

LE GUIDE ULTIME DE SURVIE CYBER V2

OU COMMENT NAVIGUER DANS LA NIS 2 (ET PLUS)

EN TOUTE SÉRÉNITÉ

Propulsé par

SPAC >ALLIANCE<

STid

SPAC
>ALLIANCE<

Nous sommes une alliance professionnelle européenne regroupant de nombreux experts de la sécurité physique et logique ainsi que des agences nationales comme l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information). Depuis notre création nous œuvrons pour aider à définir la souveraineté numérique européenne et participons à l'établissement de standards construits sur des solutions technologiques ouvertes et interopérables.

Notre démarche accompagne les ambitions du grand plan d'action européen relatif à la décennie numérique 2030 (Digital Decade Policy Program 2030). Ce dernier place la cybersécurité comme préalable à l'indépendance numérique de l'UE, une thématique particulièrement traitée dans plusieurs directives récentes, dont la fameuse NIS 2 (Network and Information Security 2) que vous allez pouvoir vous approprier facilement en parcourant ce guide.

EN EFFET PLUSIEURS QUESTIONS VOUS BRÛLENT CERTAINEMENT LES LÈVRES :

- Suis-je concerné par cette règlementation ?

- Quelles seront mes obligations ?

- Comment les agences nationales vont-elles transposer ces directives dans les droits nationaux ?

- Quand devrais-je être prêt le cas échéant ?

- Qui pourra m'accompagner dans la mise en place de cette régulation ?

Au-delà des recommandations générales données par l'ENISA, il sera nécessaire d'appliquer les lois et décrets votés par chaque État membre afin de vous mettre en conformité d'ici 2027. Les conseils et outils proposés dans notre guide vont vous simplifier la tâche !

SPAC Alliance s'engage à tenir ce document à jour en réalisant une veille pro-active sur les dernières informations disponibles.

Abonnez-vous pour recevoir les dernières mises à jour !

JE M'ABONNE

Comprendre la régulation européenne, c'est avoir à l'esprit que nous tous, citoyens, entreprises, syndicats, associations, institutions, administrations, et Etats de l'Union Européenne, sommes des acteurs ayant une responsabilité, un rôle à jouer pour définir cette souveraineté.

Notre réussite collective dépendra de la pertinence de nos actions individuelles.

TABLE DES MATIÈRES

1. **QUAND ALLEZ-VOUS ÊTRE ATTAQUÉ ?** 4

2. **UNE RÉGLEMENTATION QUI NOUS PROTÈGE** 5
   - A. La NIS 1, les fondations de la cybersécurité européenne, orientée sur la sensibilisation 5
   - B. NIS 2 : la notion du bout en bout 5

3. **ÊTES-VOUS CONCERNÉ PAR LA RÉGULATION ?** 6
   - A. Quelle entité êtes-vous ? 6
     - 1. Entités Essentielles et Importantes (NIS 2) 6
     - 2. Entités Critiques (REC) 7
   - B. Le tableau ULTIME pour tout comprendre 7

4. **SURVIVRE EN ENVIRONNEMENT HOSTILE** 8
   - A. Evaluez vos risques 8
   - B. EC / EE / EI : quelles seront vos obligations ? 9
     - 1. La réponse aux menaces physiques 9
     - 2. Le protocole de communication : un lien entre physique et logique 10
     - 3. La réponse aux menaces logiques 11

5. **SE PROTÉGER ENSEMBLE CONTRE UNE MENACE SANS FRONTIÈRE** 12
   - 1. Un maillage transfrontalier 13
   - 2. Déclaration obligatoire d'incident 14
   - 3. Des amendes dissuasives 14

6. **TRANSPOSITION DANS LES DROITS NATIONAUX** 15

7. **CONCLUSION : INVESTIR POUR PRÉPARER NOTRE FUTUR** 15

8. **ANNEXES :** 16
   - A. NIS 2 : secteurs et sous-secteurs concernés 16
   - B. REC : quelles sont les entités et secteurs concernés 17
   - C. Agenda NIS 2 / REC 18
   - D. Fiche Pratique : que faire si je suis cyber-attaqué ? 18
   - E. Liens utiles 19
   - F. Listing des agences nationales de sécurité 20

1

QUAND ALLEZ-VOUS ÊTRE ATTAQUÉ ?

OUI ! OUI ! VOUS AVEZ BIEN LU !

LA QUESTION N'EST PAS DE SAVOIR SI VOUS ALLEZ ÊTRE ATTAQUÉ, MAIS QUAND.

La proportion d'acteurs touchés par des cyberattaques suit une tendance infernale. Elle dépassait les **50% en 2021.** Et a atteint, selon une étude de Dell Technologies (Global Data Protection Index), près de **9 entreprises sur 10 en 2022**.

Des attaques sans distinction de taille, ni de secteur, tout un chacun est concerné par cette montée en puissance de la cybercriminalité, y compris les particuliers.

DES CONSÉQUENCES SOUVENT DÉSASTREUSES

La majorité des entreprises qui perdent leur système informatique ou le contrôle de leurs données durant plus d'une semaine fait faillite à court terme.
Quelques chiffres pourront vous donner une idée précise des sommes qui sont en jeu.

Depuis 2015, le coût des attaques cyber ne cesse de croître passant de **3000 milliards de dollars à 6000 en 2021**, et la prévision pour 2025 dépasse les **10000 milliards** selon Cybersecurity Ventures. Cela représente un peu plus de 10% du PIB mondial, l'équivalent de la troisième puissance économique !



