UNIVERSITÉ DE NAMUR

Cyber-security law

crids
CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

La Directive NIS et l'obligation de sécurité dans le secteur des télécoms

Franck Dumortier

franck.dumortier@unamur.be

1. Les obligations de sécurité dans la Directive NIS

UNIVERSITÉ DE NAMUR

La Directive NIS

crids
CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

- ✓ La directive NIS a été approuvée le 6 juillet par le Parlement européen.

  ➡ Doit être transposée par les EM au plus tard en mai 2018

- ✓ Cette directive est destinée à assurer un « niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne »

  - En harmonisant les législations internes de chaque État membre.
  - En améliorant la coopération entre les États membres afin de favoriser les échanges d'information sur les risques existants par la mise en place d'un réseau appelé « CSIRT ».

Raisons d'être de la Directive NIS

- ✓ *« Les réseaux et les services et systèmes d'information jouent un rôle crucial dans la société. Leur fiabilité et leur sécurité sont essentielles aux fonctions économiques et sociétales et notamment au fonctionnement du marché intérieur ».* (Considérant 1)

- ✓ *« L'ampleur, la fréquence et l'impact des incidents de sécurité ne cessent de croître et représentent une menace considérable pour le fonctionnement des réseaux et des systèmes d'information. Ces systèmes peuvent également devenir des cibles pour des actions intentionnelles malveillantes qui visent à la détérioration ou à l'interruption de leur fonctionnement. Ces incidents peuvent nuire à l'exercice d'activités économiques, entraîner des pertes financières importantes, entamer la confiance des utilisateurs et porter un grand préjudice à l'économie de l'Union ».* (Considérant 2)

Objectif de la Directive NIS

- ✓ **La Directive NIS** vise à protéger les réseaux et systèmes d'information contre les «« risques » et « incidents » que ceux-ci impliquent **ou non** des traitements de DACP. (Attention, si des DACP sont traitées, le GDPR s'applique de manière cumulative !!!)

  - **«sécurité des réseaux et des systèmes d'information»**: *la capacité des réseaux et des systèmes d'information de résister à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles.*

  - **«risque»**: *toute circonstance ou tout événement raisonnablement identifiable ayant un impact négatif **potentiel** sur la sécurité des réseaux et des systèmes d'information*

  - **«incident»**: *tout événement ayant un impact négatif **réel** sur la sécurité des réseaux et des systèmes d'information.*

A quelles entreprises s'applique la Directive NIS ?

La Directive NIS établit des exigences en matière de sécurité pour les entreprises en tant que:

- ✓ **«opérateur de services essentiels»:** une entité publique ou privée tributaire des réseaux et des systèmes d'information:
  - **Dans les secteurs** de l'énergie (électricité, gaz, pétrole), les transports (aérien, ferroviaire, par voie d'eau, routier), les banques, les infrastructures de marchés financiers, la santé, la fourniture et distribution d'eau potable, les infrastructures numériques. (// relatif avec la loi du 1/07/2011 sur les infrastructures critiques)
  - **Et** dont un incident aurait **un effet disruptif important** sur la fourniture dudit service. Au plus tard le 9 novembre 2018, pour chaque secteur et sous-secteur visé, les États membres identifient les opérateurs de services essentiels ayant un établissement sur leur territoire.

OU

- ✓ **«fournisseur de service numérique»:** une personne morale qui fournit un service numérique de type place de marché en ligne, moteurs de recherche en ligne ou service d'informatique en nuage (MAIS le chapitre V ne s'applique pas aux micro entreprises ni aux petites entreprises au sens de la Recommandation 2003/361/CE.)

