transformation et les aider à se conformer aux exigences de la directive.

NIS 2 est une nouvelle avancée dans l'amélioration de la sécurité des entreprises et organisations. Dans un contexte géopolitique incertain, les PME et collectivités territoriales, notamment, vont subir un choc de gouvernance et d'organisation dans les prochains mois. Ce choc sera d'ailleurs majeur, puisque selon le député néerlandais Bart Groothuis, c'est plus de **160 000 entités qui devront renforcer leur sécurité**. Pour absorber ce choc, ces acteurs devront s'entourer de prestataires qualifiés pour les accompagner dans leur transformation.

4. Focus sur les administrations publiques

4.1. Administration publique, un secteur critique

L'administration publique en France, comme en Europe offre à tout à chacun, citoyen comme entreprise, des services essentiels : sécurité, social, économie, politique...

Elle traite et gère des quantités de données et d'informations sensibles, faisant d'elle une cible de choix pour les cyberattaques. Ainsi, **NIS2, reconnaît les administrations publiques comme une entité essentielle à protéger.**

Mais pour parvenir à se conformer à la directive, elles doivent faire face à de nombreux enjeux :

- **Multiplication des attaques par ransomware** perturbant les services essentiels pendant de longues périodes.
- **Ressources limitées** avec peu de profils experts en cybersécurité, peu de moyens informatiques de pointes.
- **Attaques par phishing récurrentes** pour récupérer de grandes quantités de données personnelles.
- **Systèmes informatiques complexes**, difficiles à sécuriser et vulnérables aux cyberattaques.
- **Manque de sensibilisation du personnel** sur les menaces cyber accentuant les vulnérabilités.

Autant de failles de sécurité dans ce secteur qui compromettent les informations sensibles de millions de citoyens et d'entreprises, ainsi que la perturbation voire le déni de services essentiels, qu'apportent ces administrations au niveau local, national et européen.

La directive vise donc à améliorer les mesures de protection envers les administrations et à éliminer les divergences qui peuvent exister entre les Etats-membres.

Les mesures principales prévues par NIS2 pour les administrations :

- **Protection des données sensibles** : mise en œuvre de mesures de sécurité renforcées pour protéger les informations sensibles (données personnelles, informations financières, données sur les infrastructures critiques).
- **Evaluation continue des risques** : obligation de procéder à des évaluations des risques de manière régulières et de rendre compte de leur situation aux autorités compétentes.
- **Sécurité informatique et gestion des vulnérabilités** : gérer la cybersécurité tout au long du cycle de vie des réseaux et SI, élaborer, déployer et analyser la performance des mesures de cybersécurité nécessaires.
- **Continuité des services** : chaque administration devra mettre en œuvre toutes les mesures nécessaires pour garantir la continuité de ses services en cas d'incident ou de cyberattaques.
- **Sensibilisation** : le secteur de l'administration publique se doit d'investir dans la formation de cybersécurité de ses agents.
- **Prise en compte de sa chaîne d'approvisionnement** : les administrations doivent être informées des mesures et du niveau de cybersécurité de ses fournisseurs et de les obliger à s'améliorer s'ils ne respectent pas les mêmes standards.
- **Mise en place de politiques SI** : NIS2 exige l'élaboration de politiques et procédures pour soutenir toutes les mesures cyber mises en place par chaque administration. Elles ont pour objectif d'offrir un socle commun à tous les agents publics sur leurs devoirs et obligation afin de garantir la sécurité.

Ces exigences NIS2, qui seront imposées aux administrations, nécessiteront une phase de mise en conformité plus au moins longue, en fonction de la maturité de chacun. Néanmoins, cela est nécessaire au secteur public et à ses administrations afin de garantir leur sécurité.