10 000 MILLIARDS EN 2025
90% des entités touchées
impacts directs et indirects

L'IMPACT DOIT ÊTRE CONSIDÉRÉ À PLUSIEURS NIVEAUX, ET DÉPASSE LARGEMENT LES QUESTIONS MONÉTAIRES :

- Coût d'une éventuelle rançon (qu'il est fortement recommandé de ne jamais payer)
- Coût d'un arrêt de votre activité sur une période qui dépendra de la gravité de l'attaque
- Coûts liés à d'éventuelles poursuites judiciaires si votre responsabilité est engagée (vol de données à cause d'une protection insuffisante)
- Augmentation des primes d'assurance à la suite d'un cyber-incident
- Impact direct et à long terme sur votre image (perte de réputation et de crédit) au sein de votre écosystème : utilisateurs, partenaires commerciaux, banques et investisseurs ou encore salariés
- Impact d'une perte d'avantage concurrentiel : vol de résultats de recherches ou de technologies non brevetées, divulgation de plans stratégiques, copie de produit…
- Infection possible de tous les systèmes d'information liés au votre, dont ceux de vos fournisseurs et clients

Prenez quelques minutes pour évaluer, même grossièrement, ces coûts directs et indirects en ce qui vous concerne. Maintenant que nous avons toute votre attention, allons regarder cette règlementation de plus prêt.

EN BREF : **économie hyperconnectée et menace cyber omniprésente : tous les éléments sont réunis pour que des secteurs entiers soient menacés par un effet domino dévastateur, et plus seulement des acteurs indépendants. Cette mission, puisqu'il FAUT l'accepter, est plus que jamais collaborative.**

2

UNE RÉGLEMENTATION QUI NOUS PROTÈGE

A. LA NIS 1, LES FONDATIONS DE LA CYBERSÉCURITÉ EUROPÉENNE, ORIENTÉE SUR LA SENSIBILISATION

Depuis sa création, l'UE a été confrontée à une succession d'évolutions technologiques qui ont profondément modifié notre mode de vie, notre manière d'échanger et de travailler : numérisation de l'économie, téléphonie mobile, internet haut-débit, ou encore développement du travail nomade. Cette digitalisation débridée crée autant de nouvelles portes d'entrées potentielles pour les hackers mal intentionnés.

Ces avancées ont toujours été accompagnées de régulations afin de protéger utilisateurs, entreprises et infrastructures. Leur but ?

Assurer la souveraineté européenne, notamment sur le plan du numérique et de la cybersécurité.

Sur ce dernier point l'UE a d'abord misé sur la **NIS 1** (Network and Information Security 1), régulation limitée aux acteurs les plus critiques. Une stratégie bénéfique qui n'a cependant pas débouché sur un niveau de résilience suffisant. Plusieurs explications à cela ont été avancées : pas assez d'acteurs concernés, manque de coordination entre les Etats et, comme nous l'avons vu, une évolution importante de la nature et du volume des attaques.

B. NIS 2 : LA NOTION DE BOUT EN BOUT

De ce constat, la nouvelle directive européenne introduit le concept de sécurité de bout en bout détaillé dans la **NIS 2**. Il s'articule autour de trois axes forts pour assurer l'investissement total de tous les acteurs, depuis la sensibilisation jusqu'à l'action et la coopération à l'échelle européenne.

Terminé le temps de l'individualité ! L'UE apporte une réponse complète aux menaces cyber par :

- **L'augmentation importante du nombre de secteurs** visés par les textes, impliquant beaucoup plus d'acteurs. On va même y ajouter la supply chain de ces derniers, démultipliant encore la portée de ces régulations. Selon l'ANSSI, le nombre d'acteurs concernés (en France) passerait de **500 à plus de 15 000**.
- Un **accompagnement coordonné et obligatoire** depuis la prévention jusqu'aux actions transfrontalières impliquant toutes les parties prenantes. Les états doivent définir des politiques de prévention à destination de tous les citoyens.
- Une prise en compte des **menaces logiques et physiques** qui pèsent sur les systèmes d'information : le contrôle des accès ou la vidéosurveillance s'ajoutent aux mesures classiques de cybersécurité.

Ainsi, la cybersécurité doit être appréhendée de manière :

GLOBALE :
c'est l'affaire de tous, du simple utilisateur aux institutions européennes (en passant par tout le tissu économique, industriel et social).

COORDONNÉE :
une coopération au-delà des frontières est nécessaire pour répondre à un danger qui n'en a pas.

OBLIGATOIRE :
attention à ceux qui ne respecteraient pas la directive ! Les entreprises et leur gérant s'exposent à des amendes pouvant atteindre 2% du CA mondial.

ACTIVE :
il ne suffit pas de connaitre et d'être sensibilisé au problème, mais aussi d'être formé à agir en cas d'attaque. Cela passe par une définition claire des règles d'actions de manière coordonnée pour en optimiser l'impact.

COMPLETE :
le monde cyber ne se limite pas au monde digital.
Un lecteur d'accès, une clé USB trouvée par terre, une intrusion physique peuvent créer une faille dans le système malgré toutes les protections numériquement mises en place.

EN BREF :

L'UE a tiré les leçons des premiers textes et propose plus qu'une simple évolution règlementaire.

La nouvelle vision est globale : plus d'acteurs concernés, considération de toutes les types de menaces, formation de tous et accompagnement transfrontalier.

3

ÊTES-VOUS CONCERNÉS PAR LA RÉGULATION ?

DEUX TEXTES MAJEURS DÉFINISSENT LES RÈGLES QUI SONT APPLICABLES DEPUIS LE 17 OCTOBRE 2024.

La **NIS 2** et la **REC** (Critical Entities Resilience, Directive EU 2022/2557) définissent les entreprises qui sont plus ou moins critiques pour la sécurité globale européenne. Ce niveau de criticité s'accompagne d'obligations proportionnées selon des principes que nous détaillerons plus loin.

Vous comprendrez aisément qu'un datacenter hébergeant 20% des données françaises est bien plus critique (au niveau cyber) que la boulangerie de votre quartier, ou qu'un grand fabricant de chips français (qui sera néanmoins soumis à d'autres directives européennes sur la sécurité alimentaire – nous vous épargnons à ce stade).



SANS PLUS ATTENDRE, DÉCOUVRONS LES 3 NIVEAUX DE CRITICITÉ INTRODUITS PAR LES TEXTES :

Les **Entités Critiques (EC)**, définies par la CER, sont constituées des acteurs qui fournissent des services indispensables pour maintenir les fonctions sociétales vitales, les activités économiques, les services de santé ou de sécurité publique. C'est par exemple le cas de certaines entités actuellement classées OIV (Opérateur d'Importance Vitale) et des plus grandes entreprises des secteurs concernés par la règlementation.