Les opérateurs de services essentiels (1)

1. Secteur de l'Énergie

✓ Électricité

- Entreprises d'électricité qui remplit la fonction de «fourniture »
- Gestionnaires de réseau de distribution
- Gestionnaires de réseau de transport

✓ Pétrole

- Exploitants d'oléoducs
- Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole

✓ Gaz

- Entreprises de fourniture
- Gestionnaires de réseau de distribution
- Gestionnaires de réseau de transport
- Gestionnaires d'installation de stockage
- Gestionnaires d'installation de GNL
- Entreprises de gaz naturel
- Exploitants d'installations de raffinage et de traitement de gaz naturel

Les opérateurs de services essentiels (2)

2. Secteur des Transports

✓ Transport aérien

- Transporteurs aériens
- Entités gestionnaires d'aéroports et entités exploitant les installations annexes se trouvant dans les aéroports
- Services du contrôle de la circulation aérienne

✓ Transport ferroviaire

- Gestionnaires de l'infrastructure—
- Entreprises ferroviaires, y compris les exploitants d'installations de services

✓ Transport par voie d'eau

- Sociétés de transport terrestre, maritime et côtier de passagers et de fret
- Entités gestionnaires des ports, ainsi que les entités exploitant des ateliers et des équipements à l'intérieur des ports
- Exploitants de services de trafic maritime

✓ Transport routier

- Autorités routières, chargées du contrôle de gestion du trafic
- Exploitants de systèmes de transport intelligents

Les opérateurs de services essentiels (3)

3. Banques

- Établissements de crédit au sens de l'article 4, point 1), du règlement (UE) nº 575/2013 du Parlement européen et du Conseil

4. Infrastructures de marchés financiers

- Exploitants de plate-forme de négociation au sens de l'article 4, point 24), de la directive 2014/65/UE du Parlement européen et du Conseil (14)

- Contreparties centrales au sens de l'article 2, point 1), du règlement (UE) no 648/2012 du Parlement européen et du Conseil (15)

Les opérateurs de services essentiels (4)

5. Secteur de la santé

- Établissements de soins de santé (y compris les hôpitaux et les cliniques privées)

6. Fourniture et distribution d'eau potable

- Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 2, point 1) a), de la directive 98/83/CE du Conseil (17), à l'exclusion des distributeurs pour lesquels la distribution d'eaux destinées à la consommation humaine ne constitue qu'une partie de leur activité générale de distribution d'autres produits et biens qui ne sont pas considérés comme des services essentiels

Les opérateurs de services essentiels (5)

7. Infrastructures numériques

- ✓ **«point d'échange internet » (IXP):** une structure de réseau qui permet l'interconnexion de plus de deux systèmes autonomes indépendants, essentiellement aux fins de faciliter l'échange de trafic internet; un IXP n'assure l'interconnexion que pour des systèmes autonomes; un IXP n'exige pas que le trafic internet passant entre une paire quelconque de systèmes autonomes participants transite par un système autonome tiers, pas plus qu'il ne modifie ou n'altère par ailleurs un tel trafic.

- ✓ **Fournisseurs de services DNS:** une entité qui fournit des services DNS sur l'internet.

- ✓ **Registres de noms de domaines de haut niveau:** une entité qui administre et gère l'enregistrement de noms de domaine internet dans un domaine de haut niveau donné;

Les opérateurs de services essentiels (6)

- ✓ Attention ! Les 7 types d'opérateurs de services essentiels énumérés sont ceux que la Directive impose à la Belgique d'être identifiés.

MAIS

- ✓ **D'autres secteurs pourraient être rajoutés par la loi de transposition.**

- ✓ **Exemples:**
  - **Secteur public de la sécurité/défense**
  - **Autres secteurs publics**
  - **Secteur pharmaceutique**
  - **Secteur chimique**
  - **Secteur nucléaire**

Les fournisseurs de services numériques (1)

- ✓ Une place de marché en ligne permet aux consommateurs et aux professionnels de conclure des contrats de vente ou de service en ligne avec des professionnels et est la destination finale pour la conclusion desdits contrats.

- ✓ Elle ne concerne pas les services en ligne qui ne servent que d'intermédiaires pour des services fournis par un tiers à travers lequel un contrat peut en définitive être conclu. Elle ne concerne donc pas les services en ligne qui comparent le prix de certains produits ou services de plusieurs professionnels, avant de réorienter l'utilisateur vers le professionnel choisi en vue de l'achat du produit. Parmi les services informatiques fournis par la place de marché en ligne peuvent figurer le traitement de transactions, l'agrégation de données ou le profilage d'utilisateurs. Les magasins d'applications en ligne, qui fonctionnent comme des magasins en ligne permettant la distribution numérique d'applications ou de logiciels émanant de tiers, doivent s'entendre comme étant un type de place de marché en ligne.

