Centrum für Europäische Politik
FREIBURG | BERLIN

Adhoc du cep

No 9 | 2021 14 septembre 2022

Directive NIS 2 : nouvelles dispositions de l'UE en matière de cyber-sécurité

Les cyber-risques et cyber-attaques menacent de plus en plus la sécurité européenne

Philipp Eckhardt


© shutterstock

L'avancée de la numérisation et les menaces géopolitiques croissantes augmentent considérablement le risque d'accidents et de cyber-attaques. La cyber-sécurité est devenue l'un des principaux piliers de la sécurité souveraine. Le 13 mai 2022, le Parlement européen et le Conseil se sont mis d'accord sur de nouvelles règles de cyber-sécurité. À l'avenir, quelque 160 000 entreprises et autorités publiques seront soumises à des règles européennes uniformes en matière de gestion des cyber-risques et de notification des incidents et des menaces de cyber-sécurité. Cet Adhoc du cep détaille les nouvelles obligations des entreprises et des services publics en la matière et évalue les nouvelles règles.

- Le champ d'application plus clair de la directive NIS 2 apporte une plus grande sécurité juridique et prévient les distorsions de concurrence. On peut toutefois se demander si, dans la pratique, les autorités de contrôle ne sont pas dépassées par la surveillance d'environ 160 000 établissements. Une plus grande priorisation aurait donc été indiquée.
- Le fait que les risques dans les chaînes d'approvisionnement souvent transfrontalières doivent être davantage pris en compte est juste et améliore le niveau de cyber-sécurité dans l'UE. Toutefois, la responsabilité ne devrait pas reposer uniquement sur les épaules des établissements. La cyber-sécurité est d'une part un bien public et d'autre part un intérêt souverain.
- Les obligations de notification sont appropriées, car les organisations touchées par des cybers incidents sont souvent peu incitées à le faire volontairement, notamment en raison de l'atteinte à la réputation qui accompagne de telles notifications. Les notifications ont souvent une valeur externe élevée, car elles aident les autres à identifier et à combler les failles de sécurité.
- Le renforcement de la gestion des risques des entreprises et des institutions des secteurs privé et public ainsi que le renforcement des obligations de déclaration ne peuvent être qu'un élément de la réglementation nécessaire. Il est donc juste que la Commission veuille ajouter un élément central supplémentaire à la cyber-résilience de l'économie européenne en réseau avec le « Cyber Resilience Act » à venir.

Table des matières

Liste des tableaux

1 Contexte

Selon l'Office fédéral de la police criminelle (BKA), le nombre de délits de cyber-criminalité a augmenté de 12% en 2021 par rapport à l'année précédente et, selon les chiffres de l'association Bitkom, les dommages causés par la cyber-criminalité ont plus que doublé par rapport à 2019 pour atteindre un pic de 223,5 milliards d'euros.[1,2] Et même dans le contexte de l'invasion russe en Ukraine, les craintes d'une augmentation des cyber-attaques, notamment contre les infrastructures critiques telles que les fournisseurs d'énergie, les usines d'eau et les hôpitaux, ne cessent de croître.[3,4]

Au niveau de l'UE, la directive sur la sécurité des réseaux et de l'information [« directive NIS 1 », (UE) 2016/1148] est en vigueur depuis 2016. Elle oblige notamment les États membres à mettre en place des stratégies nationales de cyber-sécurité et établit différents organes afin de renforcer la coopération entre les États membres dans le domaine de la cyber-sécurité. Elle stipule également que les États membres doivent établir des règles contraignantes pour la gestion des risques de cyber-sécurité et des obligations de notification des incidents de cyber-sécurité.

Mi-décembre 2020, la Commission européenne a présenté une proposition de révision de la directive [COM(2020) 823], car elle a constaté certaines lacunes dans le cadre juridique existant. Elle a notamment critiqué le fait que le champ d'application de la directive était « trop limité » et qu'un grand nombre d'entreprises et d'organismes publics n'étaient donc pas soumis à des exigences minimales de cyber-sécurité à l'échelle de l'UE. En outre, le champ d'application « n'est pas suffisamment clair », ce qui laisse une trop grande marge de manœuvre aux États membres pour déterminer qui doit se conformer aux exigences de la directive. La Commission a également critiqué le degré de liberté excessif des États membres dans la mise en œuvre des exigences en matière de gestion des risques de cyber-sécurité, ainsi que le manque de précision des obligations de notification des cyber-incidents. Enfin, la Commission a critiqué l'inefficacité des dispositions de la directive en matière de surveillance et d'application.[5]

Le 13 mai 2022, les négociateurs du Parlement européen (PE) et du Conseil se sont mis d'accord sur une refonte de la directive NIS 1.[6] Le compromis, qui doit encore être formellement confirmé par le PE et le Conseil, a de quoi séduire. A l'avenir, environ 160.000 entreprises et institutions publiques seront concernées par des exigences minimales uniformes de l'UE visant à garantir un niveau élevé de cyber-

1 Office fédéral de la police criminelle (BKA), Cyber-crime, Bundeslagebild 2021.

2 Bitkom Research 2021, L'économie allemande visée par les attaques : plus de 220 milliards d'euros de dommages par an, information de presse, 5 août 2021.