Entités Essentielles (EE) et **Entités Importantes (EI)**, définies par la NIS 2, regroupent la majorité des acteurs avec des obligations graduées et adaptées aux moyens et à la criticité de chacun. Les actuels OSE (Opérateurs de Services Essentielles selon la NIS 1) seront automatiquement des EE. Pour les autres, tout dépend du secteur et de la taille de l'entité concernée.

Afin de savoir si vous êtes potentiellement concerné par l'une de ces règlementations, il faut valider que vous appartenez à l'un des secteurs retenus et que vous répondiez à certains critères de taille, de chiffre d'affaires ou de résultat.

Rassurez-vous, nous avons compilé tout cela dans un tableau ultime à la fin de ce chapitre !

Afin de savoir si vous êtes concerné, entrez en contact avec votre agence nationale de cybersécurité. La plupart des pays proposent un outil permettant de savoir si vous êtes dans le scope NIS 2 / REC.
Retrouvez la liste des agences nationales en Annexe de notre guide !

A. QUELLE ENTITÉ ÊTES-VOUS ?

1. ENTITÉS ESSENTIELLES ET IMPORTANTES (NIS 2)

La NIS 2 passe le nombre de secteurs concernés à 18 (contre 7 pour la NIS 1).
Vous serez (normalement) désigné Entité Essentielle si :

- Vous êtes actuellement un Opérateur de Service Essentiel (NIS 1) au 16 janvier 2023.
- Vous appartenez à l'un des 11 secteurs hautement critiques et êtes une grande entreprise (CA > 50M € ou résultat > 43 M € ou plus de 250 salariés).

Vous serez (possiblement) désigné Entité Importante si :

- Vous appartenez à l'un des secteurs concernés (11 hautement critiques ou 7 critiques)
- Et que votre entreprise réalise plus de 10 M € de CA ou de résultat, ou compte plus de 50 salariés.

Selon le principe de chaîne de responsabilité, quelle que soit votre taille vous pourrez être désigné EE ou EI si :

- Vous êtes le seul prestataire d'un service essentiel.
- Vous appartenez à la chaîne d'approvisionnement d'une entité particulière qui peut être atteinte à travers vous.

2. ENTITÉS CRITIQUES (REC)

Comme son nom l'indique la REC concerne spécifiquement les acteurs les plus stratégiques de 12 secteurs listés dans le texte. Si vous êtes concerné, vous pourrez devenir une Entité Critique (EC) sans distinction de taille.

Toujours selon le principe de chaîne de responsabilité, et quelle que soit votre taille, vous pourrez être concerné par la REC si vous appartenez à la chaîne d'approvisionnement d'une EC qui peut être atteinte à travers vous.

Enfin (juré, c'est le dernier), si vous fournissez des services essentiels dans 6 états membres ou plus, vous aurez un statut d'Entité Critique d'Importance Européenne Particulière induisant une surveillance continue par les agences nationales de sécurité afin de vérifier la bonne application des textes.

B. LE TABLEAU ULTIME POUR TOUT COMPRENDRE

Liste des secteurs hautement critiques (NIS 2 + CER)	Type d'entités			Liste des secteurs critiques (NIS2)	Type d'entités
	Haute criticité	CA			
		>50M€	< 50M€		
Energie	EC	EE	EI	Services postaux	EI
Transport	EC	EE	EI	Gestionnaires de déchets	EI
Secteur bancaire	EC	EE	EI	Fabrication, production et distribution de produits chimiques	EI
Infrastructures de marchés financiers	EC	EE	EI	Fabrication, production et distribution de denrées alimentaires	EI
Santé	EC	EE	EI	Fabrication de matériel	EI
Eau Potable	EC	EE	EI	Fournisseurs de services numériques	EI
Eaux usées	EC	EE	EI	Recherche	EI
Infrastructures numériques	EC	EE	EI		
Gestion des services TIC	EC	EE	EI		
Administrations publiques	EC	EE	EE		
ESPACE	EC	EE	EI		
Fabrication, production et distribution de denrées alimentaires	EC				

EC = entités critiques (REC)

EE = Entité Essentielle (NIS 2)

EI = Entité importante (NIS 2)

Derniers points importants :

- Chaque Etat peut vous désigner comme entité particulière sans considération de taille (y compris les petites et micro-entreprises).
- Les entités concernées par la REC devront aussi se conformer à la NIS 2.

4

SURVIVRE EN ENVIRONNEMENT HOSTILE

SI VOUS VENEZ D'ÊTRE DÉSIGNÉ COMME EE, EI OU EC, OU SI VOUS SOUHAITEZ AVOIR UN MEILLEUR NIVEAU DE RÉSILIENCE, VOUS DEVEZ ENGAGER PLUSIEURS DÉMARCHES DÈS MAINTENANT :

- Identifier les failles physiques et logiques.
- Définir les équipements, logiciels et process adaptés.
- Evaluer l'impact d'un incident au sein votre chaîne d'approvisionnement.
- Définir une stratégie de prévention.
- Etablir un plan de continuité / redémarrage de votre activité.

La réglementation européenne vise à sécuriser notre espace et il est toujours utile de s'y conformer, même sans obligation.

Souvenez-vous des chiffres indiqués plus haut. La question n'est pas de savoir si vous allez subir une attaque, mais quand. Que ce soit dans un but financier (rançon, revente de données), idéologique (cyberterrorisme), géopolitique (conflit russo-ukrainien) ou économique (guerre commerciale), les cybercriminels n'attendront pas que vous soyez prêt.

A. ANALYSE DE RISQUES

L'évaluation des risques est la première action à déclencher.
Si cette question est nouvelle pour vous, nous vous invitons à consulter le catalogue de prestations d'accompagnement proposées par nos membres, et réaliser un mini-audit de sécurité.

Les agences nationales de cybersécurité ainsi que de nombreux organismes européens (dont SPAC Alliance) pourront être des appuis fiables pour vous accompagner et vous guider au travers de publications, de fiches pratiques ou de formations (MOOC et webinars).