Les fournisseurs de services numériques (2)

- ✓ Un moteur de recherche en ligne permet à l'utilisateur d'effectuer des recherches sur, en principe, tous les sites internet sur la base d'une requête lancée sur n'importe quel sujet. Il peut aussi se limiter aux sites internet dans une langue donnée.

- ✓ La définition d'un moteur de recherche en ligne ne s'applique pas aux fonctions de recherche qui se limitent au contenu d'un site internet spécifique, indépendamment de la question de savoir si la fonction de recherche est assurée par un moteur de recherche externe. Elle ne concerne pas non plus les services en ligne qui comparent le prix de certains produits ou services de différents professionnels et qui réorientent ensuite l'utilisateur vers le professionnel choisi en vue de l'achat du produit.

Les fournisseurs de services numériques (3)

- ✓ Les termes «services d'informatique en nuage» couvrent des services qui permettent l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées. Ces ressources informatiques comprennent des ressources telles que les réseaux, serveurs et autres infrastructures, le stockage, les applications et les services.

- ✓ Le terme «modulable» renvoie aux ressources informatiques qui sont attribuées d'une manière souple par le fournisseur de services en nuage, indépendamment de la localisation géographique de ces ressources, pour gérer les fluctuations de la demande. Les termes «ensemble variable» sont utilisés pour décrire les ressources informatiques qui sont mobilisées et libérées en fonction de la demande pour pouvoir augmenter ou réduire rapidement les ressources disponibles en fonction de la charge de travail. Les termes «pouvant être partagées» sont utilisés pour décrire les ressources informatiques qui sont mises à disposition de nombreux utilisateurs qui partagent un accès commun au service, le traitement étant effectué séparément pour chaque utilisateur bien que le service soit fourni à partir du même équipement électronique.

Champ d'application territorial de la future loi de transposition belge ?

- ✓ La loi s'appliquera :

- Aux opérateurs de services essentiels ayant un établissement sur le territoire belge. L'établissement suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable. La forme juridique retenue pour un tel établissement, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard.

- Aux fournisseurs de services numériques qui ont leur principal établissement sur le territoire belge, ce qui correspond en principe à l'endroit où il a son siège social. Lorsqu'un fournisseur de service numérique n'est pas établi dans l'Union et propose des services à l'intérieur de l'Union, il doit désigner un représentant dans un des pays UE où il offre ses services.

Obligation de sécurité dans la Directive NIS (1)

Les opérateurs de services essentiels prennent des mesures techniques et organisationnelles:

- **nécessaires et proportionnées** pour **gérer les risques de sécurité.** Le niveau de sécurité doit être **adapté au risque existant**, compte tenu de **l'état des connaissances.**

- **appropriées** en vue de **prévenir/limiter les incidents de sécurité dans le but d'assurer la continuité de ces services.**

➡ **Pas de référence aux frais.**

Obligation de sécurité dans la Directive NIS (2)

Les fournisseurs de service numérique :

- ✓ **identifient les risques** de sécurité et prennent les mesures techniques et organisationnelles :
  - nécessaires et proportionnées pour les gérer.
  - compte tenu de l'état des connaissances

- ✓ Le niveau de sécurité doit être **adapté au risque existant** en prenant en compte:
  a) la sécurité des systèmes et des installations;
  b) la gestion des incidents;
  c) la gestion de la continuité des activités;
  d) le suivi, l'audit et le contrôle;
  e) le respect des normes internationales.

- ✓ **prennent des mesures pour éviter/limiter l'impact des incidents** de sécurité de manière à garantir la continuité de ces services.

Autorités de contrôle dans la Directive NIS (1)

La Directive NIS prévoit que:

- Chaque État membre désigne une ou plusieurs « autorités nationales compétentes » qui contrôlent l'application de la directive au niveau national.

  ➡ **« Autorités sectorielles »** pour chaque secteur couvert par la Directive ?