3 Par exemple, le Conseil a récemment souligné que "les actes malveillants dans le cyber-espace [...] par des acteurs étatiques et non étatiques [...] ont augmenté [...] et [...] qu'avec le retour de la politique de puissance, certains pays cherchent de plus en plus à remettre en question l'ordre international fondé sur des règles dans le cyber-espace". Il met en garde contre le fait que "les cyber-attaques à grande échelle, qui menacent le système, [...] se sont multipliées, pourraient saper notre sécurité économique et porter atteinte à nos institutions et processus démocratiques" [Conseil de l'Union européenne, conclusions du Conseil sur le développement de la cyber-défense de l'Union européenne, 23 mai 2022].

4 Dans le cadre des négociations sur la création d'un fonds spécial pour la Bundeswehr, le gouvernement fédéral allemand a également décidé de prendre des mesures pour renforcer la cyber-sécurité, qui seront financées par le budget fédéral. Il entend présenter rapidement une "stratégie de renforcement de la sécurité dans le cyberespace et l'espace d'information".

5 Commission européenne, COM(2020) 823, Proposition de directive relative à des mesures visant à assurer un niveau élevé commun de cyber-sécurité dans l'Union et abrogeant la directive (UE) 2016/1148, p. 5 et 6.

6 Conseil de l'UE, Renforcer la cyber-sécurité et la résilience à l'échelle de l'UE - accord provisoire entre le Conseil et le Parlement européen, communiqué de presse, 13 mai 2022.

sécurité dans l'UE.[7,8] Le présent **Adhoc** du cep montre ce qui attend les entreprises et les administrations publiques concernées et donne une brève évaluation des changements intervenus. Nous nous concentrons sur les adaptations de la directive NIS 2 concernant le champ d'application, la gestion des cyber-risques, les obligations de notification révisées ainsi que les dispositions relatives à la surveillance, à l'application de la loi et aux sanctions.

2 Directive NIS 2 : renforcement de la législation européenne en matière de cyber-sécurité

2.1 Adaptation du champ d'application

Le champ d'application de la directive doit être considérablement élargi selon les idées du PE et du Conseil. En vertu de la directive NIS 2, un grand nombre d'autres entreprises de certains secteurs et, pour la première fois, des organismes du secteur public devront se conformer à des exigences de cyber-sécurité uniformes dans toute l'UE.

2.1.1 Dispositions principales

Comme par le passé, la directive s'applique à un certain nombre d'entités qui sont considérées comme « essentielles »[9] , car elles sont d'une importance critique pour le fonctionnement d'une société. Il s'agit notamment des fournisseurs d'électricité, des entreprises ferroviaires et des banques. Mais à l'avenir, la liste des entités « essentielles » sera considérablement élargie. Ainsi, cette catégorie comprendra également les installations de production, de stockage et de transport d'hydrogène, les fabricants de produits pharmaceutiques, les entreprises de traitement des eaux usées et certains organismes de l'administration publique (voir tableau 1).[10]

Tableau 1: Institutions publiques et privées essentielles

Les établissements marqués en rouge et en gras sont ajoutés par la directive NIS 2.		
Secteur	**Sous-secteur**	**Type d'établissement**
Énergie	Électricité	• Fournisseur d'électricité • Gestionnaire de réseau de distribution • Gestionnaire du réseau de transport • **Producteur d'électricité** • **Opérateurs du marché de l'électricité nominés (NEMO)** • **Acteurs du marché de l'électricité (services d'agrégation, de gestion de la charge ou de stockage d'énergie)** • **Opérateur d'infrastructure de recharge**
	Chauffage et refroidissement urbains	**le chauffage ou le refroidissement urbain pour promouvoir l'utilisation d'énergie produite à partir de sources renouvelables**
	Pétrole	• Opérateurs d'oléoducs • Exploitant d'installations de production, de raffinage et de traitement du pétrole • Exploitants de dépôts et d'oléoducs • **les centrales de stockage de pétrole**

7 Commission de l'industrie, de la recherche et de l'énergie (ITRE), Cyber-sécurité : un accord avec le Conseil pour renforcer la résilience à l'échelle de l'UE, communiqué de presse, 13.05.2022.

8 Directive concernant des mesures relatives à un niveau commun élevé de cyber-sécurité dans l'Union et abrogeant la directive (UE) 2016/1148 (directive NIS 2).