VOICI LE DÉROULEMENT TYPE D'UN AUDIT DE SÉCURITÉ ET DE SON DÉPLOIEMENT :

L'évaluation des besoins se construit depuis le référentiel de conformité NIS 2 / REC indiqué par chaque état.
En initiant une démarche cyclique d'audit, vous pourrez mieux comprendre où vous vous situez en matière de sécurité, identifier vos faiblesses et gagner en réactivité en cas de menace.
Pour les entités critiques, une stratégie de double audit (interne et externe) en continu sera obligatoire.
D'une manière générale, un suivi proportionné en fonction de votre niveau de criticité est souhaitable.



EN BREF :
**Au risque de nous répéter, même sans cadre légal la cybersécurité concerne tout un chacun.
S'y préparer le plus tôt possible et maintenir une évaluation continue garantit
un bon niveau de sécurité et permet une planification des investissements nécessaires.**

B. EC / EE / EI : QUELLES SERONT VOS OBLIGATIONS ?

SPAC Alliance regroupe de nombreux acteurs majeurs de la sécurité et accompagne continuellement le législateur. Fort de l'expérience de tous nos membres, et participant à de nombreuses commissions européennes, nous vous proposons de faire un tour d'horizon des outils et solutions nécessaires pour préparer une ligne de défense adaptée.

1. LA RÉPONSE AUX MENACES PHYSIQUES

L'article 21 de la NIS 2 est limpide. Il est nécessaire d'adopter une «approche tous risques visant à protéger les réseaux et les SI ainsi que leur environnement physique». Voici certains points qui méritent votre attention :

- Sécurisation de l'abord des locaux.
- Sécurisation de l'accès dans les locaux.
- Gestion des zones critiques (datacenter, salle blanche, machines, etc.).
- Gestion des visiteurs.
- Gestion des catastrophes naturelles.

L'ENISA suggère à tous de s'inspirer / d'intégrer l'ISO 27001 ou le NIST CSF 2.0, référentiels incluant certaines obligations en matière de sécurité physique et de contrôle des accès. Cependant, NIS 2 et REC étant des directives, chaque état propose ses propres lois, decrets et référentiels de conformité. Ces référentiels peuvent ajouter des obligations à celles imposées par l'ISO ou le CSF.

RECOMMANDATION ENISA (PAS DE CONFORMITÉ AUTOMATIQUE)	LOI, DECRET ET REFERENTIEL DE CONFORMITÉ	CERTIFICATIONS SPÉCIFIQUES (SELON CRITICITÉ)
ISO 27001 NIST CSF 2.0	PROPRE À CHAQUE PAYS	ENTITÉS CRITIQUES et certaines ENTITÉS ESSENTIELLES

Ainsi, chaque pays dispose potentiellement de sa propre réglementation et certaines différences peuvent être observées d'un pays à l'autre. Par exemple, un pays pourra considérer une certification ISO 27001 comme une présomption de conformité mais ce ne sera pas le cas de son voisin.

Une commission des 27 agences cyber européenne travail continuellement pour homogénéiser ces réfenrentielles afin de simplifier la conformité pour les entités présentes dans différents pays.

A la discrétion de chaque agence, des certifications spécifiques pourront être demandées. Par exemple, la France et l'Allemagne pourraient exiger des solutions certifiées CSPN / BSZ selon la criticité des entités.

CLIQUEZ POUR CONSULTEZ LA LISTE DES RÉFÉRENTIELS DE CONFORMITÉ

RAPPEL : EN MATIÈRE DE SÉCURITÉ PHYSIQUE, PROTÉGER REVIENT À

Décourager : clôture, panneaux de signalisation, éclairage automatique
Détecter : caméra de surveillance, détecteur de mouvement, patrouille
Retarder : verrou, multiplication des enceintes, porte de sécurité
Interdire : contrôle d'accès avec un niveau de sécurité adapté à la criticité (badge, lecteur haute sécurité, PIN Code, biométrie…)

2. LE PROTOCOLE DE COMMUNICATION : UN LIEN ENTRE PHYSIQUE ET LOGIQUE

Vous aurez pu le constater en parcourant les nombreuses menaces potentielles : le contrôle des accès est l'un des facteurs essentiels de la cybersécurité. Il représente aussi la dernière défense entre l'extérieur de votre site d'exploitation et votre système d'information. Plus précisément, le système filaire qui relie votre lecteur de badge à votre système de sécurité est un véritable lien entre l'univers logique et physique.

Clé de voûte de ce système de contrôle d'accès, le protocole de communication utilisé devra se montrer à la hauteur. Quatre standards sont majoritairement utilisés :



Si les deux premiers sont totalement obsolètes, ils représentent pourtant plus de 70 % du marché mondial et sont à proscrire. Seuls les protocoles **OSDP™** et **SSCP®** proposent aujourd'hui des niveaux de sécurité élevés mais, s'ils partagent certaines caractéristiques, des différences notoires font pencher la balance en faveur de la solution européenne.

Ainsi, les protocoles **OSDP™** et **SSCP®** partagent l'avantage d'être bidirectionnels et d'inclure des commandes permettant une gestion facile, intelligente et performante d'un écosystème complet de solutions de sécurité.
Cependant, ils s'opposent en matière de conception et de philosophie.

En effet, **OSDP™** a été pensé pour être ouvert mais n'est pas sécurisé par défaut. Une entité utilisant **OSDP™** n'a donc pas de garantie de sécurité et doit s'assurer que l'option de sécurité appelée « Secure Channel » ait bien été activée, lors du déploiement.

Tout aussi ouvert, le protocole **SSCP®** a été conçu pour fournir le plus haut niveau de sécurité possible. Avec **SSCP®**, les communications sont systématiquement authentifiées, signées et chiffrées, respectant ainsi les exigences des certifications les plus strictes (comme la **CSPN** de l'**ANSSI**, requise pour les entités les plus critiques. **SSCP®** surclasse même la version d'**OSDP™**.

Si vous avez à choisir, nous vous recommandons d'o**pter pour SSCP®**, protocole ouvert et souverain le plus intégré dans les solutions certifiées du marché, incluant la **CSPN** française.



