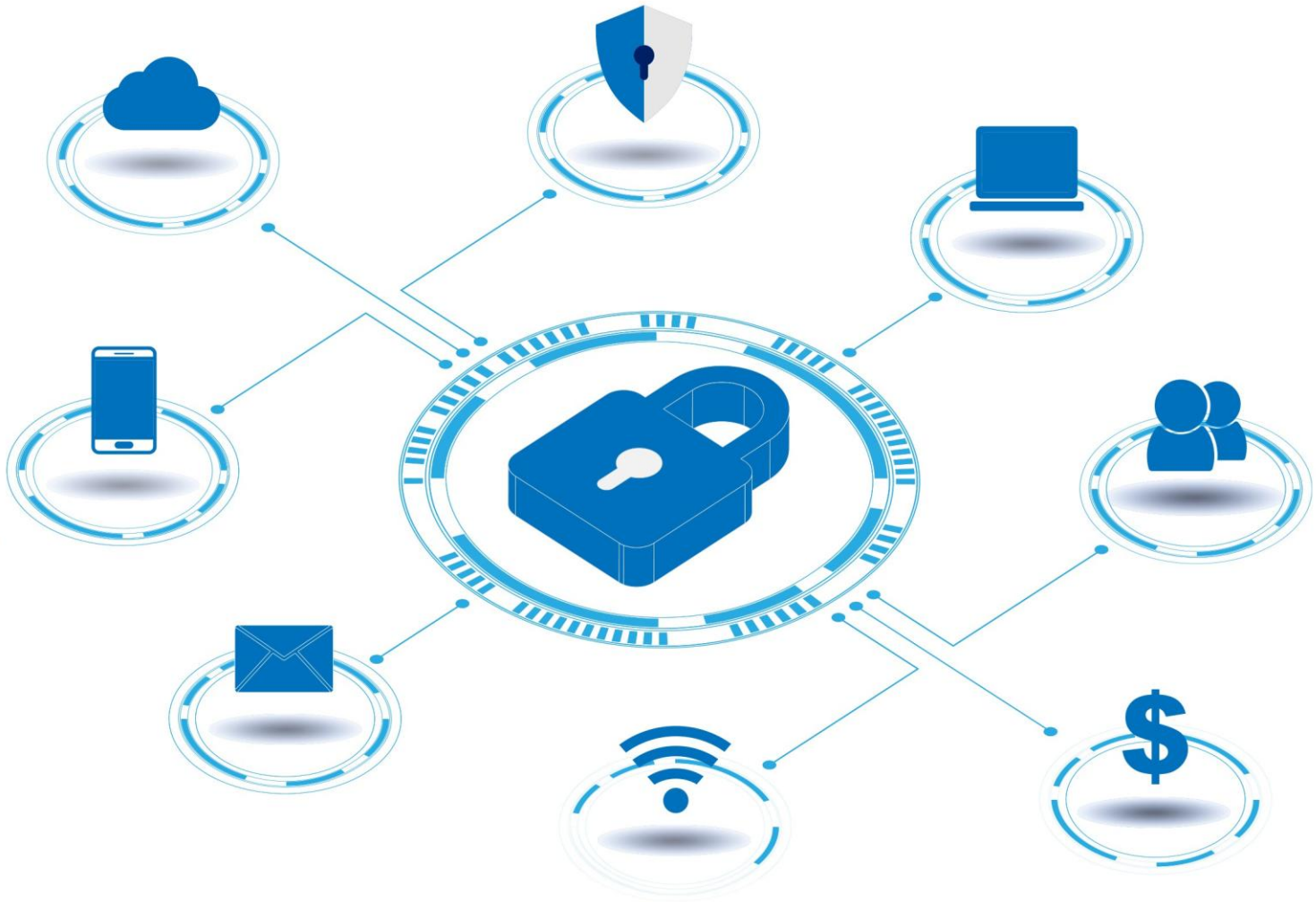
CyberActive

sirris innovation forward

VUB VRIJE UNIVERSITEIT BRUSSEL

UCLouvain

howest hogeschool



Funded by

economie

Funded by the European Union
NextGenerationEU

NIS2 & Cybersécurité

L'ESSENTIEL POUR DIRIGEANTS ET ADMINISTRATEURS

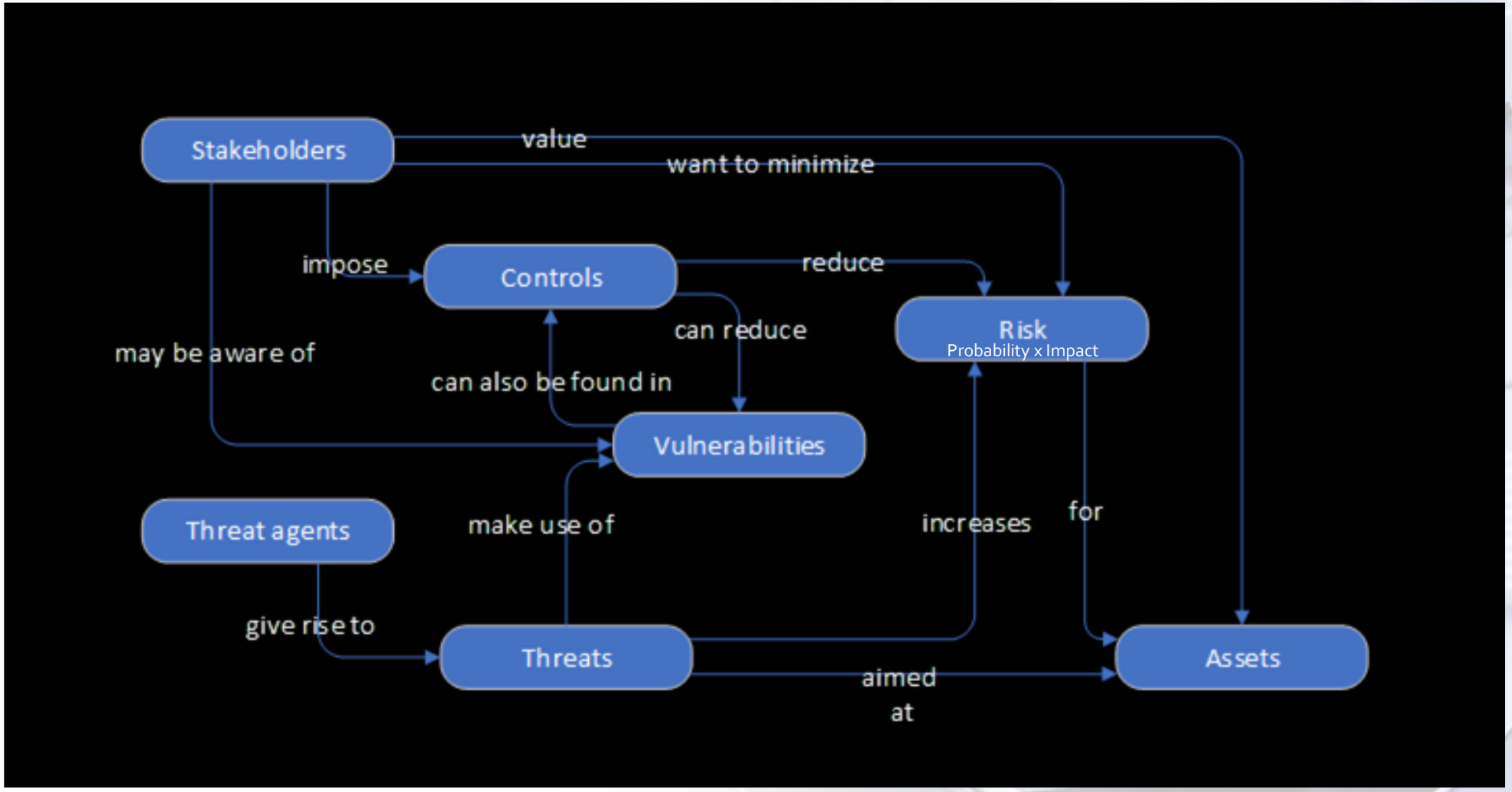
Agenda

- Les fondamentaux de la cybersécurité
- NIS 2 et responsabilités du conseil d'administration et de la direction générale
- Gouvernance de la cybersécurité, gestion des risques et conformité :
  - Exigences légales et réglementaires
  - Evaluation des risques cybernétiques et continuité des activités
  - Gestion des incidents et réponse aux crises
- Budget Cybersécurité : retour sur investissement vs réduction des risques
- Sensibilisation des employés et culture de la cybersécurité
- Wrap-up
- Annexe : NIS2 et Cyfun, comment démarrer ?