9 Ils étaient jusqu'à présent appelés "opérateurs de services essentiels".

10 Art. 2 en relation avec la directive. Annexe I, Directive NIS 2.

	Gaz naturel	• Société de distribution de gaz naturel • Gestionnaire de réseau de distribution de gaz naturel • Gestionnaire de réseau de transport de gaz naturel • Exploitants d'installations de stockage de gaz naturel • Exploitants d'installations de GNL • Société de gaz naturel • Exploitants d'installations de raffinage et de traitement du gaz naturel
	Hydrogène	**Opérateurs dans le domaine de la production, du stockage et du transport de l'hydrogène**
Trafic	Transport aérien	• Les transporteurs aériens utilisés à des fins commerciales • Organes de gestion de l'aéroport • Aéroports • Opérateurs de systèmes de gestion et de contrôle du trafic routier
	Transport ferroviaire	• Gestionnaire d'infrastructure • Entreprise ferroviaire
	Navigation	• Entreprises de transport de passagers et de fret dans la navigation intérieure, maritime et côtière • Organes de gestion des ports • Opérateur de services de transport maritime
	Circulation routière	• Les autorités routières chargées de la gestion et du contrôle du trafic, à l'exception de celles pour lesquelles il ne s'agit que d'une partie négligeable de leurs activités • Opérateurs de systèmes de transport intelligents
Banque et infrastructures des marchés financiers		• Banques • Opérateurs de salles de marché • Contreparties centrales (CCP)
Santé publique		• Fournisseur de soins de santé • Laboratoires de référence de l'UE sur les menaces sanitaires transfrontalières graves • **Les organismes exerçant des activités de recherche et de développement en matière de médicaments** • **Fabricants de produits pharmaceutiques** • **Les fabricants de dispositifs médicaux considérés comme critiques lors d'une urgence de santé publique**
Eau potable		Les fournisseurs d'eau potable et les entreprises de distribution d'eau potable, à l'exception de celles pour lesquelles il ne s'agit que d'une partie négligeable de leur activité
Eaux usées		**Les entreprises qui collectent, éliminent ou traitent des eaux usées, à l'exception de celles pour lesquelles ces activités ne représentent qu'une partie négligeable de leur activité**
Infrastructure numérique		• Opérateurs de nœuds Internet • Les fournisseurs de services DNS, à l'exception des opérateurs de serveurs de noms racine • Registre des noms de TLD • Fournisseurs de services de cloud computing[1] • **Fournisseurs de services de centres de données** • **Fournisseurs de réseaux de diffusion de contenu** • **Fournisseurs de services de confiance[2]** • **Fournisseurs de réseaux et de services publics de communications électroniques[3]** • **Fournisseur de services gérés (MSP) et Fournisseur de services de sécurité gérés (MSSP)**
Administration publique		• **Les organismes de l'administration publique des administrations centrales, à l'exception du pouvoir judiciaire, des parlements et des banques centrales**

		• **Organismes de l'administration publique au niveau régional**[11]
Espace		**Opérateurs d'infrastructures terrestres à l'appui des services spatiaux**

[1] Jusqu'à présent, ils étaient désignés comme "fournisseurs de services numériques" dans la directive NIS 1.
[2] Elles sont jusqu'à présent couvertes par le règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur [(UE) n° 910/2014].
[3] Elles sont jusqu'à présent couvertes par la directive relative au code européen des communications électroniques [(UE) 2018/1972].

2.1.2 Dispositions secondaires

La directive NIS 1 prévoyait une deuxième catégorie d'entreprises, les "fournisseurs de services numériques". Cette catégorie sera supprimée par la directive NIS 2 et remplacée par une catégorie d'"entités importantes". Cette catégorie comprend également les fournisseurs de services numériques, par exemple les fournisseurs de places de marché et de moteurs de recherche en ligne, mais elle englobera à l'avenir, entre autres, les fabricants de dispositifs médicaux, les entreprises de construction mécanique, les fournisseurs de services postaux et de messagerie et les constructeurs automobiles (voir tableau 2).[12]

Tableau 2: Institutions publiques et privées importantes

Les établissements marqués en rouge et en gras sont ajoutés dans la directive NIS 2.		
Secteur	**Sous-secteur**	**Type d'établissement**
Industrie manufacturière / Production de biens	**Dispositifs médicaux et de diagnostic in vitro**	• **Fabricants de dispositifs médicaux** • **Fabricants de dispositifs médicaux de diagnostic in vitro**
	Équipements informatiques, électroniques et optiques	**Fabricants de produits informatiques, électroniques et optiques**
	Équipements électriques	**Fabricants d'équipements électriques**
	Génie mécanique	**Entreprise de construction mécanique**
	Véhicules automobiles et pièces de véhicules automobiles	**Fabricants de voitures et d'équipements automobiles**
	Autre construction de véhicules	**Construction navale, fabrication de bateaux, de véhicules ferroviaires, d'aéronefs et d'engins spatiaux**
Gestion des déchets		**Entreprise de gestion des déchets (en tant qu'activité principale)**
Services postaux et de courrier		**Fournisseurs de services postaux et de courrier**
Alimentation		**Production, transformation et distribution de denrées alimentaires dans le commerce de gros ou dans la production et la transformation industrielles**
Substances chimiques		**Production, fabrication de substances et de mélanges et fabricants de produits à partir de ces substances et mélanges**
Recherche		**les organismes de recherche dont les travaux de recherche ont une finalité commerciale, à l'exception des établissements d'enseignement**[13]
Fournisseurs de services numériques		• Fournisseurs de places de marché en ligne • Fournisseurs de moteurs de recherche en ligne • **Fournisseurs de plateformes de services de réseaux sociaux**