HEXATRUST
CYBERSECURITY & DIGITAL TRUST

AVIS D'EXPERT

4.2. Risque cyber des collectivités dans l'œil de NIS2 et de France Relance

Sartrouville, Métropole de Lille, Chevilly-Larue... Les collectivités sont loin d'être à l'abri des cyberattaques. Mal équipées et mal sensibilisées au risque cyber, dans un contexte de recours accru au numérique, elles sont des cibles de choix pour les cyberattaquants. En effet, dans le Panorama de la Cybermenace 2022 de l'ANSSI, **les collectivités territoriales et locales représentaient près de 23% des victimes de rançongiciels l'an passé.** Or, les cyberattaques représentent un réel coût pour les collectivités et les communes, avec un impact sur leur activité. Par exemple, l'attaque qu'a connue Lille a coûté plus d'un million d'euros à la collectivité entre mars et juin 2023.
Mais au-delà, le coût réel reste encore aujourd'hui difficile à estimer, puisque l'on oublie souvent de comptabiliser les coûts indirects, comme la gestion des ressources humaines, les frais d'avocats en cas de litige ou la hausse des frais d'assurance à laquelle les collectivités peuvent s'exposer en cas d'incident.

En dehors de ces coûts, les cyberattaques ont aussi des conséquences moins quantifiables, mais tout aussi dommageables : **perturbation et dysfonctionnement des services publics locaux, fuite de données à caractère personnel, perte des données parfois irrémédiables, atteinte à l'image et à la réputation, altération du lien de confiance tissé avec le citoyen, impact psychologique de l'attaque sur les agents et l'équipe en charge de l'informatique**... Pour éviter tout cela, il convient donc aux pouvoirs publics d'accompagner les collectivités dans le développement de leur cyber résilience, et ce, de manière énergique.

Face à cette nouvelle réalité à laquelle font face les collectivités, l'Union Européenne a décidé d'agir. En effet, la directive NIS2, publiée en décembre 2022, prévoit de **renforcer la cybersécurité des acteurs publics et privés européens en les forçant à s'équiper et à acquérir les bons réflexes en cas de cyberattaques.** Étant donné que l'administration publique fait partie des 18 secteurs concernés par la directive, les collectivités seront donc concernées par les actions à mettre en place. La transposition de cette directive **NIS2 devant être effective pour octobre 2024**. Il revient au législateur de préciser la liste des entités concernées.

En France, la démarche est à l'accompagnement. Le gouvernement a prévu **un volet cyber au programme France Relance afin d'aider les collectivités dans leur effort de cybersécurisation.** C'est dans ce cadre que l'ANSSI a proposé en 2022 aux acteurs publics volontaires plusieurs offres de services : un dispositif visant à **cofinancer des projets et des Parcours de cybersécurité** de systèmes d'information avec un accompagnement financier à l'investissement, un dispositif d'acquisition de produits et de licences mutualisés et méthodologique à la création de c**entres régionaux de réponse à des incidents cyber** (CSIRT). Ce volet cyber prévoit un **investissement de 60 millions d'euros destiné aux collectivités.**

Dans l'optique d'améliorer la lisibilité de l'offre Cyber, la filière a également créé des rencontres entre offreurs et utilisateurs tels que la **Journée Autonomie et Souveraineté Numérique.** Le groupement **Hexatrust a également publié un catalogue permettant aux Collectivités et aux Etablissements de Santé de trouver les solutions appropriées à leur parcours Cyber.**

La cybermenace qui plane au-dessus des collectivités semble avoir été pris en compte par les pouvoirs publics, tant au niveau européen que national, avec une action concertée de l'Etat, des industriels et des utilisateurs au niveau de la Filière Cyber des Industries de Sécurité. Si ces démarches de cybersécurité et les déploiements demanderont du temps et des investissements, le mouvement est enclenché, avec au bout du cercle vertueux, un futur numérique durable où les collectivités pourront soit échapper aux cyberattaques, soit amoindrir leurs conséquences. De quoi faire du numérique, un moyen d'améliorer les services publics, et la vie de tous au quotidien.