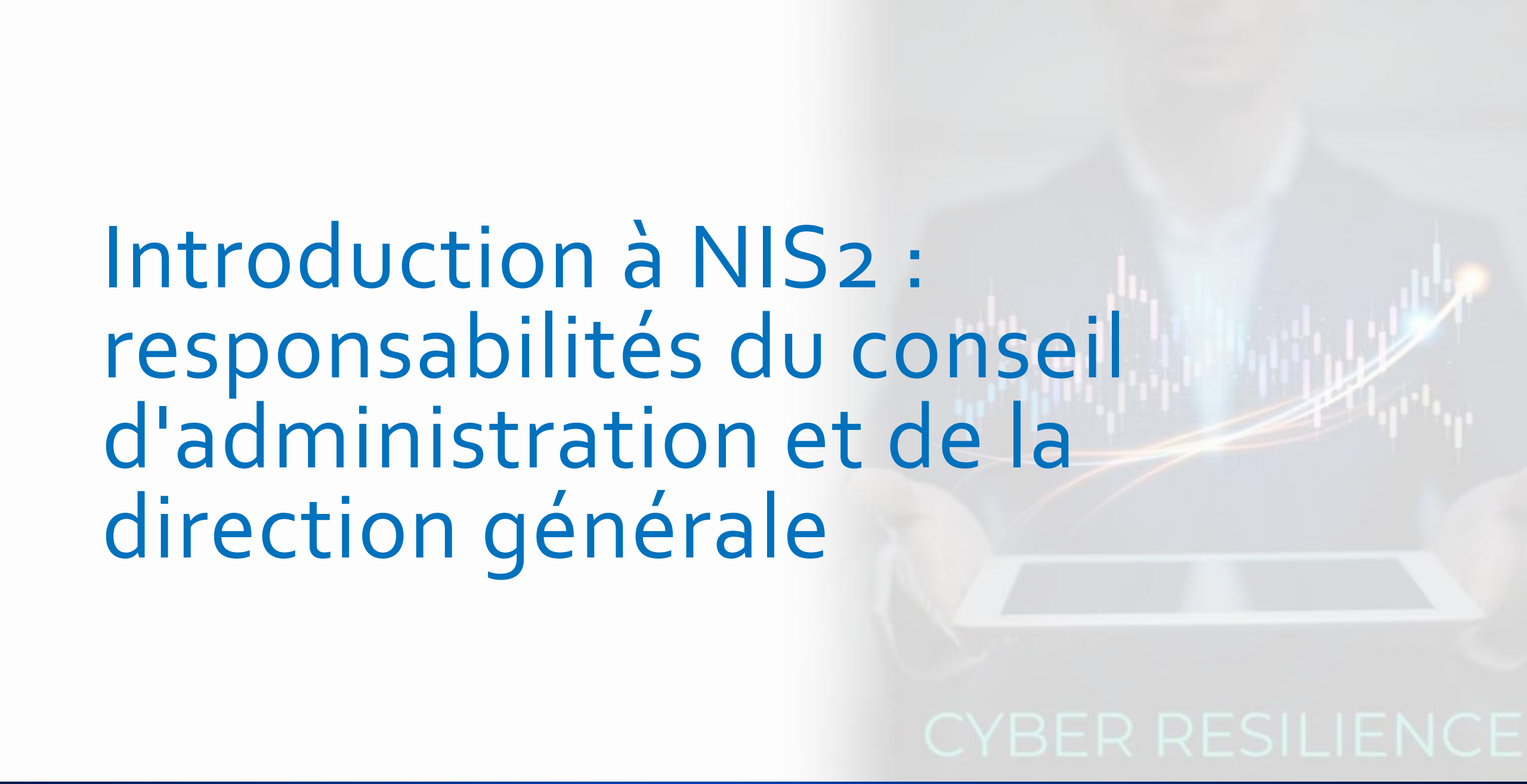
Les fondamentaux de la cybersécurité

Cube de la cybersécurité : éléments de stratégie

Terminologie

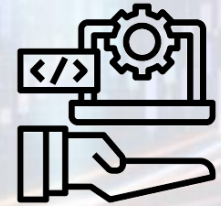


Introduction à NIS2 : responsabilités du conseil d'administration et de la direction générale



Qu'est-ce que **la directive NIS2** ? Pourquoi est-elle importante pour les PME ?

La NIS2 (directive sur la sécurité des réseaux et de l'information 2) est la dernière réglementation européenne visant à renforcer la cybersécurité des entreprises et des organisations. Elle remplace la directive NIS initiale et élargit considérablement son champ d'application.



- Le NIS2 **couvre désormais un plus grand nombre d'entreprises** qu'auparavant.

- Les cybermenaces (telles que les ransomwares, le phishing et les violations de données) sont en augmentation.

- Les CEO et les dirigeants **peuvent être tenus personnellement responsables** des défaillances en matière de cybersécurité. La responsabilité personnelle est engagée en cas de sérieuse négligence et de manquement aux obligations.

- **Les amendes peuvent atteindre 10 millions d'euros** ou **2 % du chiffre d'affaires annuel mondial**.

Qu'est-ce que **la directive NIS2** ? Pourquoi est-elle importante pour les PME ?

La NIS2 (directive sur la sécurité des réseaux et de l'information 2) est la dernière réglementation européenne visant à renforcer la cybersécurité des entreprises et des organisations. Elle remplace la directive NIS initiale et élargit considérablement son champ d'application.

- Le NIS2 **couvre désormais un plus grand nombre d'entreprises** qu'auparavant.
- Les cybermena… ont en augmentation…
- Les CEO et les … nces en matière de cybersécuri… e et de manquement aux obligations.
- **Les amendes peuvent atteindre 10 millions d'euros** ou **2 % du chiffre d'affaires annuel mondial**.

Tout comme le RGPD a fait de la protection des données une priorité, la NIS2 fait de la cybersécurité **une responsabilité au niveau du conseil d'administration.**

Quelles sont les entreprises concernées ?

« Entités essentielles » (impact élevé, réglementation plus stricte)

Secteurs tels que **l'énergie, les transports, la santé, la finance, les services publics**

Opérateurs d'infrastructures critiques

« Entités importantes » (impact modéré, réglementation stricte)

Société dans des secteurs tels que **les services numériques, la fabrication, la production alimentaire, les services postaux et la gestion des déchets**

Entreprises **de plus de 50 salariés ou dont le chiffre d'affaires est supérieur à 10 millions d'euros**

Quelles sont les entreprises concernées ?

« Entités essentielles » (impact élevé, réglementation plus stricte)

Secteurs tels que l'énergie, les **transports, la sa**
services publics

Opérateurs d'inf

« Entités importantes » (impact modéré, réglementation stricte)

Société dans des secteurs tels que **les fabrication, la , les services es déchets**

o salariés ou s est supérieur à 10 millions d'euros

📌 **Même si vous n'êtes pas directement concerné par la directive NIS2, vos partenaires et clients peuvent l'être, ce qui signifie que vous devrez tout de même répondre à *leurs* attentes en matière de cybersécurité.**

Responsabilités juridiques et financières du CEO en vertu de la NIS2

✅ Gestion des risques cybernétiques : vous devez identifier les risques, protéger les actifs critiques et atténuer les menaces avant qu'elles ne causent des dommages.

✅ Signalement des incidents : en cas de cyberattaque, vous devez la signaler dans les 24 heures aux autorités belges.

✅ Sécurité de la chaîne d'approvisionnement : vous êtes tenu de vous assurer que les fournisseurs tiers (par exemple, les prestataires informatiques) respectent les normes de cybersécurité.

✅ Sensibilisation à la cybersécurité au niveau du conseil d'administration : la directive NIS2 exige une formation à la cybersécurité et à la gestion des risques au niveau de la direction. L'ignorance n'est plus une excuse.

✅ Responsabilité et amendes : le non-respect de ces obligations peut entraîner des amendes pouvant atteindre 10 millions d'euros ou 2 % du chiffre d'affaires, et dans les cas graves, la responsabilité personnelle des dirigeants.

Responsabilités juridiques et financières du CEO en vertu de la NIS2

✅ Gestion des risques cybernétiques : vous devez identifier les risques, protéger les actifs critiques et atténuer les menaces avant qu'elles ne causent des dommages.

✅ Signalement des in heures aux autorités belges.

✅ Sécurité de la chaî rnisseurs tiers (par exemple, les prestatair

✅ Sensibilisation à la cybersécurité au niveau du conseil d'administration : la directive NIS2 exige une formation à la cybersécurité et à la gestion des risques au niveau de la direction. L'ignorance n'est plus une excuse.

✅ Responsabilité et amendes : le non-respect de ces obligations peut entraîner des amendes pouvant atteindre 10 millions d'euros ou 2 % du chiffre d'affaires, et dans les cas graves, la responsabilité personnelle des dirigeants.

📌 **Qui est responsable de l'application de la réglementation en Belgique ?**

Le **Centre pour la Cybersécurité Belgique (CCB)** supervise la conformité à la directive NIS2. Il veille à ce que les entreprises respectent les règles et signalent correctement les incidents.

Points clés à retenir pour les décideurs

La cybersécurité n'est plus seulement un problème informatique ou juridique, c'est une priorité commerciale.

Les autorités pourraient tenir les dirigeants responsables des incidents cyber, tout comme le RGPD les tient responsables des violations de données.

Il est souvent moins coûteux d'investir dans la cybersécurité que de faire face à des amendes, des poursuites judiciaires et une atteinte à la réputation.

Gouvernance en matière de cybersécurité et gestion des risques

Élaborer une stratégie de cybersécurité : l'approche fondée sur les risques

En tant que CEO, vous gérez déjà les risques tels que **les pertes financières, les défaillances opérationnelles et la responsabilité juridique**. La cybersécurité n'est pas différente.

Une stratégie de cybersécurité ne consiste pas à tout protéger de manière égale, mais à **se concentrer sur ce qui importe le plus**. → Approche basée sur les risques

Identifier ce qui importe le plus (les actifs critiques tels que les données clients, les systèmes financiers ou la boutique en ligne).

↓

Hiérarchiser les menaces susceptibles d'avoir un impact sur les opérations commerciales.

↓

Allouer les ressources de manière judicieuse (les PME ne disposent pas de budgets illimités).