[11] Sont également exclues les institutions de l'administration publique dans les domaines de la défense, de la sécurité nationale, de la sécurité publique ou de l'application de la loi.
[12] Art. 2 en relation avec la directive. Annexe I, directive NIS 2.
[13] Les États membres peuvent toutefois décider d'appliquer la directive aux établissements d'enseignement, notamment lorsque ceux-ci mènent des activités de recherche critiques (article 2, paragraphe 2b).

2.1.3 Exceptions pour les petits établissements

La directive NIS 2 ne doit en principe s'appliquer qu'aux entités essentielles et importantes qui dépassent les seuils fixés en tant qu'entités de taille moyenne. Il est ainsi prévu que les entités doivent avoir au moins 50 employés, un chiffre d'affaires annuel d'au moins 10 millions d'euros ou un bilan annuel d'au moins 10 millions d'euros.[14]

2.1.4 Organismes toujours couverts, quelle que soit leur taille

Certaines entités publiques et privées essentielles ou importantes sont également couvertes par la directive, quelle que soit leur taille (pas de seuils). C'est le cas, entre autres, de[15]

- Opérateurs de réseaux et de services publics de communications électroniques,
- Les organismes qui, dans un État membre, sont les seuls prestataires d'un service essentiel au maintien d'activités sociales ou économiques critiques, et
- Fournisseurs de services dont les perturbations risquent de compromettre gravement la sécurité, l'ordre ou la santé publics, ou la stabilité transfrontalière du système.

En principe, les institutions des administrations publiques des gouvernements centraux sont également couvertes, quelle que soit leur taille. Il en va de même pour les organismes des administrations publiques au niveau régional, dans la mesure où l'interruption des services qu'ils fournissent aurait un impact grave sur les activités sociales ou économiques. Les États membres peuvent également décider d'inclure les administrations publiques locales dans le champ d'application de la directive NIS 2 (droit d'option des États membres).[16]

2.1.5 Institutions exclues

La directive ne couvre pas les "administrations publiques" dans les domaines de la défense, de la sécurité nationale, de la sécurité publique ou de l'application de la loi, ni les parlements et les banques centrales.[17] Sont également exclues un grand nombre de banques, en particulier les banques de développement - par exemple la *Kreditanstalt für Wiederaufbau* - si un État membre a choisi de les exempter également des exigences sectorielles de cyber-sécurité de la loi sur la stabilité opérationnelle des entreprises financières [Digital Operational Resilience Act (DORA), cf. **Analyse** du cep][18] .[19]

2.1.6 Réglementations sectorielles

Lorsqu'il existe une législation européenne sectorielle en matière de cyber-sécurité pour les entités relevant du champ d'application de la directive NIS 2 - comme le règlement sur la stabilité opérationnelle des entreprises financières - ces entités ne sont pas tenues de se conformer aux exigences de la directive NIS 2 en matière de gestion des cyber-risques (voir section 2.2) et de notification des cyber-

[14] Art. 2, directive NIS 2.
[15] Art. 2, directive NIS 2.
[16] Ibid.
[17] Ibid.
[18] Le règlement DORA a été négocié parallèlement à la directive NIS 2 et complète la directive par des règles sectorielles visant à renforcer la cyber-sécurité des entreprises financières. Un résultat en trilogue sur cet acte juridique a été obtenu le 11 mai. Plus de détails ici.
[19] Article 2, paragraphe 3d, de la directive NIS 2.

incidents et des cyber-menaces (voir section 2.3), à condition que la législation sectorielle soit au moins équivalente aux exigences de la directive NIS 2 à cet égard.[20]

2.2 Gestion des cyber-risques

Comme la directive NIS 1, la directive NIS 2 impose aux entités essentielles et importantes couvertes de prendre des mesures pour gérer de manière adéquate les risques de cyber-sécurité. La directive NIS 2 est désormais plus concrète et limite considérablement la marge d'appréciation des États membres.