5. Quelques conseils pratiques pour se conformer

5.1 Evaluation des risques et sensibilisation du personnel

L'ANSSI conseille à chaque entité de se préparer dès aujourd'hui pour construire une base solide et pérenne en matière de cybersécurité. Chaque acteur de la cybersécurité, est mobilisé pour **accompagner les entités vers cette nouvelle directive et la mise en place d'actions concrètes.**

L'objectif commun restera toujours **d'élever le niveau de sécurité numérique en France en se protégeant au mieux face aux multiples menaces**. L'objectif étant d'élever le niveau de sécurité numérique en France et de protéger au mieux les infrastructures, les données et les systèmes d'information.

Pour y parvenir, il est **essentiel** d'évaluer les risques spécifiques auxquels chaque entité peut être exposée. **Une évaluation approfondie des vulnérabilités et des points faibles du système informatique permettra d'identifier les mesures de sécurité les plus appropriées à mettre en place**.

CyberSolutions by Thales peut accompagner les entreprises et les administrations publiques à adapter ou mettre en place leur stratégie de sécurité pour se conformer à cette nouvelle directive.

Autour de 5 pilliers : Identifier, Protéger, Détecter, Répondre et Rétablier, **CybersSolutions by Thales** joue un rôle clé en fournissant des solutions adaptées aux besoins de chaque entité pour atténuer les risques et renforcer la résilience face aux attaques potentielles.

En parallèle, il est primordial de **sensibiliser les équipes sur l'importance et les enjeux de la sécurité numérique.** La sensibilisation des équipes est un volet crucial pour faire face aux multiples menaces.

Cela implique de former les collaborateurs aux **bonnes pratiques** en matière de sécurité informatique, de les **sensibiliser aux risques** liés aux cyberattaques, et de les inciter à **adopter des comportements responsables** et vigilants dans leur utilisation des outils numériques.

Enfin au-delà des mesures techniques, opérationnelles et organisationnelles à mettre en place ou renforcer par les entités, il est **nécessaire de mettre à disposition les bons outils sécurisés** et de former les collaborateurs ou agents administratifs **pour développer les bons réflexes et usages.**

Ebook| Qu'est-ce que la directive NIS2

5.2 Ressources disponibles pour les entreprises et administrations

ERCOM joue un rôle clé en fournissant des solutions adaptées aux besoins de chaque entité pour atténuer les risques et renforcer la résilience face aux attaques potentielles. Grâce à notre expertise pointue, nous proposons des solutions sur mesure. Nous avons développé une gamme complète de solutions simples et certifiées en réponse aux besoins croissants des entreprises et administrations en matière de communications sécurisées.

Notre portefeuille de solutions d'Ercom inclut :

Citadel Team est une solution collaborative professionnelle multi-terminaux sécurisés. Discussions, téléphonie et visioconférence avec Citadel Team, c'est l'alternative de confiance aux solutions de messagerie instantanée grand public. Créez des salons de discussions pour vos équipes, peu importe leur volume. Boostez la communication en invitant plusieurs milliers de membres dans des salons de discussions dédiés ! Discutez en privé avec chacun de vos collaborateurs internes et conviez des partenaires externes. Afin de garantir l'entière confidentialité et une totale étanchéité entre nos clients, chaque entreprise bénéficie d'une infrastructure dédiée opérée par Thales et hébergée en France. Activé quand nécessaire, le chiffrement de bout-en-bout garantit que seuls vos appareils puissent déchiffrer vos messages.

Cybels Hub DR est la plateforme collaborative sécurisée sur le cloud pour collaborer au niveau « Diffusion Restreinte ». C'est un écosystème intégré par la TrustNest Restricted Platform permettant à des entités de collaborer entre elles en toute sécurité et confidentialité. Les entités peuvent offrir le service Cybels Hub DR à tous les collaborateurs de leur réseau « Diffusion Restreinte» grâce à une interconnexion. Ce service réunit, dès lors, les solutions Citadel et Cryptobox sur une seule plateforme afin de faciliter et booster la collaboration entre clients et partenaires dans le cadre de l'échange de données sensibles ou confidentielles.