Élaborer une stratégie de cybersécurité : l'approche fondée sur les risques

En tant que CEO, vous gérez déjà les risques tels que **les pertes fin**
défaillances opérationnelles et la responsabilité juridique. La cy
pas différente.

Parallèle avec sécurité incendie : risque d'incendie, système à déployer, formation des employés, assurance de l'entreprise

Une stratégie de cybersécurité ne consiste pas à tout protéger de
mais à **se concentrer sur ce qui importe le plus**. → Approche basé

Identifier ce qui importe le plus (les actifs critiques tels que les données clients, les systèmes financiers ou la boutique en ligne).

↓

Hiérarchiser les menaces susceptibles d'avoir un impact sur les opérations commerciales.

↓

Allouer les ressources de manière judicieuse (les PME ne disposent pas de budgets illimités).

Cadre d'évaluation des risques en trois étapes

Identifier ce qui doit être protégé

Quels sont les systèmes, les actifs et les données qui causeraient des dommages importants s'ils étaient piratés ?

Évaluer les menaces les plus importantes

- Quelles sont les cybermenaces les plus probables (hameçonnage, ransomware, tiers) ?
- Utilisez une notation faible-moyenne-élevée

Agir : atténuer et surveiller (diminuer la vraisemblance)

- Mesures de sécurité simples et rentables (sauvegarde, authentification multifactorielle, formation)

CYBER RESILIENCE

Fiche d'évaluation des risques

	Étape	Description
1	Identifier les actifs critiques	Répertoriez les données, systèmes ou opérations les plus importants (par exemple, les données clients, le système financier, le site Web).
2	Évaluer les menaces les plus importantes	Identifiez les menaces potentielles (par exemple, hameçonnage, ransomware, violation de la sécurité chez un fournisseur).
3	Évaluer le niveau de risque	Évaluer la probabilité et l'impact des menaces (faible, moyen, élevé).
4	Mesures d'atténuation	Spécifiez des mesures de sécurité simples (par exemple, sauvegardes, authentification multifactorielle, formation des employés).
5	Responsable	Attribuez la responsabilité à un membre de l'équipe ou à un expert externe.
6	Planification des mesures	Fixer des délais/un budget pour la mise en œuvre des mesures de sécurité.

Revue et amélioration continue

Surveiller et améliorer en permanence →

Les cyber risques évoluent, votre stratégie de sécurité doit donc en faire autant.

Leadership en matière de cybersécurité : nomination d'un responsable de la sécurité (CISO ou équivalent)

- Dans le cadre de la directive NIS2, **la direction doit assumer la responsabilité** de la cybersécurité, et pas seulement les équipes informatiques ou le sous-traitant.

- Même si votre PME ne dispose pas d'un **responsable de la sécurité des systèmes d'information (CISO)** à temps plein, quelqu'un doit être **chargé de la cybersécurité**.

Qui peut occuper ce poste ?

- **Responsable informatique interne** (s'il est qualifié en cybersécurité). Mais attention au potentiel conflit d'intérêt. Il est juge et partie.

- **Conseiller externe en cybersécurité** (consultant externe pour les PME)

- **Un cadre supérieur/membre du conseil d'administration sensibilisé à la cybersécurité** (même un CEO, un directeur financier ou un directeur des opérations peut superviser les décisions en matière de sécurité avec l'aide d'un expert).

Que fait cette personne ?

- **Supervise la gestion des risques et la conformité** (veille au respect des exigences NIS2 ou des ambitions) – (Outils : CyFun self-assessment, CISOAssistant,…)
- **Elle conseille la direction** sur les décisions en matière de sécurité.
- **Coordonne les mesures liées à la sécurité** telles que la formation des employés et les plans d'intervention en cas d'incident.
- **Collabore avec des prestataires informatiques tiers** pour garantir la sécurité des systèmes.

📌 **Pour les petites entreprises, l'embauche d'un CISO à temps plein peut être irréaliste, mais la désignation d'un responsable clairement chargé de la cybersécurité est une exigence non négociable en vertu de la directive NIS2.**

Responsabilité au niveau du conseil d'administration: rapports sur les risques liés à la cybersécurité

✔ **Les cyber risques doivent être discutés au niveau du conseil d'administration**, et pas seulement lors des réunions « informatiques ».

✔ **Les cadres dirigeants doivent suivre une formation en cybersécurité** afin de comprendre leurs responsabilités.

✔ **La cybersécurité doit être intégrée à la gestion financière et** non considérée comme un coût informatique à réduire.

Comment faire part des cyber risques au conseil d'administration ?

- **Les 3 à 5 principaux cyber risques** affectant l'entreprise (par exemple : hameçonnage, mots de passe faibles, logiciels non mis à jour).
- **Impact des cybermenaces sur l'entreprise** (combien de temps d'arrêt, de pertes financières ou d'atteinte à la réputation cela entraînerait-il ?).
- **Mesures de sécurité actuelles** (quelles protections sont en place ? Où se trouvent les failles ?).
- **Plan d'action** (Que faut-il faire ensuite ? Qui est responsable ?).

✅ **Exemple de rapport au conseil d'administration :**
*« Au cours du dernier trimestre, nous avons identifié **les e-mails de phishing comme le plus grand risque pour notre entreprise.***
*Lors d'un test récent, **60 % des employés** n'ont pas su reconnaître une tentative d'hameçonnage.*
*Pour atténuer ce risque, nous allons organiser **une formation obligatoire sur la cybersécurité** et mettre en place **des solutions de filtrage des e-mails**.*
*Calendrier : **3 prochains mois + budget 20k**. »*

Comment faire part des cyber risques au conseil d'administration ?

- **Les 3 à 5 principaux cyber risques** affectant l'entreprise (par exemple : hameçonnage, mots de passe faibles, logiciels non mis à jour).
- **Impact des cybermenaces sur l'entreprise** (combien de temps d'arrêt, de pertes financières ou d'atteinte à la réputat
- **Mesures de sécurité** t les failles ?).
- **Plan d'action** (Que fa

📌 **Message clé pour les CEO: si vous ne suivez pas les risques liés à la cybersécurité, vous ne pouvez pas les gérer.**

✅ **Exemple de rapport au conseil d'administration :**

*« Au cours du dernier trimestre, nous avons identifié **les e-mails de phishing comme le plus grand risque pour notre entreprise.***
*Lors d'un test récent, **60 % des employés** n'ont pas su reconnaître une tentative d'hameçonnage.*
*Pour atténuer ce risque, nous allons organiser **une formation obligatoire sur la cybersécurité** et mettre en place **des solutions de filtrage des e-mails**.*
*Calendrier : **3 prochains mois + budget 20k**. »*

Points clés à retenir pour les CEO

Une stratégie de cybersécurité fondée sur les risques garantit que les ressources sont concentrées sur les menaces les plus critiques.

La nomination d'un responsable de la cybersécurité (interne ou externe) est obligatoire en vertu de la directive NIS2.

Les CEO doivent recevoir régulièrement des rapports sur les cyber risques et discuter de la cybersécurité au niveau du conseil d'administration.

Exigences légales et réglementaires

Obligations de conformité en Belgique : pour les entreprises belges relevant du champ d'application de la directive NIS2

Mettre en œuvre des mesures **appropriées de gestion des risques liés à la cybersécurité**.

Établir **des procédures d'intervention en cas d'incident** et signaler les violations de sécurité.

Assurer **la sécurité de la chaîne d'approvisionnement**, en particulier pour les fournisseurs de services informatiques.

Suivre **une formation de sensibilisation à la cybersécurité au niveau de la direction** (y compris aux CEO et aux cadres supérieurs).

Obligations de conformité en Belgique : pour les entreprises belges relevant du champ d'application de la directive NIS2

Mettre
mesures
gestion d
la cyb

océdures
n en cas
gnaler les
sécurité.

Assurer **la**
c
d'approvis
particu
fournisseurs de services informatiques.

nation de
on à la
u niveau de
ompris aux
CEO et aux cadres supérieurs).

📌 **Qui est responsable de l'application de la réglementation en Belgique ?**
Le **Centre pour la Cybersécurité Belgique (CCB)** supervise la conformité à la directive NIS2. Il veille à ce que les entreprises respectent les règles et signalent correctement les incidents.

Règles de notification des incidents

Si votre entreprise est victime d'une cyberattaque (par exemple, ransomware, violation de données) et si l'incident est significatif, vous devez :

- **Notifier l'incident dans les 24 heures** à **l'autorité belge chargée de la cybersécurité (CCB)**.
- Fournir un **rapport détaillé dans les 72 heures** sur l'impact, la cause et les mesures prises.
- **Une mise à jour finale dans un délai d'un mois** avec les enseignements tirés et les améliorations futures en matière de sécurité.

🚨 **Le non-signalement des incidents dans les délais impartis peut entraîner des amendes.**

Règles de notification des incidents

Si votre entreprise est victime d'une cyberattaque (par exemple, ransomware, violation de données) et si l'incident est significatif, vous devez :

- **Notifier l'incident dans les 24 heures** à **l'autorité belge chargée de la cybersécurité (CCB).**
- Fournir un **rapport détaillé dans les 72 heures** sur l'impac
- **Une mise à jour finale dans un délai d'un mois** avec les e de sécurité.