De plus, **choisir SSCP®, c'est participer activement à la création d'une véritable forteresse européenne face aux menaces cybers** en privilégiant des solutions souveraines accompagnant ainsi l'objectif européen qui est au cœur de la NIS 2 et de la CER, un vœu que nous partageons, comme vous aurez pu le deviner !

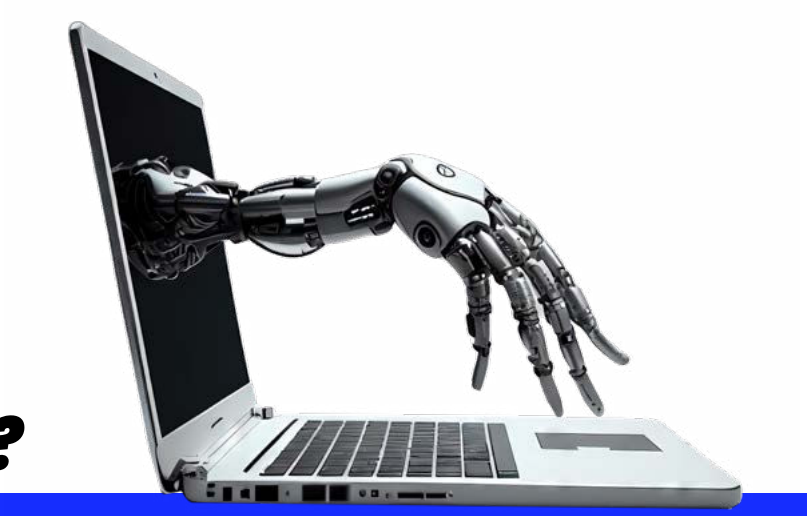
EN BREF : **La connexion entre votre lecteur et la centrale de gestion est le lien naturel entre la sécurité physique, essayer d'accéder, et la sécurité logique, essayer de corrompre. La fiabilité de toute solution de contrôle d'accès dépend directement de celle du protocole de communication qui la pilote. SSCP®, porté par SPAC Alliance, est la référence de sécurité.**

3. LA RÉPONSE AUX MENACES LOGIQUES

La défaillance humaine est la principale cause d'intrusion cyber, une réalité qui montre combien la formation et la prévention sont déterminantes lorsque l'on veut protéger de manière efficace un système d'information, qui doit lui-même être parfaitement pensé et maintenu.

Comme indiqué dans les textes, les obligations seront proportionnelles à la criticité et à la taille des entités. Ainsi, certaines contre-mesures incontournables seront applicables à tous (et fortement recommandées aux micro-entreprises et TPE hors-scope, ainsi qu'aux particuliers) :

- La formation à l'hygiène numérique et aux bonnes pratiques de cybersécurité.
- L'installation d'une suite antivirale (anti-virus, anti-spam, anti-hameçonnage).
- L'utilisation et le renouvellement régulier de mots de passe forts.
- L'utilisation d'un coffre-fort de gestion de mots de passe.
- La mise à jour automatique des postes de travail et des softwares.
- La sauvegarde des données à distance.
- Utilisation d'un pare-feu par poste afin de se prémunir des attaques par internet.
- L'utilisation de certificats sur tout site internet.



Le saviez-vous ?

L'ATTAQUE SILENCIEUSE !

Les attaques logiques sont parfois vicieuses, et certaines ont pour but de ne pas être visibles et peuvent même ne pas avoir comme objectif de voler ou d'espionner. De nombreux terminaux numérique discrètement infectés, comme le smartphone que vous avez en ce moment même dans votre poche ou votre ordinateur familial (souvent moins bien protégés), deviennent des machines relais (contrôlables à distance par un pirate) dont la puissance et/ou la mémoire seront employées pour réaliser des attaques de plus grande ampleur dont les fameux DDoS (attaque par déni de service : saturation d'un réseau ou d'un site internet par un grand nombre de connexions simultanées).

Les entités nouvellement définies par la NIS 2 (EE et EI) devront déployer une couche complémentaire de sécurité en fonction de leur statut, en voici quelques exemples :

- Désignation d'un RSSI (Responsable de la Sécurité des Systèmes d'Information).
- Traçabilité du parc informatique.
- Limitation des droits aux besoins (Administrateur, Utilisateur, Visiteur).
- Politique de gestion du travail nomade.
- Mise en place d'un pare-feu local pour protéger votre réseau.
- Chiffrage des échanges de données et utilisation d'un VPN.
- Outil de pilotage et de monitoring du système d'information.
- Contrôle d'accès physique des zones critiques (authentification pour accéder à votre datacenter).
- Simulation d'attaque pour éprouver votre process de réponse et de redémarrage.

Le saviez-vous ?



L'ATTAQUE DE LA PRISE MASQUÉE !

Que ce soit dans le cadre du télétravail ou à l'occasion d'un déplacement, le nomadisme s'accompagne de risques qu'il faut anticiper. Par exemple, l'utilisation de réseaux WIFI publics est à proscrire et vous devez utiliser un filtre de confidentialité pour empêcher la lecture de votre écran. Il faut même se méfier des prises USB à disposition dans l'espace public. Il peut sembler pratique de recharger son téléphone dans un aéroport, mais cela revient à y insérer clé USB potentiellement infectée.

Arrivent enfin les Entités Critiques de la REC qui, vous vous en doutez, devront viser l'excellence en matière de cybersécurité :

- Stratégie zero trust : authentification systématique d'un utilisateur sur une machine, et d'une machine sur un réseau.
- Interdiction de connexion de matériel externe (clé USB, disque dur, téléphone personnel).
- Cloisonnement des réseaux et des sauvegardes pour limiter toute propagation.
- Test d'intrusion par des organismes indépendants
- Audits réguliers par l'agence nationale de cybersécurité référente

Le saviez-vous ?

L'ATTAQUE COMME AU CINÉMA !

Les cas d'attaques hybrides réussies se multiplient. Leur principe est d'avoir un accès direct à une machine via, principalement, une simple clé USB qui installera directement un virus au cœur du système. De quoi contourner la plupart des protections logiques classiques et causer de nombreux dommage. Les cyber-attaquants savent mettre en pratique ce que l'on voit au cinéma !