2.2.1 Mesures de gestion des cyber-risques :

Les entités couvertes par la directive doivent prendre des "mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées" afin de maîtriser les risques pour la sécurité des systèmes de réseau et d'information (SRI) qu'elles utilisent pour leurs activités ou pour la fourniture de leurs services. En outre, les mesures prises doivent limiter ou prévenir les conséquences des cyber-incidents sur les destinataires de leurs services et sur d'autres services.[21] Les mesures visant à protéger, outre la sécurité des SRI, leur environnement physique doivent notamment comprendre[22]

- L'analyse des risques,
- L'élaboration de concepts de sécurité pour les systèmes d'information,
- Les mesures prises pour faire face aux cyber-incidents, c'est-à-dire leur prévention, leur détection, leur analyse, leur atténuation, ainsi que les étapes de la réponse à l'incident et de la récupération après un incident,
- Les mesures de maintien de l'activité (par exemple, la gestion des sauvegardes et la reprise après sinistre) et de gestion des crises,
- Démarches visant à garantir la sécurité des chaînes d'approvisionnement,
- Les pratiques de base en matière de cyber-hygiène et la formation à la cyber-sécurité,
- L'utilisation de solutions d'authentification à facteurs multiples ou de solutions d'authentification continue ; et
- Stratégies et procédures pour l'utilisation de la cryptographie et, le cas échéant, des techniques de cryptage.

La proportionnalité des mesures doit être évaluée en fonction du degré d'exposition au risque de l'établissement, de sa taille, de la probabilité de survenue de cyber-incidents et de leur gravité. L'impact social et économique doit également être pris en compte.[23]

La Commission peut définir des spécifications techniques, méthodologiques et, le cas échéant, sectorielles pour les mesures de gestion des risques au moyen d'actes d'exécution.[24]

[20] Art. 2b, directive NIS 2.
[21] Article 18, paragraphe 1, de la directive NIS 2.
[22] Article 18, paragraphe 2, de la directive NIS 2.
[23] Article 18, paragraphe 1, de la directive NIS 2.
[24] Article 18, paragraphe 5, de la directive NIS 2.

2.2.2 Focus sur la chaîne d'approvisionnement

La directive NIS 2 met l'accent sur les cyber-menaces au sein de la chaîne d'approvisionnement. Ainsi, les établissements essentiels et importants sont tenus de prendre des mesures pour renforcer la sécurité de leur chaîne d'approvisionnement. L'accent doit être mis sur les relations entre les institutions et leurs fournisseurs et prestataires de services "directs" (par exemple, les fournisseurs de services en cloud). Ainsi, les institutions doivent se pencher sur les vulnérabilités et les pratiques de cyber-sécurité spécifiques de chaque fournisseur ou prestataire de services "direct" et, en particulier, examiner de près la qualité des produits livrés. En outre, dans le cadre de leur gestion des risques, les institutions doivent examiner en particulier les produits et services TIC de leurs fournisseurs et prestataires de services que la Commission européenne, en collaboration avec un groupe de coopération[25] et l'ENISA[26] , a identifiés comme étant particulièrement critiques.[27]

2.2.3 Certification en matière de cyber-sécurité

Si la Commission estime que le niveau de cyber-sécurité est insuffisant, elle pourra, par voie d'actes délégués, exiger de certaines catégories d'entités essentielles ou importantes qu'elles n'utilisent que des produits ou services TIC certifiés ou nécessitant une certification dans le cadre de systèmes européens de cyber-sécurité. Les États membres peuvent également obliger certaines entités essentielles et importantes à n'utiliser que certains produits ou services TIC qu'elles développent elles-mêmes ou qu'elles achètent à des tiers et qui sont certifiés dans le cadre de systèmes européens de certification de la cyber-sécurité. Cela permettrait également aux institutions de démontrer leur conformité aux mesures de gestion des cyber-risques.[28]

2.2.4 Responsabilité des organes directeurs

Dans le cadre de la directive NIS 2, la responsabilité des organes de direction des établissements essentiels et importants en matière de gestion des cyber-risques doit également être considérablement accrue. Il leur incombera explicitement d'approuver les mesures de gestion des risques et de contrôler leur mise en œuvre. Les organes de direction peuvent être tenus pour responsables en cas de non-respect des exigences de la directive. Ils seront également tenus de participer régulièrement à des formations sur les risques de cyber-sécurité et leur impact sur l'établissement, et ils devront permettre à tous leurs employés de participer également à des formations similaires.[29]

2.3 Signalement des cyber-incidents et des cyber-menaces

Tout comme la directive NIS 1, la directive NIS 2 révisée oblige les entités couvertes à notifier les incidents de cyber-sécurité. Alors que les dispositions de la directive NIS 1 étaient assez vagues et laissaient une grande marge d'interprétation, la directive NIS 2 prévoit désormais des règles plus claires sur ce qui doit être notifié, quand, à qui et comment les incidents doivent être notifiés.

---

[25] Le groupe de coopération est un organe composé de représentants des États membres, de la Commission et de l'ENISA. Il soutient l'échange d'informations entre les États membres concernant l'application de la directive.

[26] L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) est une agence de cyber-sécurité de l'UE établie dès 2004.

[27] Art. 18, al. 2 et 3, art. 19, directive NIS 2.

[28] Art. 21, directive NIS 2.

[29] Art. 17, directive NIS 2.