📌 **Qui prévenir en Belgique ?**
Centre pour la cybersécurité Belgique (CCB) et l'Autorité de Protection des Données (APD), si des données à caractère personnel sont compromises
(conformément au RGPD)

🚨 **Le non-signalement des incidents dans les délais impartis peut entrainer des amendes.**

NIS2 et RGPD

- Si une **cyberattaque expose les données de vos clients**, votre PME peut être sanctionnée **à la fois** par **la NIS2 et le RGPD**.
- **Une bonne cybersécurité réduit les risques liés au RGPD** (par exemple, le chiffrement des données clients empêche les violations).
- **Conformité au RGPD ≠ conformité à la NIS2** → Votre entreprise doit respecter les deux !

NIS2	RGPD
Se concentre sur **les risques liés à la cybersécurité** et la continuité des activités.	Se concentre sur **la protection des données personnelles**.
Exige **des mesures de gestion des risques cybernétique**	Exige des pratiques **de traitement des données axées sur la confidentialité**.
Signalement des incidents à **la CCB (autorité belge chargée de la cybersécurité)**.	Signalement des violations de données à **l'APD (Autorité de protection des données)**.
Amendes en cas de pratiques de sécurité insuffisantes.	Amendes en cas de mauvaise gestion des données à caractère personnel.

Comment signaler un incident de cybersécurité conformément à la directive NIS2

- Depuis le **18 octobre 2024, toutes les entités NIS2 sont tenues de signaler** les incidents significatifs au CCB:

24h - 72h – sur demande – final : 1 mois

- Les incidents importants peuvent être signalés au CCB via sa plateforme de notification des incidents

https://notif.safeonweb.be/

- ou par téléphone au

+32 (0)2 501 05 60 (**uniquement pour les urgences concernant les entités NIS2**)

- Guide des notifications : https://ccb.belgium.be/sites/default/files/2025-08/NIS2_Notification_guide_v1.3-FR.pdf

Amendes et responsabilité : que se passe-t-il en cas de non-conformité ?

Problème de non-conformité	Sanction
Non-signalement d'incidents	Amendes pouvant atteindre **10 millions d'euros** ou **2 % du chiffre d'affaires mondial**.
Absence de gestion des risques liés à la cybersécurité	Mesures réglementaires, sanctions financières et restrictions commerciales potentielles.
Négligence des responsabilités du conseil d'administration en matière de cybersécurité	**Les PDG et les dirigeants peuvent être tenus personnellement responsables**.

Une PME ne met pas à jour ses systèmes →

Des pirates informatiques volent les données des clients →

Amende en vertu du RGPD et de la directive NIS2

Amendes et responsabilité : que se passe-t-il en cas de non-conformité ?

Problème de non-	
Non-signalement	uros ou 2 % du
Absence de gestio cybersécurité	res et restrictions
Négligence des re d'administration e cybersécurité	us

📌 **Message clé pour les CEO** :

- Vous **ne pouvez pas déléguer l'entière responsabilité au service informatique ou juridique** : vous devez vous impliquer !
- **Une cybersécurité proactive** coûte moins cher!
- **Les poursuites judiciaires et l'atteinte à la réputation** ont un impact sur votre entreprise.

Une PME ne met pas à jour ses systèmes →

Des pirates informatiques volent les données des clients →

Amende en vertu du RGPD et de la directive NIS2

Points clés à retenir pour les CEO

La loi NIS2 exige une gouvernance et un reporting rigoureux en matière de cybersécurité

Le signalement des incidents significatifs dans les 24h est obligatoire

La direction générale et les membres du conseil d'administration doivent être directement impliqués dans la cybersécurité

Évaluation des risques cybernétiques et continuité des activités

Identification des actifs critiques et des vulnérabilités potentielles : quels sont les risques ?

Les actifs critiques sont les **données, les systèmes et les processus** sans lesquels votre entreprise ne peut fonctionner.

- *Bases de données clients*
- *Systèmes financiers et de facturation*
- *Plateformes de commerce électronique*
- *Systèmes de gestion des employés et de la paie*
- *Outils de messagerie électronique et de communication interne*

POURQUOI EST-CE IMPORTANT ?

Une vulnérabilité est un **point faible** de vos systèmes numériques que les pirates peuvent exploiter.

- *Logiciels obsolètes*
- *Mots de passe faibles*
- *Absence de sauvegardes*
- *Employés non sensibilisés aux menaces de hameçonnage (phishing)*

Identification des actifs critiques et des vulnérabilités potentielles : quels sont les risques ?

Les actifs critiques sont les **données, les systèmes et les processus** sans lesquels votre entreprise ne peut fonctionner.

- *Bases de données clients*
- *Systèmes financiers*
- *Plateformes de con*
- *Systèmes de gestio*
- *Outils de messager*
  communication int

Une vulnérabilité est un **point faible** de vos systèmes numériques que les pirates peuvent exploiter.

- *Logiciels obsolètes*

les

isés aux menaces de
ng)

📌 **Conseil d'action pour la direction** :
Demandez à votre fournisseur informatique un **inventaire** de base **des actifs** et une liste des vulnérabilités connues. Même une simple feuille Excel vaut mieux que des suppositions !

POURQUOI EST-CE IMPORTANT ?

CYBER RESILIENCE

Sécurité de la chaîne d'approvisionnement et conformité des entités tierces : mesures clés

*Si votre **fournisseur informatique**, **votre service cloud** ou **votre comptable externe** est piraté et que cela affecte votre entreprise, **vous restez responsable**.*

Identifiez tous **les fournisseurs tiers** essentiels (assistance informatique, plateformes logicielles, services cloud, etc.)

Demandez à ces fournisseurs :

Avez-vous mis en place des politiques de cybersécurité ?

Vos systèmes sont-ils régulièrement mis à jour et corrigés ?

Comment gérez-vous le signalement des incidents ?

Incluez **des clauses de cybersécurité dans les contrats** avec les partenaires externes.

Sécurité de la chaîne d'approvisionnement et conformité des entités tierces : mesures clés

*Si votre **fournisseur informatique**, **votre service cloud** ou **votre comptable externe** est piraté et que cela affecte votre entreprise, **vous restez responsable**.*

Identifiez tous **les fournisseurs tiers** essentiels (assistance informatique, plateformes logicielles, services cloud, etc.)

Demandez à ces fournisseurs :

Avez-vous mis en place des politiques de cybersécurité ?

Vos systèmes sont-ils régulièrement mis à jour et corrigés ?

Comment gérez-vous le signalement des incidents ?

Incluez **des clauses de cybersécurité dans les contrats** avec les partenaires externes.

Planification de la continuité des activités et reprise après sinistre

Un **plan de continuité des activités (PCA)** décrit comment votre entreprise **continuera à fonctionner** après un incident cybernétique ou une panne système.

Un plan de reprise d'activité (PRA) détaille la manière dont vous **restaurerez les données et les systèmes perdus** après une interruption.

Mesures minimales que toute PME devrait prendre

Sauvegardes : sauvegardez automatiquement les données critiques au moins une fois par jour. Stockez les sauvegardes hors ligne ou dans un cloud distinct.
Règle 3 – 2 – 1 – 1 - 0

Contrôle d'accès : sachez qui peut accéder à quelles données. Limitez les accès administrateur, y compris sur les postes de travail

Plan de reprise : rédigez un document simple répondant aux questions suivantes :

Qui fait quoi si nous sommes attaqués ?

À quelle vitesse pouvons-nous rétablir les opérations ?

Qui sont nos contacts essentiels (informatique, juridique, assurance, communication, etc.) ?

Mesures minimales que toute PME devrait prendre

Sauvegardes : sauvegardez automatiquement les données critiques au moins une fois par jour. Stockez les sauvegardes hors ligne ou dans un cloud distinct.

Règle 3 – 2 – 1 – 1 - 0

Contrôle d'accès : sachez qui peut accéder à quelles données. Limitez les accès administrateur, y compris sur les postes de travail

📌 La continuité des activités n'est pas seulement l'affaire du service informatique. Elle a des répercussions sur **les ventes, le service client, les finances et la réputation.** Vous devez diriger les efforts de reprise.

Qui fait quoi si nous sommes attaqués ?

À quelle vitesse pouvons-nous rétablir les opérations ?

Qui sont nos contacts essentiels (informatique, juridique, assurance, communication, etc.) ?

Fiche de travail sur la continuité des activités (PCA)

	Section	Description
1	Fonctions commerciales essentielles	Énumérez les 3 à 5 processus essentiels que votre entreprise doit maintenir (par exemple, les ventes, le service client, la facturation).
2	Personnel clé et coordonnées	Noms, rôles et coordonnées des membres du personnel chargés des tâches de continuité et de reprise.
3	Procédure de sauvegarde	Décrivez comment les données sont sauvegardées (fréquence, emplacement, méthode) et comment y accéder.
4	Modalités de travail alternatives	Prévoyez comment les employés peuvent continuer à travailler si les bureaux ou les systèmes sont inaccessibles (par exemple, travail à distance).
5	Plan de communication	Comment vous informerez les employés, les clients et les partenaires en cas d'incident (outils, canaux, calendrier).
6	Étapes de réponse aux incidents	Réponse étape par étape : détecter, évaluer, contenir, signaler et récupérer après l'incident.
7	Calendrier de rétablissement (PRA)	Fixer des objectifs réalistes : à quelle vitesse chaque fonction doit être restaurée (par exemple, 24h, 48h).
8	Partenaires externes et fournisseurs	Dressez la liste des principaux fournisseurs (par exemple, informatique, cloud, fournisseurs) et leur rôle dans la reprise. Assurez-vous à l'avance d'une disponibilité minimale des acteurs essentiels.
9	Leçons apprises et mises à jour du plan	Documentez ce qui a bien fonctionné ou ce qui n'a pas fonctionné après un incident réel ou simulé ; mettez régulièrement à jour le plan.