  Ex: le secteur des finances - la BNB; secteur de l'énergie – Ministre fédéral de l'Energie, etc

- Chaque État membre désigne « un point de contact national unique » qui exerce une fonction de liaison pour assurer une coopération transfrontalière entre les autorités des EM. ➡ **CCB ?**

- Chaque État membre désigne un ou plusieurs CSIRT chargés de la gestion des incidents et des risques selon un processus bien défini. ➡ **CERT.be ?**

Autorités de contrôle dans la loi de transposition ? (1)

- ✓ Le Centre pour la Cybersécurité Belgique (CCB) a été fondé par l'arrêté royal du 10 octobre 2014. Le CCB relève de l'autorité du Premier Ministre.

- ✓ Missions:
  1. Superviser, coordonner et veiller à la mise en œuvre de la stratégie belge en la matière ;
  2. Gérer par une approche intégrée et centralisée les différents projets relatifs à la cybersécurité ;
  3. Assurer la coordination entre les services et autorités concernés mais aussi entre autorités publiques et le secteur privé ou le monde scientifique ;
  4. Formuler des propositions pour l'adaptation du cadre légal et réglementaire en matière de cybersécurité
  5. Assurer la gestion de crise en cas de cyberincidents, en coopération avec le Centre de coordination et de crise du gouvernement ;
  6. Elaborer, diffuser et veiller à la mise en œuvre des standards, directives et normes de sécurité pour les différents types de systèmes informatiques des administrations et organismes publics ;
  7. Coordonner la représentation belge aux forums internationaux sur la cybersécurité, le suivi des obligations internationales et la présentation du point de vue national en la matière ;
  8. Coordonner l'évaluation et la certification de la sécurité des systèmes d'information et de communication ;
  9. Informer et sensibiliser les utilisateurs des systèmes d'information et de communication.

Autorités de contrôle dans la loi de transposition (2)

- ✓ CERT.be est la **cyber emergency team (l'équipe d'intervention d'urgence en sécurité informatique) fédérale** qui, en tant que spécialiste neutre de la sécurité, peut aider votre entreprise ou votre organisation en :

  - prenant en charge la coordination lors des incidents de cybersécurité
  - donnant des conseils permettant de trouver une solution en cas d'un incident de cybersécurité
  - offrant un soutient permettant de prévenir les incidents de sécurité.

➡ **À partir du 1 janvier 2017 CERT.be sera exploité par le Centre pour la Cybersécurité Belgique (CCB).**

Compétences des autorités de contrôle

✓ Exigences de sécurité ?

- Chaque EM adopte une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information (CCB ? Avec consultation des « autorités compétentes » ?)

- + rôle du groupe de coopération et de l'ENISA d'harmoniser ces critères au niveau EU

✓ Les « autorités compétentes » peuvent :

- **Exiger les informations nécessaires pour évaluer la sécurité**, y compris les documents relatifs à leurs politiques de sécurité; et des éléments prouvant la mise en œuvre effective tels que les résultats d'un audit de sécurité.

- **Donner des instructions contraignantes** pour corriger les manquements.

Obligation de notification en cas d'incident

- ✓ **Incident** : « *tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information* »

- ✓ Obligation de notification des opérateurs de services essentiels et des fournisseurs de services numériques auprès de l' « autorité compétente ou du CSIRT » ➡ CERT.be ?

- ✓ La notification doit être effectuée:
  - sans retard injustifié
  - si impact significatif sur la continuité des services qu'ils fournissent

- ✓ Possibilité du CERT.be (?) d'informer le public si la sensibilisation est nécessaire pour prévenir un incident ou gérer un incident en cours

NIS: Sanctions

- ✓ **NIS**: **Responsabilité pénale**: la loi de transposition doit prévoir des sanctions effectives, proportionnées et dissuasives.

- ✓ Attention, en cas de violation d'obligations relatives au traitement de données à caractère personnel, les sanctions du GDPR peuvent également s'appliquer !