2.3.1 Quels sont les cyber-incidents et les cyber-menaces qui doivent être signalés ?

Les institutions essentielles et importantes doivent déclarer tous les cyber-incidents "significatifs". Les cyber-incidents sont considérés comme "significatifs" s'ils [30]

- Entraînent ou risquent d'entraîner des perturbations importantes du fonctionnement du service de l'établissement,
- Entraînent des pertes financières considérables pour l'établissement,
- Entraînent ou sont susceptibles d'entraîner des pertes matérielles ou immatérielles importantes pour d'autres personnes physiques ou morales.

Les institutions doivent également, le cas échéant, informer les utilisateurs de leurs services potentiellement affectés par une "cyber-menace importante"[31] des mesures (correctives) qu'ils peuvent prendre pour faire face à la menace. Le cas échéant, ils doivent également informer les utilisateurs de la menace elle-même.[32]

2.3.2 Quand les cyber-incidents doivent-ils être signalés ?

Déclaration de 24 heures : La notification doit en principe être effectuée "immédiatement". Dans tous les cas, une notification au sens d'une "alerte précoce" doit cependant être effectuée au moins dans les 24 heures suivant la connaissance d'un tel incident. Cette notification initiale doit indiquer si l'incident est présumé avoir été causé par un acte illégal ou malveillant et dans quelle mesure il a des conséquences transfrontalières.[33]

Déclaration 74h : Une deuxième notification doit être envoyée dans les 72 heures suivant la découverte du cyber-incident. Celle-ci doit actualiser la première déclaration et contenir une première analyse de l'incident, notamment en ce qui concerne sa gravité et son impact et, si possible, les indicateurs de risque.[34]

Rapport intermédiaire : un autre rapport doit être établi à la demande du CSIRT ou de l'autorité compétente. Elle prend la forme d'un rapport intermédiaire et doit contenir des mises à jour d'état.[35]

Rapport final : un rapport final décrivant la gravité et l'impact de l'incident, la nature de la menace, la cause et les mesures correctives prises doit également être fourni dans un délai d'un mois à compter de la notification de l'échéance 74h.[36]

Rapport d'avancement : si un cyber-incident n'est toujours pas résolu dans un délai d'un mois, un rapport d'avancement doit être présenté à la place du rapport final. Le rapport final doit alors être présenté au plus tard un mois après la résolution de l'incident.[37]

---

30 Art. 20, al. 1 et 3, directive NIS 2.
31 Une "cyber-menace significative" est une cyber-menace dont on peut supposer qu'elle a le potentiel de porter gravement atteinte au SRI d'une entité ou de ses utilisateurs en causant des pertes matérielles ou immatérielles importantes [art. 4, al. 1, ch. 7a].
32 Article 20, paragraphe 2, de la directive NIS 2.
33 Art. 20, al. 1 et 4, directive NIS 2.
34 Article 20, paragraphe 4, de la directive NIS 2.
35 Ibid.
36 Ibid.
37 Ibid.

2.3.3 À qui les cyber-incidents doivent-ils être signalés ?

Les cyber-incidents doivent être signalés en premier lieu aux équipes nationales de réaction aux incidents de sécurité informatique (CSIRT) ou, le cas échéant, aux autorités nationales compétentes. Si la notification est adressée à une autorité compétente, celle-ci doit la transmettre au CSIRT. Le cas échéant, les institutions doivent également informer leurs utilisateurs de services.[38] Il est précisé que la notification d'un tel cyber-incident ne doit pas entraîner un accroissement de la responsabilité de l'entité qui l'a signalé.[39]

2.3.4 Réaction des autorités de surveillance

Le CSIRT ou l'autorité compétente doit fournir un premier retour d'information sans délai et, si possible, dans les 24 heures et, à la demande de l'entreprise, fournir une assistance pour la mise en œuvre de mesures correctives. Le CSIRT ou l'autorité compétente peut informer le public de l'incident ou demander à l'entité concernée de le faire, à condition que la sensibilisation du public puisse prévenir l'incident, contribuer à sa résolution ou servir l'intérêt public.[40]

2.4 Surveillance, application et sanctions

La directive NIS 2 prévoit que les entités essentielles et importantes soient soumises à une surveillance. Les autorités de surveillance nationales doivent veiller à ce que les entités respectent les exigences en matière de gestion des risques et de notification des cyber-incidents. D'une manière générale, les autorités nationales doivent disposer d'un minimum de pouvoirs de surveillance, y compris pour les inspections sur place ou les audits de sécurité réguliers et ciblés des entités réglementées, y compris les inspections ad hoc en cas de cyber-incidents graves.[41]

La surveillance des entités importantes doit être moins stricte que celle des entités essentielles. Alors que pour ces dernières, il n'est prévu qu'une surveillance ex post, qui ne sera activée que sur la base d'indications et d'informations relatives à des violations potentielles de la directive, une surveillance complète - c'est-à-dire ex ante et ex post - doit intervenir pour les entités essentielles.[42]