Points clés à retenir pour les dirigeants

Sachez ce qu'il est le plus important de protéger (actifs/process critiques)

Le risque lié aux entités tierces est votre risque

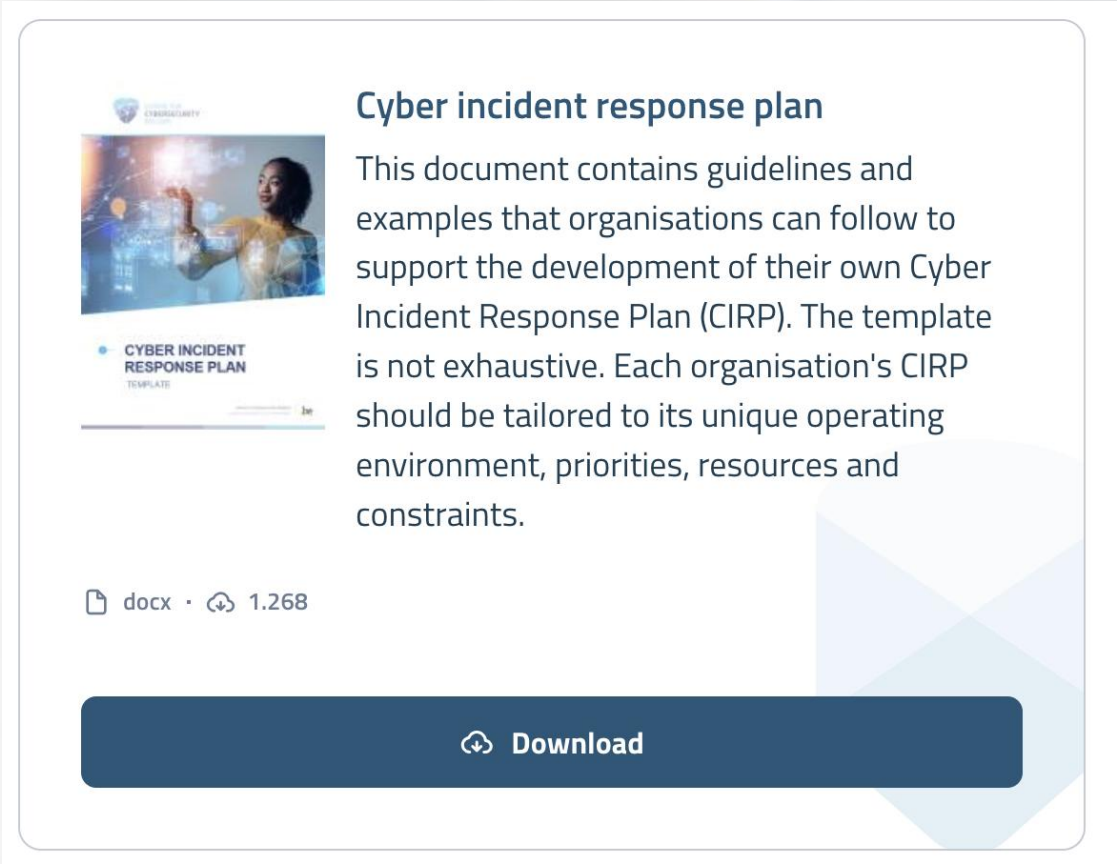
Prévoyez non seulement de prévenir les attaques, mais aussi de **rebondir** rapidement

Gestion des incidents et réponse aux crises

Qu'est-ce qu'un plan de réponse aux incidents (PRI) ?

Plan étape par étape qui guide votre équipe :

- **Détecter** la menace
- **Contenir** les dommages
- **Eradiquer** de la menace
- **Reprendre** les opérations
- **Tirer les leçons** de l'incident



📌 Disposez-vous d'un plan de réponse en cas d'incident ?

https://atwork.safeonweb.be/fr/tools-resources/policy-templates

Éléments clés du PRI

Rôles et responsabilités

- Qui est responsable de quoi ?

Processus de détection

- Comment l'équipe reconnaîtra-t-elle une violation d'accès ?

Plan de communication

- Qui doit être informé (en interne et en externe) ?

Mesures de confinement

- Comment empêcher la propagation ?

Mesures de rétablissement

- Comment restaurer les systèmes et les données ?

Obligations de déclaration

- Informer **le CCB** (Centre pour la cybersécurité Belgique) dans **les 24 heures** conformément à la directive NIS2

Examen post-incident

- Qu'est-ce qui n'a pas fonctionné ? Que peut-on améliorer ?

📌 **Conseil aux PME** : votre PRI n'a pas besoin d'être complexe. Une simple liste de contrôle avec des responsabilités clairement définies peut éviter le chaos en cas de crise.

Comment réaliser une simulation basique d'incident cybernétique ?

- Choisissez un scénario simple : par exemple, un e-mail contenant un ransomware arrive dans la boîte de réception d'un employé.
- Passez en revue le plan d'intervention avec les membres clés de l'équipe.
- Demandez :
  - Que ferait chaque personne ?
  - Qui doit être informé ?
  - Quels sont les systèmes affectés ?
- Chronométrez la réponse et identifiez les goulots d'étranglement ou les points de confusion.

https://cyber4sme.be/nos-ateliers/

Comment réaliser une simulation basique d'incident cybernétique ?

- Choisissez un scénario simple : par exemple, un e-mail contenant un ransomware arrive dans la boîte de réception d'un employé.
- Passez en revue le plan d'intervention avec les membres clés de l'équipe.
- Demandez :
  - Que ferait chaque
  - Qui doit être infor
  - Quels sont les systèmes affectés ?
- Chronométrez la réponse et identifiez les goulots d'étranglement ou les points de confusion.

📌 **Commencez modestement** : un bref exercice tous les six mois peut considérablement améliorer votre état de préparation.

https://cyber4sme.be/nos-ateliers/

Rôle de la direction dans la gestion de crise

Restez informé. Même si vous n'êtes pas un expert technique.

Prenez des décisions rapides : approuvez, informez les autorités, déclenchez le plan de communication.

Communiquez clairement :

En interne : rassurez les employés et donnez des instructions claires.

En externe : informez les clients, les partenaires ou les médias si nécessaire, avec précision et calme.

Points clés à retenir pour la direction générale

Un plan d'intervention en cas d'incident est essentiel et doit être **testé.**

Les exercices et les simulations rendent votre équipe **plus rapide, plus intelligente** et plus calme

Dirigez avec clarté, rapidité et transparence

Budget cybersécurité : retour sur investissement vs réduction des risques

Combien devrions-nous dépenser pour la cybersécurité ?

- Plutôt que de considérer la cybersécurité comme un **centre de coûts**, voyez-la comme un **outil de gestion des risques** similaire aux alarmes incendie, aux conseils juridiques ou au contrôle qualité.
- Le retour sur investissement en matière de cybersécurité ne concerne pas le profit direct, mais la prévention des pertes.

Catégorie	Exemple Valeur (EUR)	Explication
Coût estimé d'une attaque par ransomware (sans investissement)	50000	Coût total estimé en cas de cyberattaque (par exemple, temps d'arrêt, frais juridiques, reprise).
Investissement dans la cybersécurité (annuel)	5000	Coût annuel pour la sécurité (par exemple, authentification multifactorielle, sauvegardes, formation).
Probabilité d'incident sans protection	30%	Probabilité qu'une cyberattaque touche votre entreprise sans protection.
Probabilité d'incident avec protection (les mesures de base protègent contre 80 % des attaques)	5%	Réduction de la probabilité d'incident après la mise en œuvre de mesures de sécurité de base.
Perte prévue sans protection	=50000*0,3	Perte estimée multipliée par la probabilité sans sécurité.
Perte attendue avec protection	=50000*0,05	Perte estimée multipliée par la probabilité avec sécurité.
Économies estimées grâce à l'investissement	12 500	Réduction de la perte attendue moins le coût annuel de la cybersécurité.

Principes budgétaires pour les PME

- Commencez par établir un **budget de base** (généralement 5 à 10 % des dépenses informatiques).
- Concentrez-vous d'abord sur **les actions à fort impact et à faible coût** (par exemple : formation des employés, authentification multifactorielle, sauvegardes).
- Investissez dans **l'amélioration continue**, et pas seulement dans des solutions ponctuelles.
- Évaluez la cybe **es risques**.

📌 Conseil **de la direction**
Demandez-vous : *« Quel serait le coût pour notre entreprise d'être 'hors ligne' pendant 3 jours ? »*, puis planifiez vos investissements en matière de cybersécurité en conséquence.

Assurance contre les cyber risques : les PME devraient-elles investir ?

- Permet de récupérer les **pertes financières** résultant d'un incident cybernétique, tel que :
  - Violations de données
  - Attaques par ransomware
  - Interruption d'activité
  - Frais juridiques et amendes réglementaires
  - Coûts liés à la gestion de la réputation et à la notification des clients
- Assistance dans le cadre de **la réponse aux incidents** et des enquêtes judiciaires
- Aide à **la conformité juridique** (par exemple, notification des autorités, des clients)

- **Les primes** varient en fonction de la taille de votre entreprise, de votre secteur d'activité et de votre niveau de cybersécurité.
- La plupart des assureurs exigent **des mesures de cybersécurité de base** (authentification multifactorielle, sauvegardes, formation).
- Les polices ne couvrent pas **les amendes NIS2 -** lisez attentivement les conditions générales.