2. Les obligations de sécurité

dans la loi du 13 juin 2005 relative aux communications électroniques

Les obligations de sécurité dans la loi du 13 juin 2005 (1)

- ✓ Les obligations de sécurité de l'art. 114 et s. de la loi du 13 juin 2005 relative aux communications électroniques ne sont pas affectées par la Directive NIS…:

Cons. 7: « *les obligations imposées aux opérateurs de services essentiels et aux fournisseurs de service numérique ne devraient pas s'appliquer aux entreprises qui fournissent des réseaux de communications publics ou des services de communications électroniques accessibles au public au sens de la directive 2002/21/CE* »

- ✓ Ni par le GDPR.

Cons. 173: « Le présent règlement devrait s'appliquer à tous les aspects de la protection des libertés et droits fondamentaux à l'égard du traitement des données à caractère personnel qui ne sont pas soumis à des obligations spécifiques ayant le même objectif énoncées dans la directive 2002/58/CE »

➡ La Directive 2002/58 est en cours de review

Les obligations de sécurité dans la loi du 13 juin 2005 (2)

- ✓ Les opérateurs prennent les mesures d'ordre technique et organisationnel appropriées pour gérer le risque en matière de sécurité des réseaux et des services (DACP ou non):
  - Compte tenu des possibilités techniques les plus récentes;
  - Niveau de sécurité adapté aux risques existants.
- ✓ Lorsqu'elles concernent des données à caractère personnel, les entreprises qui fournissent des services de communications électroniques accessibles au public prennent des mesures qui visent pour le moins à :
  - garantir l'accès des seules des personnes habilitées;
  - protéger contre la destruction, la perte ou l'altération, etc;
  - assurer la mise en oeuvre d'une politique de sécurité.

Les obligations de sécurité dans la loi du 13 juin 2005 (3)

- ✓ Les entreprises fournissant des réseaux publics de communications électroniques prennent toutes les mesures nécessaires, y compris préventives, pour :

  1° assurer l'intégrité de leur réseau et garantir ainsi la continuité des services fournis sur ce réseau;

  2° assurer la disponibilité la plus complète possible des services téléphoniques accessibles au public fournis via leur réseau en cas de défaillance catastrophique des réseaux ou de force majeure.

- ✓ Les opérateurs offrent gratuitement à leurs abonnés, compte tenu de l'état de la technique, les services de sécurité adéquats, afin de permettre aux utilisateurs finals d'éviter toute forme de communication électronique non souhaitée

Contrôle des obligations de sécurité dans la loi du 13 juin 2005

- ✓ L'IBPT est habilité à vérifier les mesures prises les entreprises qui fournissent des services de communications accessibles au public, ainsi qu'à émettre des recommandations sur les meilleures pratiques concernant le degré de sécurité que ces mesures devraient permettre d'atteindre.

- ✓ L'IBPT a le pouvoir de donner des instructions contraignantes aux opérateurs en vue de l'application des articles 114 et s.

- ✓ Les opérateurs fournissent à l'IBPT, à sa demande, toutes les informations nécessaires pour évaluer la sécurité ou l'intégrité, ou les deux, de leurs services et réseaux, y compris les documents relatifs à leur politique de sécurité.

- ✓ A la demande de l'IBPT, les opérateurs se soumettent à un contrôle de sécurité effectué par un organisme qualifié indépendant ou l'Institut lui-même

Notifications dans la loi du 13 juin 2005

- ✓ Lorsqu'il existe un risque particulier de violation de la sécurité du réseau, les entreprises informent les abonnés et l'IBPT de ce risque
- ✓ Les opérateurs notifient sans délai à l'IBPT toute atteinte à la sécurité ou perte d'intégrité ayant eu un impact significatif sur le fonctionnement des réseaux ou des services (pas forcément DACP).
- ✓ En cas de violation de données à caractère personnel, l'entreprise fournissant des services de communications électroniques accessibles au public avertit sans délai la CPVP de la violation de données à caractère personnel, qui en avertit sans délai l'Institut
- ✓ Lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier, l'entreprise fournissant des services de communications électroniques accessibles au public avertit également sans délai l'abonné ou le particulier concerné de la violation.

UNIVERSITÉ DE NAMUR

crids
CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Merci pour votre attention !

Franck Dumortier
Chercheur senior et chargé de cours
Centre de Recherche Information, Droit et Société (CRIDS)
franck.dumortier@unamur.be