Les autorités nationales de surveillance doivent en outre disposer d'un certain nombre de pouvoirs d'exécution. Par exemple, elles pourront adresser des avertissements aux entités essentielles et importantes si elles ne se conforment pas aux exigences de la directive. Elles doivent également pouvoir donner des instructions contraignantes, par exemple sur les mesures à prendre pour prévenir ou atténuer les cyber-incidents, y compris des délais pour leur mise en œuvre.[43]

Si les entreprises ne se conforment pas aux mesures d'exécution, les autorités peuvent imposer des sanctions. Des sanctions peuvent être infligées aux entités et aux personnes responsables de la gestion.[44]

---

38 Art. 20, paragraphe 1, de la directive NIS 2.
39 Art. 20, paragraphe 1, de la directive NIS 2.
40 Art. 20, paragraphe 7, de la directive NIS 2.
41 Art. 29, paragraphes 1 et 2, et art. 30, paragraphes 1 et 2, directive NIS 2.
42 Considérant 70, art. 29 et art. 30, directive NIS 2.
43 Art. 29, par. 4 et art. 30, par. 4, directive NIS 2.
44 Art. 29 al. 5 et 6, art. 30 al. 5 et 6, directive NIS 2.

2.5 Mise en œuvre de la directive NIS 2

Maintenant que le Conseil et le PE sont parvenus à un accord en trilogue, les deux organes législatifs doivent encore approuver formellement le compromis trouvé. Cela devrait se faire au début de l'automne. Après l'entrée en vigueur de la directive, les États membres disposeront de 21 mois pour intégrer les dispositions législatives et administratives nécessaires dans leur droit national.[45] La directive ne devrait donc pas être appliquée avant 2025 au plus tôt.

[45] Art. 38, directive NIS 2.

3 Évaluation

Dans le contexte de l'augmentation des menaces et des incidents cybernétiques, le Parlement Européen et le Conseil ont décidé d'utiliser la directive NIS 2 pour obliger un grand nombre d'entreprises et d'institutions du secteur public à prendre des mesures de gestion des risques de cyber-sécurité et à signaler les cyber-incidents significatifs aux autorités de contrôle. Mais ces exigences réglementaires sont-elles vraiment nécessaires pour renforcer la cyber-résilience européenne ? En principe, on pourrait argumenter que les entreprises devraient déjà avoir un intérêt propre à protéger suffisamment leurs systèmes de réseau et d'information (NIS) contre les cyber-incidents et les menaces. En effet, si elles ne le font pas, cela peut entraîner des pertes de chiffre d'affaires et des dommages de réputation considérables en cas d'attaque. Les entreprises devraient donc être prêtes à investir dans la stabilité de leurs systèmes. Mais c'est souvent une erreur. En effet, les incitations économiques à investir dans la cyber-sécurité sont régulièrement insuffisantes. Tout d'abord, les entreprises victimes d'un cyber-incident n'ont souvent pas à supporter l'intégralité des coûts liés au manque de sécurité de leur réseau et de leurs systèmes d'information. Au lieu de cela, elles peuvent régulièrement répercuter une partie de ces coûts sur des tiers, comme leurs clients. Deuxièmement, les efforts d'une entreprise pour renforcer sa cyber-résilience augmentent souvent la résilience d'autres entreprises. Cependant, les entreprises intègrent rarement ces externalités positives dans leurs calculs de décision. Des normes uniformes pour la gestion des cyber-risques sont donc appropriées, notamment en raison de la nature de la cyber-sécurité en tant que bien public et de l'intérêt souverain fondamental pour des économies stables et résilientes. Cela est d'autant plus vrai qu'une entreprise est importante pour les services de base ou pour le fonctionnement d'une société, car sa dégradation ou sa défaillance est liée à des coûts particulièrement élevés pour la société. La gradation envisagée dans la profondeur de la réglementation entre les entreprises essentielles et les entreprises importantes est donc appropriée, indépendamment des multiples interdépendances et dépendances critiques qui existent également entre les entreprises essentielles et les entreprises importantes.

Le champ d'application de la directive NIS 2 fait toutefois l'objet de critiques. Certes, la révision de la directive NIS 1 clarifie le champ d'application, créant ainsi une plus grande sécurité juridique quant à savoir qui est concerné par les dispositions de la directive NIS 2. Cela limite également les possibilités d'arbitrage réglementaire et prévient les distorsions de concurrence. Toutefois, le champ d'application de la directive est désormais trop large : En effet, de nombreuses entreprises qui n'offrent pas de produits ou de services pouvant être considérés comme absolument essentiels à l'approvisionnement et au fonctionnement d'une société sont également concernées. Il s'agit par exemple des entreprises de l'industrie manufacturière, comme les entreprises de construction mécanique. En outre, on peut se demander si, dans la pratique, les autorités de contrôle ne sont pas débordées par la surveillance d'environ 160 000 entreprises et organismes publics et si, par conséquent, une plus grande priorisation n'aurait pas été indiquée. En outre, la taille d'une entité n'est pas un critère approprié en soi pour l'inclure dans le champ d'application, car elle n'indique pas nécessairement à elle seule un risque plus élevé en matière de cyber-sécurité. D'autres critères auraient également dû être pris en compte, comme le nombre de clients d'une entreprise.