Assurance contre les cyber risques : les PME devraient-elles investir ?

- Permet de récupérer les **pertes financières** résultant d'un incide
  - Violations de donné
  - Attaques par ransomware
  - Interruption d'activité
  - Frais juridiques et amendes réglementaires
  - Coûts liés à la gestion de la réputation et à la notification des clients
- Assistance dans le cadre de **la réponse aux incidents** et des enquêtes judiciaires
- Aide à **la conformité juridique** (par exemple, notification des autorités, des clients)

📌 L'assurance cyber ne remplace pas la prévention.

- **Les primes** varient en fonction de la taille de tre secteur d'activité et ersécurité.
- La plupart des assureurs exigent **des mesures de cybersécurité de base** (authentification multifactorielle, sauvegardes, formation).
- Toutes les polices ne couvrent pas **les amendes NIS2 -** lisez attentivement les conditions générales.

Exemple de budget pour la cybersécurité

Catégorie	Coût estimé (EUR)
1. Mesures techniques	
• Logiciel antivirus/anti-malware	600
• Pare-feu et protection réseau	800
• Solutions de sauvegarde des données	700
• Authentification multifactorielle (MFA)	400
2. Politique et conformité	
• Élaboration de politiques de sécurité	500
• Outils de conformité et consultation juridique	700
3. Formation et sensibilisation	
• Formation des employés à la cybersécurité	600
• Simulations et exercices de phishing	300
4. Réponse aux incidents	
• Élaboration d'un plan d'intervention en cas d'incident	1000
• Assistance informatique d'urgence / expertise judiciaire	
5. Cyberassurance	1200
• Prime annuelle	
6. Budget annuel total estimé	6800

Les catégories de base sont les suivantes :
mesures techniques,
formation,
conformité,
réponse aux incidents,
et assurance

Points clés à retenir pour la direction générale

Une cyberassurance peut vous protéger, mais vous devez tout de même mettre en place des mesures de sécurité.

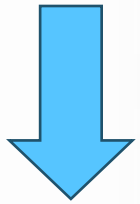
Les dépenses en matière de cybersécurité ne concernent pas le retour sur investissement, mais la réduction d'éventuelles pertes.

La budgétisation de la cybersécurité est une **décision stratégique**, et pas seulement une dépense informatique.

Sensibilisation des employés et culture de la sécurité

La sécurité avant tout pour les PME

- **La cause la plus fréquente des incidents cybernétiques est l'erreur humaine**
- Un simple clic sur un lien de phishing peut **mettre à mal l'ensemble de votre entreprise**.
- **Il est moins coûteux de** créer une culture de la sécurité **que de se remettre d'une cyberattaque**.



MENTALITÉ AXÉE SUR LA SÉCURITÉ
Une culture d'entreprise où **chacun se sent responsable de la cybersécurité, et** pas seulement l'équipe informatique

Le commencement

Faites de la sécurité une **priorité visible**

Parlez-en régulièrement

Faites y référence dans le processus d'intégration

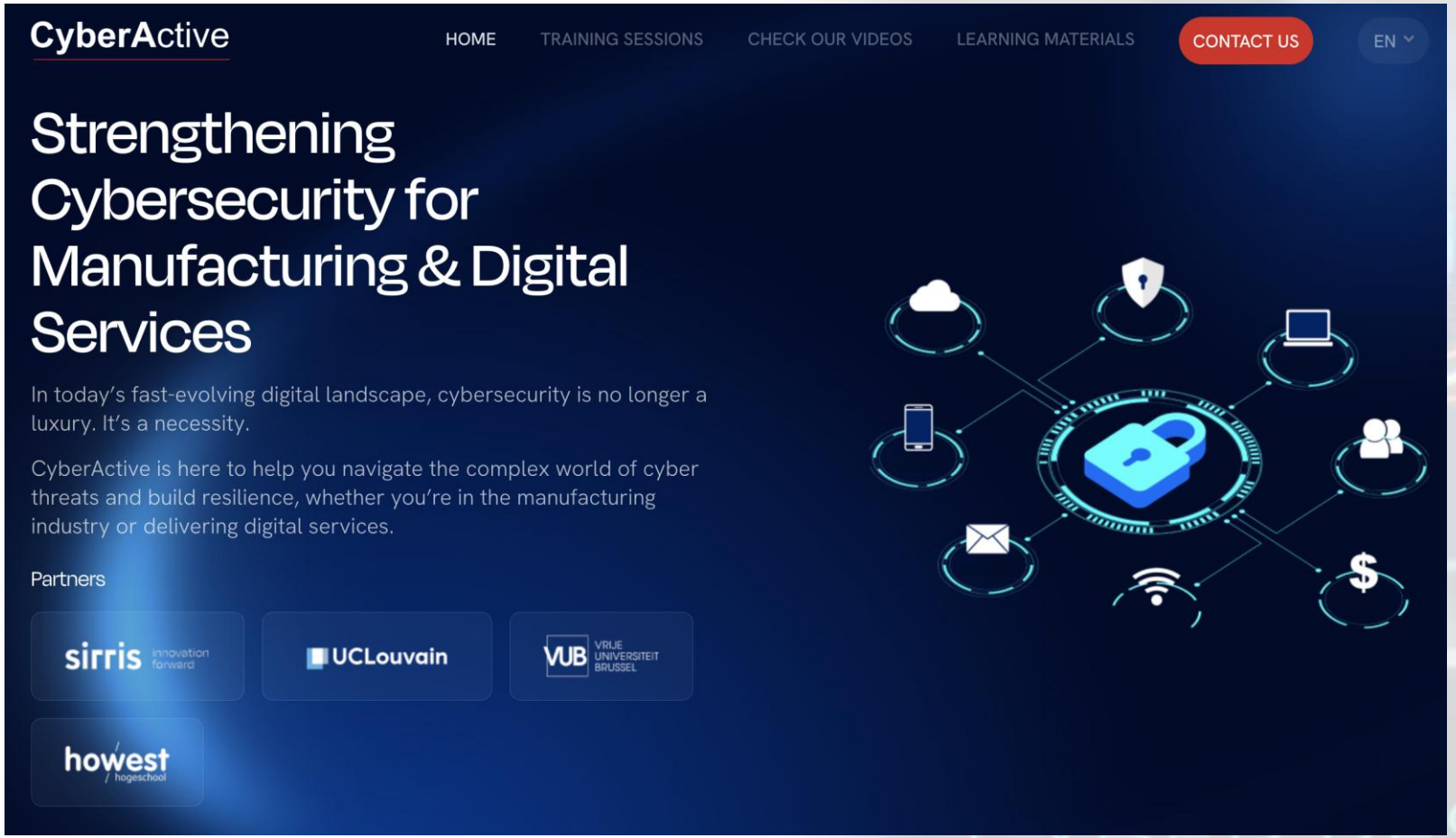
Montrez l'exemple

Mesures pratiques pour la direction

- Intégrez la cybersécurité dans **les réunions et les e-mails à l'échelle de l'entreprise**
- **Récompensez les bonnes pratiques en matière de sécurité** (par exemple, identification des e-mails de phishing)
- Veillez à ce que **les nouveaux employés reçoivent une formation en matière de sécurité** dans le cadre de leur intégration
- Exigez **une formation de base annuelle pour tout le personnel**
- Demandez au service informatique ou à des partenaires externes de fournir **chaque mois de brefs conseils ou des vidéos**

🔒 Lorsque la direction montre qu'elle se soucie de la sécurité, **les employés commencent eux aussi à s'y intéresser**.

Nous vous accompagnons avec des formations, des vidéos et du matériel pédagogique !



Bonnes pratiques pour le personnel

Hameçonnage

Faux e-mails ou messages conçus pour **inciter les employés** à cliquer sur des liens dangereux ou à partager leurs mots de passe.

Meilleure pratique : apprenez à vos employés à **passer la souris sur les liens**, à vérifier les adresses des expéditeurs et **à signaler les messages suspects**.

Ingénierie sociale

Tactiques manipulatrices dans lesquelles les attaquants **se font passer pour une personne de confiance** (par exemple, un technicien informatique ou un fournisseur).

Meilleure pratique : vérifiez l'identité avant de partager des informations. Établissez des règles claires : **« Ne partagez jamais vos mots de passe par e-mail ou par téléphone. »**

Authentification multifactorielle (MFA)

Un outil simple mais puissant : il nécessite un mot de passe **et une deuxième étape** (par exemple, un code SMS, une confirmation via une application).

Meilleure pratique : appliquez l'authentification multifactorielle pour **les e-mails, les plateformes cloud et les comptes administrateur**. Elle **bloque 99 % des attaques visant à compromettre les comptes**.

Points clés à retenir pour la direction générale

La culture de la cybersécurité commence par l'impulsion du management

Investissez dans la formation des employés

Utilisez des outils simples tels que l'authentification multifactorielle (MFA) et la formation **de sensibilisation**

Wrap-up

Liste de contrôle de conformité NIS2 pour les dirigeants

Comprenez vos obligations légales

- Sachez si votre PME est considérée comme une entité « importante » ou « essentielle ».
- Informez-vous sur les règles de déclaration et les amendes potentielles.

Nommez un responsable de la sécurité

- Désignez une personne (interne ou externe) chargée de superviser la stratégie de cybersécurité.