Comme vous aurez pu le constater, quel que soit le niveau de criticité des entités les failles sont majoritairement humaines. A l'échelle de l'Europe, le rôle des entreprises est donc central pour propager les bonnes pratiques et définir une meilleure résilience et souveraineté numériques.

EN BREF : **En matière de cybersécurité, le facteur humain est la fois la plus grande menace et la meilleure solution. La formation, la bonne application des directives européennes et le maintien de l'investissement nécessaire sont les clés d'une protection efficace et durable.**

5

SE PROTÉGER ENSEMBLE CONTRE UNE MENACE SANS FRONTIÈRE

MIEUX VAUT PRÉVENIR QUE GUÉRIR : L'ACCOMPAGNEMENT EST AU CŒUR DU NOUVEAU DISPOSITIF EUROPÉEN AVEC UNE STRATÉGIE LÀ AUSSI DE BOUT EN BOUT VISANT PLUSIEURS OBJECTIFS :

- L'éducation à l'hygiène numérique et aux bonnes pratiques.
- La surveillance des réseaux.
- L'obligation de déclaration d'incident.
- La conception de solutions en cas de menace ou d'attaque, ainsi que leur diffusion.

Une stratégie notamment accompagnée par SPAC Alliance qui regroupe de nombreux experts de la question et participe activement à la définition de standards robustes en matière de sécurité.

PRÉVENTION ET DÉTECTION

Pour les EE, EI et EC, ainsi que pour tous ceux qui se trouvent en dehors du scope réglementaire, un travail important de prévention est mis en place. Son caractère obligatoire dépend du niveau de criticité de chaque entité, mais chaque pays est tenu de mettre à disposition outils et formations comme, par exemple, le **MOOC** sur les bonnes pratiques numériques développé par l'**ANSSI** en France.

En outre, l'Union Européenne investit dans plusieurs **Centres Opérationnels de Sécurité** (SOC) qui utilisent des supercalculateurs capables de détecter les malveillances à grande échelle précocement, et a créé une **Cyber Skill Academy européenne** répondant aux besoins de formation. De quoi rendre notre bouclier cyber toujours plus résistant et résiliant.

1. UN MAILLAGE TRANSFRONTALIER

Un mandat a été donné à l'**ENISA** (Agence de l'Union Européenne pour la Cybersécurité) pour mettre en place l'Unité Conjointe Cyber dont le but sera de structurer la coordination européenne et d'offrir le meilleur accompagnement possible à toutes les entités désignées (EE, EI et EC).

Ce maillage commence au cœur même de chaque entreprise avant de se déployer dans toute l'Union Européenne :

Responsable de la sécurité des systèmes d'information (RSSI) de chaque entité.

CERT (Centre gouvernemental de réponse aux incidents de sécurité informatique) pour chaque pays, et CERT EU au niveau européen.



Point de contact unique déterminé dans chaque pays et premier organisme à contacter en cas d'incident. Il pourra être un CSIRT (centre de réponse aux incidents de sécurité informatique) régional ou national. L'ANSSI prône une approche territoriale de la cybersécurité, le politique doit soutenir les entreprises de chaque région.

ENISA, CyCLONe (Cyber Crises Liaison Organisation Network).

EUROPOL : coopération policière européenne dont le Centre Européen Cybercrime.

La communication constante et bidirectionnelle doit permettre une grande efficacité dans l'identification des menaces, la recherche de contre-mesures et la transmission de connaissances.

2. DÉCLARATION OBLIGATOIRE D'INCIDENT

En cas d'incident, vous avez l'obligation de vous rapprocher d'un Point de Contact Unique qui est le déclencheur d'une procédure commune à toutes les entités :

- **Dans les 24 heures** : notification au Point de contact unique et au réseau CSIRT.
- **Rapport intermédiaire** à la demande d'une autorité ou du réseau CSIRT.
- **Dans les 30 jours :** rapport final indiquant sévérité et impact, type de menace et cause, présentation de la solution apportée.

Notez que ce point de contact unique peut être sollicité par toutes les entreprises en cas d'attaque.
Porter plainte de manière systématique est un réflexe à prendre afin de bénéficier d'un accompagnement total : enquête, indemnisation et suivi par les différents organismes précités.



3. DES AMENDES DISSUASIVES

En cas de non-respect des directives de la NIS 2, les EE et les EI s'exposent à des amendes administratives.

Pour les Entités Essentielles, le montant maximal s'élèvera à au moins **10 millions d'euros ou à au moins 2% du chiffre d'affaires mondial**, le montant le plus élevé étant retenu.

Pour les Entités Importantes, le montant maximal s'élèvera à au moins **7 millions d'euros ou à au moins 1.4% du chiffre d'affaires mondial,** le montant le plus élevé étant retenu.

Ces montants ont été calqués sur ceux généralement demandés par les hackers lorsqu'ils arrivent à crypter les données d'une entreprise.

Les sanctions applicables aux Entités Critiques seront déterminées par chaque pays. Elles devront être effectives, proportionnées et dissuasives.

EN BREF : **Vous n'êtes plus seul face à un sinistre, mais vous DEVEZ prendre des mesures pour améliorer votre niveau de cybersécurité. En cas de non-respect des textes, l'addition pourrait être très lourde, et venir s'ajouter aux coûts directs et indirects liés à une attaque réussie.**

6 TRANSPOSITION DANS LES LOIS NATIONALES

LA NIS 2 ET LA REC SONT ENTRÉES EN VIGUEUR EN JANVIER 2023, LANÇANT LE COMPTE À REBOURS DE LA TRANSPOSITION DES TEXTES PAR CHAQUE NATION MEMBRE DE L'UNION EUROPÉENNE.

Initialement attendu pour le 17 octobre 2024, le travail de transposition en lois nationales a souvent pris du retard. Il en va de même pour les décrets spécifiant les obligation pour chaque type d'entité ainsi que les référentiels de conformité.

D'une manière générale, les recommandations suivent les objectifs listés dans l'ISO 27001 ou le NIST CSF 2.0, deux référentiels soutenus par l'ENISA. Prochaine date butoir : 2027 et le début de l'application des amendes.