Le fait que les entités essentielles et importantes doivent désormais tenir compte des risques de la chaîne d'approvisionnement dans le cadre de leur gestion des risques, dans une plus large mesure qu'en vertu de la directive NIS 1, peut améliorer le niveau de cyber-sécurité dans l'UE. Toutefois, la

responsabilité de garantir la cyber-sécurité ne devrait pas reposer uniquement sur les épaules des entités essentielles et importantes à la fin de la chaîne de valeur. En effet, un contrôle intensif de chaque fournisseur de la chaîne d'approvisionnement prendrait non seulement beaucoup de temps, mais entraînerait également des coûts énormes. Il est donc approprié de se concentrer sur les fournisseurs directs. Il est aussi essentiel que les fournisseurs de produits et de services TIC soient également soumis à des exigences directes, c'est-à-dire qu'ils soient également tenus responsables. Il faut donc saluer le fait que la Commission prévoit de prendre des mesures législatives à cet effet, probablement le 13 septembre 2022, avec le "Cyber Resilience Act", et de créer des exigences de cyber-sécurité pour les produits numériques.

L'obligation de notifier les cyber-incidents graves aux autorités de contrôle est appropriée. En effet, les entités concernées par ces incidents sont souvent peu incitées à le faire volontairement en raison des coûts élevés de notification et des dommages potentiels pour leur réputation. Cependant, les notifications ont souvent une valeur externe élevée, car elles aident les autres à identifier et à combler les failles de sécurité. La fixation de délais et de procédures clairs pour la notification des cyber-incidents est également positive. D'une part, elles améliorent la clarté juridique et, d'autre part, elles réduisent la charge administrative pour les entités soumises à l'obligation de notification, étant donné qu'elles peuvent désormais soumettre leur notification à un organisme central. Il est impératif de signaler rapidement les cyber-incidents afin de pouvoir endiguer rapidement les dommages. Le délai de 24 heures est donc certes ambitieux, mais finalement sans alternative. Néanmoins, la valeur de cette première notification ne doit pas être surestimée. En effet, il n'est pas certain que des informations suffisamment pertinentes puissent être transmises dans ce court délai. Cela vaut en particulier pour les petites entreprises qui ne peuvent pas toujours compter sur des ressources internes trop importantes pour analyser les cyber-incidents, d'autant plus que des exigences de notification aussi rapides peuvent également mobiliser des capacités précieuses qui devraient être utilisées pour la gestion des cyber-incidents.

En principe, les mesures plus strictes de gestion des risques et les obligations de notification de la directive NIS 2 ne suffisent évidemment pas à assurer la résilience du paysage européen des entreprises face aux cyber-risques. Elles ne peuvent être qu'un élément constitutif. Elles constituent toutefois une pierre angulaire centrale dans un concert de nombreuses mesures réglementaires, notamment nationales, mais aussi européennes. Outre les étapes présentées dans cet Adhoc du cep, la directive NIS 2 contient par exemple de nombreuses mesures visant à améliorer la coopération entre les États membres ou les autorités compétentes en cas de cyber-incident. En outre, l'Agence de l'Union européenne pour la cyber-sécurité (ENISA) s'est vu confier de nombreuses nouvelles tâches et un cadre réglementaire européen a déjà été créé pour la certification de la cyber-sécurité des technologies de l'information et de la communication [règlement (UE) 2019/881, voir Analyse du cep (sur l'ENISA) et Analyse du cep (sur la certification de la cyber-sécurité)]. Et le "Cyber Resilience Act", annoncé pour cette semaine, devrait également contribuer de manière significative au renforcement de la sécurité des économies européennes interconnectées.

Centrum für Europäische Politik
FREIBURG | BERLIN

Auteur :

Philipp Eckhardt, chargé de recherche au département Marchés financiers et Technologies de l'information

eckhardt@cep.eu

Traduction :

Mathilde Baudouin,
cepfrance@cep.eu

Centre de politique européenne FREIBURG | BERLIN
Kaiser-Joseph-Straße 266 | D-79098 Fribourg
Schiffbauerdamm 40 Salle 4315 | D-10117 Berlin
Tél. + 49 761 38693-0

Le **Centrum für Europäische Politik** FREIBURG | BERLIN, le **Centre de Politique Européenne** PARIS, et le **Centro Politiche Europee** ROMA forment le **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA.

Le Centre de Politique Européenne, reconnu d'utilité publique, analyse et évalue la politique de l'Union européenne indépendamment des intérêts particuliers et partisans, dans une orientation fondamentalement favorable à l'intégration et sur la base des principes réglementaires d'un ordre libéral et d'une économie de marché.