Réalisez une évaluation des risques

- Identifiez vos actifs critiques et vos principales vulnérabilités.
- Documentez-les (exigence de la directive NIS2)

Mettre en place des procédures de signalement des incidents

- Assurez-vous que votre équipe est en mesure de détecter et de signaler les incidents cybernétiques majeurs dans les 24 heures.

Sécurisez votre chaîne d'approvisionnement

- Interrogez vos principaux fournisseurs sur leurs mesures de cybersécurité. Intégrez-les dans vos contrats.

Formez votre personnel

- Organisez des formations de sensibilisation, en particulier sur le phishing, l'ingénierie sociale et l'authentification multifactorielle (MFA).

Obtenez l'engagement du conseil d'administration

- Examinez les cyber risques idéalement tous les trimestres. Intégrez-les aux discussions de la direction.

Construisez et conservez la documentation

- Conservez des traces écrites de votre stratégie de cybersécurité, de vos contrôles, de vos formations et de vos mesures de réponse aux incidents.

Collaboration avec les équipes informatiques et juridiques

Avec l'équipe informatique :

- S'accorder sur **les actifs critiques** et les priorités en matière de sécurité.
- Demander des **explications claires** (ne pas se contenter du jargon).
- Les impliquer dans **les exercices de réponse aux incidents** et la documentation relative à la conformité.

Avec l'équipe juridique :

- Examiner l'impact de la directive NIS2 sur votre entreprise.
- Clarifier **les obligations en matière de signalement des incidents**, les contrats avec les fournisseurs et la responsabilité du conseil d'administration.
- S'assurer que votre stratégie de protection des données est conforme au **RGPD et** à la **directive NIS2**.

Points clés à retenir pour les CEO

Commencez modestement et améliorez-vous progressivement

Utilisez des outils pratiques et définissez clairement les rôles

Collaborez avec les services informatiques et juridiques

Annexe : NIS2 & CyFun – comment démarrer

Guide en 6 étapes pour NIS2

https://atwork.safeonweb.be/tools-resources/nis-2-quickstart-guide

Suis-je concerné par la norme NIS2 ?

Utilisez l'outil de détermination de la portée en ligne : https://atwork.safeonweb.be/sites/default/files/2024-07/NIS2%20scope%20assessment.v1.0.1.xlsx

Dans le champ d'application : entités NIS2

Suivez le guide de démarrage rapide : inscrivez-vous, déclarez, déterminez votre niveau, planifiez la formation, mettez en œuvre les mesures.

Dans la chaîne d'approvisionnement d'une entité NIS2

Mettre en œuvre au moins le niveau BASIC

Attention au CRA à partir de 2025

Outil de cadrage NIS2

https://atwork.safeonweb.be/sites/default/files/2024-07/NIS2%20scope%20assessment.v1.0.1.xlsx

Pour télécharger, rendez-vous ici : https://atwork.safeonweb.be/fr/tools-resources/guide-de-demarrage-rapide-avec-nis2

1. Am I affected by NIS2?

A. In scope: NIS2 entities

Use our scope test tool to determine whether or not your organisation falls within the scope of the Belgian NIS2 Law.

Download the scoping tool

CENTRE FOR CYBERSECURITY BELGIUM

Scope Assessment

The following questions aim to determine if your organisation may potentially be in scope of the Belgian NIS2 legislation. Depending on its size and the service provided, your organisation may be considered as an essential or important entity.

More information about the NIS2 law can be found here

A. Organisation size ("size-cap") (i) Further information

Please select the size of your organisation before continuing.

These thresholds are calculated on the basis of the figures for the entire legal entity (including all its activities, even outside of the EU), proportionately consolidated with the figures from its partner or linked enterprises.
For more details on the method for calculating these thresholds, see the annex I of Commission Recommendation 2003/361/CE of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, the guide released by the European Commission, or its online tool (linked below).

Link to Commission Recommandation 2003/361/EC
Link to the "User guide on the SME definition" from the European Commission
Link to the SME self-assessment tool from the European Commission

Select your staff headcount range (in full-time equivalents - FTE):	50 - 249 FTE
Select your turnover range:	< 10 million € annual turnover
Select your balance sheet total:	< 10 million € annual balance sheet total

Your organisation's size : Medium-sized Enterprise

B. Sectors and service provided

Please select at least one sector, or the field 'None of the above' if your organisation does not correspond to any of the sectors, before you can continue.

5 étapes pour se conformer à la norme NIS2 pour les entités NIS2

https://atwork.safeonweb.be/tools-resources/nis-2-quickstart-guide

ÉTAPE 1 : INSCRIVEZ-VOUS

- Inscrivez-vous sur Safeonweb@Work : https://atwork.safeonweb.be/register-my-organisation
- Numérique -- avant le 18 décembre 2024.
- Autres - avant le 18 mars 2025

ÉTAPE 2 : SIGNALER

- Signalez tous les incidents importants dans les 24 heures
- Depuis le 18 octobre 2024

ÉTAPE 3 : DÉTERMINER

- **Déterminez votre niveau CyberFundamentals (CyFun®)**
- https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework/

ÉTAPE 4 : PLANIFIER

- **Planifiez une formation en cybersécurité pour** les conseils d'administration et les dirigeants, idéalement avant avril 2025

ÉTAPE 5 : METTRE EN ŒUVRE

- **Mettez en œuvre les mesures de sécurité**
- Réalisez une analyse des lacunes à l'aide de l'outil d'auto-évaluation CyFun®
- Mettre en œuvre les mesures requises.
- Mettez à jour votre auto-évaluation

Quelles sont les amendes en cas de non-conformité ?

NIS 2 Improvements & Novelties

	Increase of sectoral scope	Hardening expectations for cyber resilience and incident response	Expansion of sanctions	Enhancement of EU cyber crisis cooperation
NIS 1	Several sectors of Operators of Essential Services (OSE) & Digital Service Providers (DSP) **30 types of entities**	Risk based approach, with no obligation of prior compliance to the directive	Sanctions TBD by Member States	
NIS 2	Sectors of high criticality and critical sectors **67 types of entities** **Inclusion of SMEs under certain criteria** **Inclusion of Supply Chain**	**Ex ante audits by authorities** **Incident notification in 24h and a more detailed report in 72h** **Clear responsibility matrix across all entities and supply chain** **Supply chain compliance** **Risk management TOMs covering multiple areas**	10/7 millions € or 2/1,4% of the turnover **Suspension of certifications or pending authorizations** **Criminal sanctions** **Temporary ban on management positions**	Creation of the Cyber Crisis Liaison Organisation Network - **EU-CyCLONe**

CYBER RESILIENCE

En Belgique - CYBERFUNDAMENTALS

Small

Le niveau de départ **Small** permet à une organisation de procéder à une première évaluation. Il est destiné aux micro-organisations ou aux organisations ayant des connaissances techniques limitées.

01/03/2023 · pdf

Download

Basic

Le niveau d'assurance **Basic** contient les mesures de sécurité de l'information standard pour toutes les entreprises. Ceux-ci fournissent une valeur de sécurité efficace avec des technologies et des processus qui sont généralement déjà disponibles. Lorsque cela se justifie, les mesures sont adaptées et affinées.

01/03/2023 · pdf

Download

Important

Le niveau d'assurance **Important** est conçu pour minimiser les risques de cyberattaques ciblées par des acteurs disposant de compétences et de ressources communes, en plus des risques de cybersécurité connus.

01/03/2023 · pdf

Download

Essentiel

Le niveau d'assurance **Essentiel** va plus loin et est conçu pour faire face au risque de cyberattaques avancées par des acteurs disposant de compétences et de ressources étendues.

01/03/2023 · pdf

Download

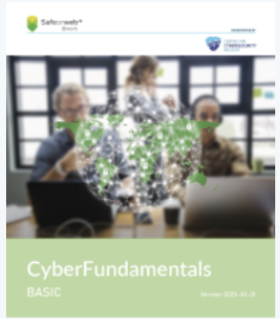
Niveaux SMALL et BASIC de CyFun

- SMALL s'applique aux particuliers et aux micro-entreprises qui n'ont aucun client dans le champ d'application de NIS2

Small

The starting level Small allows an organisation to make an initial assessment. It is intended for **micro-organisations or organisations with limited technical knowledge.**

- BASIC – pour le reste des entreprises non directement sujettes à NIS2



Basic

The assurance level Basic contains the **standard information security measures for all enterprises**. These provide an effective security value with technology and processes that are generally already available. Where justified, the measures are tailored and refined.

Code couleur et cadre NIST

- Identifier
  - Identifiez les cybermenaces importantes qui pèsent sur vos actifs les plus précieux. En effet, vous ne pouvez pas protéger ce dont vous ignorez l'existence. Cette fonction aide à développer une compréhension organisationnelle de la manière de gérer les risques liés à la cybersécurité concernant les systèmes, les personnes, les actifs, les données et les capacités.
- Protéger
  - La fonction de protection se concentre sur le développement et la mise en œuvre des mesures de protection nécessaires pour atténuer ou contenir un risque cybernétique.
- Détecter
  - L'objectif de la fonction « Détecter » est d'assurer la détection rapide des incidents de cybersécurité.
- Réagir
  - La fonction Réagir concerne les contrôles qui permettent de réagir aux incidents de cybersécurité. La fonction Réagir soutient la capacité à contenir l'impact d'un incident de cybersécurité potentiel.
- Récupération
  - La fonction Récupérer se concentre sur les mesures de protection qui permettent de maintenir la résilience et de restaurer les services qui ont été affectés par un incident de cybersécurité.