SPAC >ALLIANCE<

SPAC Alliance contribue à de nombreuses commissions de mise en place règlementaire, de définition de standards ou de conception de normes en y apportant toute l'expertise et la connaissance de ses membres. La mise en commun de solutions et le partage du savoir sont et resteront le cœur de SPAC Alliance.

EN BREF : **La mise en place d'une stratégie cyber est un processus à initier le plus tôt possible. Attendre est toujours la pire des options.**

7 CONCLUSION : INVESTIR POUR PRÉPARER NOTRE FUTUR

« ENCORE DES CONTRAINTES ? »

Oui, NIS 2 et REC sont deux nouvelles règlementations majeures. Comme toujours, elles s'accompagnent de contraintes qui doivent être appliquées dans des délais assez courts.

Il faut cependant voir le bon côté des choses.
Citoyens, salariés, collectivités locales et entreprises : beaucoup mesuraient mal la menace cyber ou surestimaient leurs défenses. Avec ces textes, nous disposons maintenant d'une vision objective des dangers et pouvons déployer les outils et pratiques nécessaires pour les écarter.

Certes, une telle mise à niveau aura un coût. Mais, loin de n'être qu'une dépense, c'est aussi et surtout un investissement rentable et mesuré permettant d'envisager notre développement avec sérénité.

Cette étape majeure dans le grand **plan d'action européen relatif à la décennie numérique 2030 (Digital Decade Policy Program 2030)** pose les premières pierres d'une souveraineté numérique européenne durable.

En outre, elle prépare le terrain pour d'autres sujets structurants en matière de sécurité et d'évolution des usages : identité numérique (eIDAS V2), intelligence artificielle (AI Act), blockchain européenne (EBSI), CyberResilience Act.

Mais rassurez-vous ! Nous vous apporterons en temps voulu toutes les clés pour appréhender ces notions et identifier les opportunités qui les accompagnent.

ABONNEZ-VOUS **DEVENEZ MEMBRE** **ADHÉREZ AU CLUB**

8

ANNEXES

A. NIS 2 : SECTEURS ET SOUS-SECTEURS CONCERNÉS

Les acteurs déjà concernés par la NIS le seront aussi par la NIS 2.
Le périmètre est cependant plus large et l'on distinguera désormais deux secteurs :

LES SECTEURS ET SOUS-SECTEURS HAUTEMENT CRITIQUES

- Energie
  - Electricité
  - Réseau de chaleur et de froid
  - Pétrole
  - Gaz
  - Hydrogène
- Transport
  - Transports aériens
  - Transports ferroviaires
  - Transports par eau
  - Transports routiers
- Secteur bancaire
- Infrastructures de marchés financiers
- Santé
- Eau potable
- Eaux usées
- Infrastructures numériques
- Gestion des services TIC : datacenters, services de cloud ou encore CDN
- Administration publique
- Espace



LES AUTRES SECTEURS ET SOUS-SECTEURS CRITIQUES

- Services postaux et d'expédition
- Gestion de déchets
- Fabrication/production/distribution de produits chimiques
- Production/transformation/distribution de denrées alimentaires
- Fabrication
  - Dispositifs médicaux / dispositifs médicaux de diagnostic in vitro
  - Produits informatiques, électroniques et optiques
  - Equipements électriques
  - Machines et équipements
  - Construction de véhicules automobiles, re morques et semi-remorques
  - Autres matériels de transport
- Fournisseurs de services numériques (FSN) : places de marché en ligne, moteurs de recherche, réseaux sociaux
- Recherche

B. REC : QUELLES SONT LES ENTITÉS ET SECTEURS CONCERNÉES

Les acteurs désignés par chaque pays comme des entités critiques ou des entités critiques d'importance européenne tombent dans le scope du **REC (Critical Entities Resilience Directive)** quelle que soit leur taille (nombre d'employés ou chiffre d'affaires).

LES SECTEURS CONCERNÉS PAR LE REC :

- Energie (Electricité, réseaux de chaleur et de froid, Pétrole, Gaz, Hydrogène)
  - Electricité
  - Réseau de chaleur et de froid
  - Pétrole
  - Gaz
  - Hydrogène
- Transport
  - Transports aériens
  - Transports ferroviaires
  - Transports par eau
  - Transports routiers
  - Transports publics
- Secteur bancaire
- Infrastructure des marchés financiers
- Santé
- Eau potable
- Eaux résiduaires
- Infrastructures numériques
- Administration publique
- Espace
- Production, transformation et distribution de denrées alimentaires



C. AGENDA NIS 2 / CER

Les agendas de la NIS 2 et du CER sont identiques concernant leur date limite de transposition, et donc d'application, au sein de l'Union Européenne.

01/2023	17/10/2024	17/10/2024	17/01/2025	17/04/2025	17/07/2027	17/10/2027
Entrée en vigueur de la NIS 2 et de la REC.	Transposition des textes.	Application des textes dans chaque état.	Au plus tard puis tous les deux ans : le réseau des CSIRT adopte un rapport formulant progrès et recommandations. Un travail équivalent est rendu par l'ENISA.	Au plus tard puis au moins tous les deux ans : les Etats fournissent une liste des EE et EI qui vient renseigner une base européenne.	Premier rapport d'évaluation de la REC.	Au plus tard puis tous les trois ans : réexamen de la NIS 2 par la Commission Européenne et proposition législative le cas échéant.

D. FICHE PRATIQUE : QUE FAIRE SI JE SUIS CYBER-ATTAQUÉ ?

En cas de cyberattaque, il est essentiel de prendre des mesures immédiates pour minimiser les dommages et protéger vos données. Voici quelques bonnes pratiques à suivre :

1/Isoler et déconnecter :

Identifiez rapidement la source de l'attaque et isolez les systèmes ou les appareils infectés en les déconnectant du réseau. Cela peut aider à contenir la propagation de l'attaque.

2/Notifier les parties concernées :

Informez les personnes concernées au sein de votre organisation, y compris les équipes informatiques, la direction et les éventuels responsables de la sécurité, afin qu'ils puissent prendre les mesures appropriées.

3/Collecte de preuves :

Documentez toutes les informations pertinentes concernant l'attaque, telles que les journaux système, les captures d'écran ou les fichiers malveillants. Ces preuves peuvent être utiles pour les enquêtes ultérieures et les mesures de rétablissement.