Cryptobox, est la solution de travail collaboratif et de transfert de fichiers agréée Diffusion Restreinte par l'ANSSI* qui chiffre vos données de bout en bout, disponible dans n'importe quel environnement, Cloud ou On Premise. Vos documents sont alors accessibles de manière totalement sécurisée depuis votre PC, smartphone et tablette. Aucun risque de piratage de vos données puisqu'elles sont chiffrées depuis votre terminal jusqu'au stockage et que votre mot de passe n'est stocké sur aucun serveur.
Partagez, collaborez et échangez vos documents chiffrés de bout en bout avec les collaborateurs ou les partenaires externes. *(renouvellement en cours)*

Cryptosmart Mobile est l'unique solution, développée en partenariat avec SAMSUNG, qui sécurise vos communications, données, terminaux mobiles, avec un niveau de sécurité élevé (agrément Diffusion Restreinte délivré par l'ANSSI*), sur des smartphones et tablettes grand public de dernière génération. Grâce au chiffrement de bout en bout, vos données sont protégées contre les risques d'interception des communications, la perte ou de vol de votre smartphone.

Pour faire face aux nouveaux enjeux de mobilité et de travail à distance, Ercom a développé **Cryptosmart PC,** une solution souveraine de VPN pour sécuriser les connexions de vos ordinateurs Windows distants, avec un niveau de sécurité gouvernemental.

Dans l'ensemble, l'adoption de ces solutions permettront de renforcer la sécurité communications et réduire les risques de cyberattaques et de fuites de données, renforçant ainsi la confiance des clients, des partenaires et des autorités réglementaires envers l'entreprise.

EN SAVOIR PLUS

Cyber Solutions by Thales

Ercom est une entité de **Cyber Solutions by Thales, leader européen de la cybersécurité et leader mondial de la protection des données.**

Thales accompagne les organisations pour les aider à répondre à leurs besoins de cybersécurité, quels que soient leur domaine d'activité, le niveau de confidentialité de leurs données ou les exigences réglementaires spécifiques à chaque pays, et pour leur apporter **une cybersécurité qui apporte de la valeur à leur cœur de métier** et leur permet de capter les dividendes du numérique.

Thales est un acteur opérationnel de la cybersécurité sur l'ensemble de la chaîne de valeur des données et compte **plus de 40 ans d'expertise** en cybersécurité.

Répondant aux réglementations mondiales et aux besoins de cybersécurité pour les domaines critiques, **Thales propose une gamme complète de solutions et de services de cybersécurité** qui répondent à l'évolution des menaces auxquelles sont confrontées les entreprises et les infrastructures critiques. Qu'il s'agisse de l'**évaluation des risques et des menaces, de la sécurité dès la conception, de la cyberformation, des capacités avancées de détection et de réponse aux menaces, de la cyber intégration, des communications sécurisées ou de la protection des réseaux et des données**, Thales est à l'avant-garde du secteur de la cybersécurité et veille à ce que ses clients soient hautement protégés contre les cyber menaces les plus récentes.

Evaluation des risques et des menaces

Identifier les risques et les priorités de votre organisation en matière de cybersécurité

>

Protéger

Notre mission est de fournir des solutions cryptographiques et d'authentification haut de gamme

>

Détecter et Répondre

Fortement personnalisés pour répondre aux besoins spécifiques des environnements IT, OT, Multi Cloud...

>

Entrainer et Expérimenter

Une offre complète de cyber sécurité visant à former, tester et favoriser l'entrainement des équipes cyber

>

Vous voulez en savoir plus sur les solutions, actualités et CyberInsights ?

DÉCOUVREZ LE NOUVEAU SITE INTERNET DÉDIÉ

sales_cybersec_web@ercom.fr

www.ercom.fr