POUVEZ-VOUS DONNER DES EXEMPLES DE CES FONCTIONS ?

Niveau SMALL (mesures préliminaires)

Protégez toutes les connexions avec l'authentification multifactorielle (MFA)

Installez immédiatement toutes les mises à jour de sécurité

Installez un antivirus

Sécurisez votre réseau -> pare-feu, Wi-Fi, accès à distance

Sauvegardez vos données -> régulièrement, hors ligne

Droits d'administrateur -> ne les utilisez pas sans raison, protégez-les avec l'authentification multifactorielle

Limitez l'accès physique, Sachez qui contacter en cas d'incident

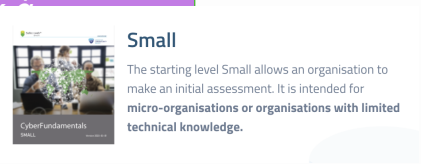
Conformité – niveau d'entrée

- Tout le monde respecte-t-il les règles ?
- Qu'est-ce qui manque ?

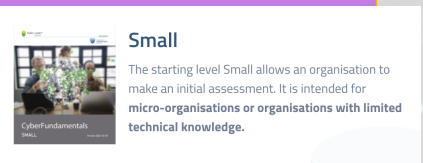
13 mesures clés du niveau BASIC : sécurité du réseau

Les réseaux de l'organisation doivent être sécurisés lorsqu'ils sont accessibles à distance, notamment grâce à l'authentification multifactorielle (MFA).

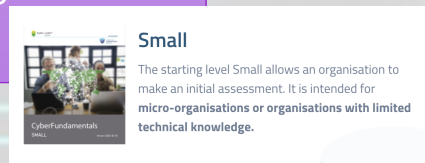
C'est-à-dire 2FA pour les e-mails, les bureaux à distance et les VP



Des pare-feu doivent être installés et activés sur tous les réseaux de l'organisation.



Le cas échéant, l'intégrité du réseau des systèmes critiques de l'organisation doit être protégée par la segmentation et la ségrégation du réseau.
C'est-à-dire créer des VLAN et contrôler le trafic



13 mesures clés du niveau BASIC : comptes utilisateurs

L'accès des employés aux données et aux informations doit être limité aux systèmes et aux informations spécifiques dont ils ont besoin pour faire leur travail (principe du moindre privilège).

C'est-à-dire que tout le monde n'a pas accès à tout, limiter le nombre de connexions.

Personne ne doit disposer de privilèges d'administrateur pour les tâches quotidiennes.

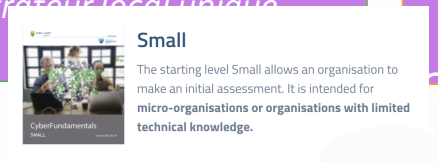
C'est-à-dire séparer le compte administrateur, créer un compte administrateur local unique

Les autorisations d'accès des utilisateurs aux systèmes de l'organisation doivent être définies et gérées.

C'est-à-dire vérifier les comptes Active Directory, utiliser des comptes distincts.

Il convient d'identifier les personnes qui doivent avoir accès aux informations et technologies critiques de l'organisation, ainsi que les moyens d'y accéder.

C'est-à-dire code, mot de passe, clé, privilège



13 mesures clés du niveau BASIC : identifiants et sauvegardes

Les identités et les identifiants des appareils et des utilisateurs autorisés doivent être gérés.

C'est-à-dire une politique en matière de mots de passe

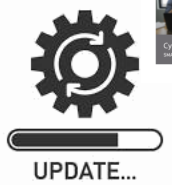
Les sauvegardes des données critiques de l'organisation doivent être effectuées et stockées sur un système différent de celui sur lequel se trouvent les données originales.

C'est-à-dire sauvegarde régulière, sauvegarde hors ligne

13 mesures clés du niveau BASIC : sécurité des logiciels

Les correctifs et les mises à jour de sécurité pour les systèmes d'exploitation et les composants critiques du système doivent être installés.

C'est-à-dire choisir des logiciels pris en charge par le fournisseur, installer les correctifs immédiatement



Des programmes antivirus, anti-logiciels espions et autres programmes anti-malware doivent être installés et mis à jour.

C'est-à-dire au bureau et à domicile.

13 mesures clés du niveau BASIC : « logs »

Les journaux doivent être conservés, documentés et examinés.

C'est-à-dire enregistrer les journaux.

La fonctionnalité d'enregistrement des activités du matériel ou des logiciels de protection/détection (par exemple, pare-feu, antivirus) doit être activée, sauvegardée et examinée.

C'est-à-dire examiner les journaux.

Références

- https://ccb.belgium.be/en/nis-2-directive-what-does-it-mean-my-organization
- Les trois piliers du NIS2 et portée (diapositives 6 et 7) : https://blog.cybersecuritycoalition.be/wp-content/uploads/20221205_NIS2-Directive_CCB.pdf
- Montants et dates exacts (diapositives 8 et 9) : https://www.devoteam.com/expert-view/ensure-compliance-with-the-sri2-nis2/
- Cyberfundamentals (diapositive 10) : https://atwork.safeonweb.be/fr/tools-resources/cyberfundamentals-framework

Glossaire

Sauvegarde

- Création d'une copie des données de votre système que vous utilisez pour la récupération en cas de perte ou de corruption de vos données d'origine

Cyberhygiène

- Mesures que les utilisateurs d'ordinateurs et d'autres appareils peuvent prendre pour améliorer leur sécurité en ligne et maintenir la santé du système.

Incident de cybersécurité

- Tout événement lié à la compromission de données ou d'opérations commerciales résultant de mesures de sécurité manquantes ou défaillantes.

Identifiant

- Ensemble de données de connexion qui vérifient l'identité d'un utilisateur et lui accordent l'accès à un système ou un service particulier, c'est-à-dire un nom d'utilisateur et un mot de passe.

NIS2 :

- La directive NIS2 (sécurité des réseaux et de l'information) est la législation européenne en matière de cybersécurité. Elle prévoit des mesures juridiques visant à renforcer le niveau global de cybersécurité dans l'UE.

VLAN :

- Moyen de séparer logiquement un groupe d'ordinateurs en un réseau distinct. Ceux-ci ne communiqueront entre eux et non avec d'autres appareils connectés au même réseau physique.

Chaîne d'approvisionnement :

- réseau de personnes et d'entités impliquées dans la création d'un produit et sa livraison au consommateur.

Sécurité de la chaîne d'approvisionnement :

- partie de la gestion de la chaîne d'approvisionnement qui se concentre sur la gestion des risques liés aux fournisseurs externes, aux vendeurs, à la logistique et au transport.

Glossaire

CSIRT :

- Un élément essentiel de la stratégie de cybersécurité de toute organisation. En cas de cyberattaque, une équipe d'intervention efficace peut rapidement détecter, contenir et atténuer les dommages, minimisant ainsi l'impact sur l'entreprise.

Contrôle d'intégrité :

- méthodes visant à garantir que les données sont exactes, réelles et protégées contre toute modification ou destruction non autorisée par des utilisateurs.

Analyse des vulnérabilités :

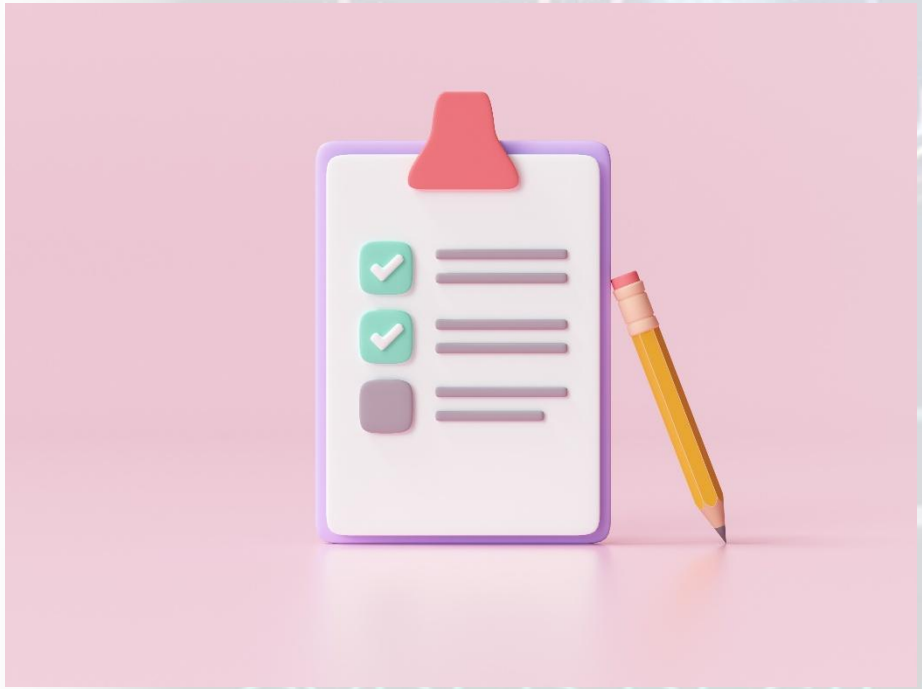
- processus d'identification des faiblesses et des failles de sécurité dans les systèmes et les logiciels qui y sont exécutés.

Malware :

- logiciel spécialement conçu pour perturber, endommager ou obtenir un accès non autorisé à un système informatique.

Evaluation de cette session
Merci de prendre 2 minutes pour compléter le formulaire

https://forms.cloud.microsoft/e/MZC5QqCbae



CyberActive