4/Contacter les autorités compétentes :

Signalez l'incident aux organismes de lutte contre la cybercriminalité ou aux forces de l'ordre compétentes dans votre région. Ils peuvent fournir des conseils et une assistance dans la gestion de l'attaque. Comme nous l'avons vu, les règlementations définissent différents process en fonction de votre criticité. Il est important de déposer plainte.

5/Rétablissement à partir de sauvegardes :

Si vous disposez de sauvegardes régulières de vos données, utilisez-les pour restaurer les systèmes et les fichiers touchés. Veillez à ce que les sauvegardes soient sécurisées et ne soient pas compromises par l'attaque.

6/Analyse de l'incident :

Menez une enquête approfondie pour comprendre la nature de l'attaque, les points faibles exploités et les mesures correctives à prendre. Cette analyse vous aidera à renforcer la sécurité de votre infrastructure informatique pour éviter de futures attaques.

7/Renforcement de la sécurité :

Identifiez les lacunes de sécurité qui ont permis l'attaque et prenez des mesures pour les corriger. Cela peut impliquer la mise à jour des logiciels, l'amélioration des pratiques d'authentification, la sensibilisation des employés à la sécurité informatique, etc.

8/Sensibilisation des employés :

Éduquez et informez régulièrement votre personnel sur les menaces de cybersécurité, les techniques d'ingénierie sociale et les bonnes pratiques en matière de sécurité. Les employés bien informés peuvent être une première ligne de défense efficace contre les attaques.

9/Réévaluation de la politique de sécurité :

Passez en revue votre politique de sécurité informatique et mettez-la à jour si nécessaire. Assurez-vous qu'elle couvre tous les aspects pertinents de la cybersécurité et qu'elle est conforme aux meilleures pratiques de l'industrie.

10/Surveillance continue :

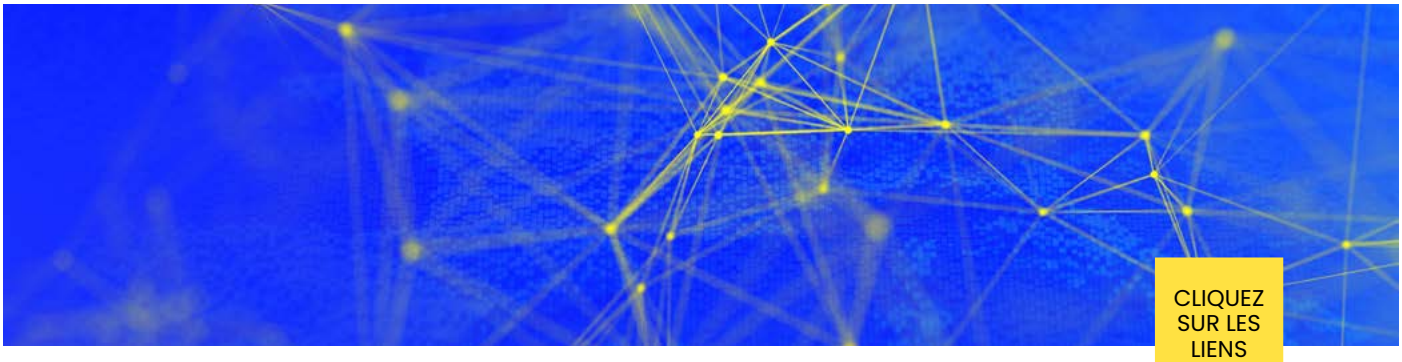
Mettez en place des mécanismes de surveillance continue pour détecter rapidement les activités suspectes ou les tentatives d'intrusion. Cela peut inclure l'utilisation de logiciels de détection des intrusions, de pare-feu avancé et de systèmes de prévention des intrusions.

Il est également recommandé de consulter des professionnels de la cybersécurité et de collaborer avec des experts pour gérer efficacement les conséquences d'une cyberattaque et renforcer la résilience.

E. LIENS UTILES

Textes de référence :
- NIS 2
- Critical Entities Resilience Directive

F. LISTING DES AGENCES NATIONALES DE SÉCURITÉ



COUNTRY	NATIONAL COORDINATION CENTRE
Austria	Federal Chancellery of Austria in cooperation with the Austrian Research Promotion Agency
Belgium	Centre for Cybersecurity Belgium (CCB)
Bulgaria	Ministry of Electronic Governance
Cyprus	Digital Security Authority (DSA)
Czech Republic	National Cyber and Information Security Agency
Germany	National Coordination Centre for Cybersecurity - Federal Office for Information Security (BSI)
Denmark	The Danish Business Authority
Estonia	Estonian Information System Authority
Greece	National Cybersecurity Authority of Greece
Ireland	National Cyber Security Centre of Ireland
Spain	National Cybersecurity Institute (INCIBE)
Finland	NCSC-FI
France	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
Italy	Agenzia per la Cybersicurezza Nazionale (ACN)
Lithuania	National Coordination Centre, Ministry of National Defence
Luxembourg	National Cybersecurity Competence Center Luxembourg
Latvia	Ministry of Defence
Malta	Malta Information Technology Agency
Netherlands	The Netherlands Enterprise Agency (RVO)
Poland	National Cybersecurity Coordination Centre Unit in the Chancellery of the Prime Minister
Portugal	Portuguese National Coordination Centre
Romania	Centrul Național de Coordonare
Sweden	Swedish Civil Contingencies AgencyEN
Slovenia	Office of the Government of the Republic of Slovenia for Information Security
Slovakia	Cyber Security Competence and Certification Centre (KCCKB)

ORGANISMES DE COORDINATION EUROPÉENNE ET DÉCLARATION D'INCIDENT

- CSIRT Network
- CERT ET CERT EU
- ENISA et Liste de officiers de liaison de l'ENISA
- Europol

DÉCOUVREZ TOUS NOS MEMBRES

SPAC ALLIANCE MEMBERS

REJOIGNEZ LE CLUB SPAC ALLIANCE

SPAC ALLIANCE CLUB

DECOUVREZ NOS SERVICES NIS 2 / REC

