FANC AFCN

FEDERAAL AGENTSCHAP VOOR
NUCLEAIRE CONTROLE

AGENCE FÉDÉRALE DE
CONTRÔLE NUCLÉAIRE

Agenda

- Mot d’introduction
- Travail antérieur – Objectif de la consultation – Questions posées lors de la consultation de 2023
- Cadre juridique
- Présentation du projet d’AR cybersécurité modifié
- Présentation par le CCB
- Way forward
- Varia

Pourquoi MAINTENANT?

- Transposition NIS2, elle distingue
  - Services essentiels
  - Services importants
- Modification des compétences du CCB:
  - Propre service d'inspection
  - Font appel à des "autorités sectorielles" – l'AFCN en est un pour le secteur nucléaire / radiologique et pour les infrastructures critiques
  - Le CCB a été désigné comme l'Autorité nationale de certification en matière de cybersécurité

Services essentiëls

- Energy
- Banking / Financial Markets and Infrastructure
- Health
- Digital infrastructure
- Drinking water
- Space
- Transport
- Wastewater & water management

Services importants

- Digital providers
- Food production, processing and distribution
- Manufacture production and distribution of chemicals
- Manufacturing
- Postal and courier service
- Waste management

Pourquoi MAINTENANT?

- L'AFCN souhaite s'aligner le plus possible sur le cadre réglementaire existant
- L’AFCN souhaite aligner le secteur nucléaire et radiologique sur d’autres secteurs
- La Cybersécurité Nucléaire traite surtout des conséquences nucléaires ou radiologiques, conformément à notre mission
- Le NIS s'intéresse principalement à la disponibilité et à l'impact financier, économique et sanitaire.

Pourquoi MAINTENANT?

- Et les pays environnants? Discussion au sein de l'ENSRA:
  - S'aligner sur le NIS2
  - Le secteur nucléaire à exclure du NIS
  - Tenir compte de l'évolution rapide du secteur – aligner les mesures sur cette évolution rapide
- Pour cette raison, s'aligner sur le NIS2 en utilisant les Cyberfundamentals et les services d'audit certifiés

Situation

- Directive NIS1: 06/07/2016
- Modification de la loi 05/04/2019: ajout de compétences en matière de cybersécurité nucléaire
- Première consultation des parties prenantes en décembre 2019: présentation générale de la cybersécurité
- Réunion SPOCs cybersécurité en mai 2021 (en ligne)
- Réunion CCB-NCCN-AFCN en juin 2021
- Directive NIS2 du 14/12/2022, à transposer pour le 17/10/2024 (NIS2-richtlijn van 14/12/2022, (exclut le secteur nucléaire)
- Le CCB est désigné comme l'Autorité nationale de certification en matière de cybersécurité et est responsable de la transposition de la directive NIS
- Deuxième consultation des parties prenantes le 15 juin 2023 (présentation des principes du projet d'AR)

Objectif de la consultation

- Réunion d'information
  - FANC
  - CCB
- Exposé des modifications
- Clarification du cadre juridique
- Présentation sur le fond du Projet AR Cyber
- Consultation formelle des parties prenantes afin de commencer le processus de feedback

Travail antérieur (1)

- Nombre de questions supplémentaires
  - 14 questions / 3 exploitants
  - Topics
    - IT vs OT
    - Certification du Délégué à la Cybersécurité
    - Impact financier vs impact sureté
    - Sous-traitance / chaîne d'approvisionnement
    - Zones physiques vs zones virtuelles
    - Gestion des versions cyberfundamentals
    - Les fondamentaux sont orientés IT
    - Législation cyber des pays environnants

Travail antérieur (2)

- Classification des catégories cyber liées à un niveau concret de sécurité où le lien est mis avec les Cyber Fundamentals du CCB.
- Exemption pour les établissements couverts par la directive NIS2.
- Procédure d'agrément (Chapitre VII)
- Mesures transitoires (Chapitre VIII)
    - Dépend de la catégorie cyber qui est d'application
    - Délai

Loi AFCN

Base = Loi AFCN (article 17sexies) du 05/04/2019

- Répartition en catégories sur base du risque cyber associé
- Les mesures de cybersécurité nucléaire nécessaires et proportionnées pour les catégories les plus hautes de réseaux et de système d'information:
  - La gestion des risques cyber
  - La prévention des incidents cyber et/ou l'impact de ceux-ci
  - La notification à l'Agence et aux autorités désignées par le Roi les cyber-incidents ayant un impact significatif.
- Procédure d'agrément pour les mesures de cybersécurité nucléaires

Loi AFCN

- Échange sur la notification des risques cyber et des incidents cyber auxquels les exploitants sont ou peuvent être confrontés
- Les principes des mesures de cybersécurité nucléaire concernant la gestion prudente pour les catégories les plus basses des réseaux et systèmes d'information

Loi-AFCN

- Informer et sensibiliser les utilisateurs de ces réseaux et systèmes d'information
- Collaboration avec le CCB et le NCCN
- Premier AR avec entrée en vigueur + désignation des autorités compétentes:
  - Prêt pour l’avis du CCB et du NCCN
  - Lancer la procédure d’approbation officielle

Q&A

AFCN
AGENCE FÉDÉRALE DE CONTRÔLE NUCLÉAIRE

AFCN
AGENCE FÉDÉRALE DE CONTRÔLE NUCLÉAIRE

Projet d'AR

Projet d'AR – Champ d'application

Cet arrêté s'applique aux réseaux et systèmes informatiques des:

1° installations nucléaires;

2° établissements où des matières radioactives sont produites, fabriquées, détenues ou utilisées;

- Entrée en vigueur par étape, d'abord les installations nucléaires, ensuite les autres installations
- Si l'exploitant est déjà soumis au NIS2
  - Pas de mesures supplémentaires

Projet d'AR Cyber: catégories

AFCN
AGENCE FÉDÉRALE DE CONTRÔLE NUCLÉAIRE

On distingue 5 catégories:

Les réseaux et systèmes d'information qui supervisent et dirigent les processus qui permettent directement ou indirectement la gestion, le contrôle ou la sécurisation des **matières nucléaires** ET:

- 1re Catégorie "Cyber-1"
  - qui se situent dans la zone très hautement protégée, la zone hautement protégée, la zone protégée et la zone vitale
- 2e Catégorie "Cyber-2"
  - qui se situent dans la zone sécurisée ou en dehors d'une zone sécurisée

Projet d'AR Cyber: catégories

Les réseaux et systèmes d'information qui assurent la supervision et le pilotage des processus qui permettent, assurent ou appuient directement ou indirectement, la gestion, le contrôle ou la sécurisation des **substances radioactives** et

- 3e Catégorie "Cyber-3"
  - qui se situent dans un espace sécurisé du niveau de sécurité A au sens de l'AR – RAMAS;
- 4e Catégorie " Cyber-4"
  - qui se situent dans un espace sécurisé du niveau de sécurité B ou C au sens de l'AR - RAMAS;

Projet d’AR Cyber: catégories

- 5e Catégorie “Cyber-5”
  - réseaux et systèmes d'information qui assurent la supervision et le pilotage des processus qui permettent, assurent ou appuient directement ou indirectement, la gestion, le contrôle ou la sécurisation des substances radioactives qui appartiennent aux catégories 4 ou 5 au sens de l’AR - RAMAS et qui se situent dans l’établissement;

Projet d'AR Cyber: catégories

AFCN
AGENCE FÉDÉRALE DE CONTRÔLE NUCLÉAIRE

D'application sur toutes les catégories:

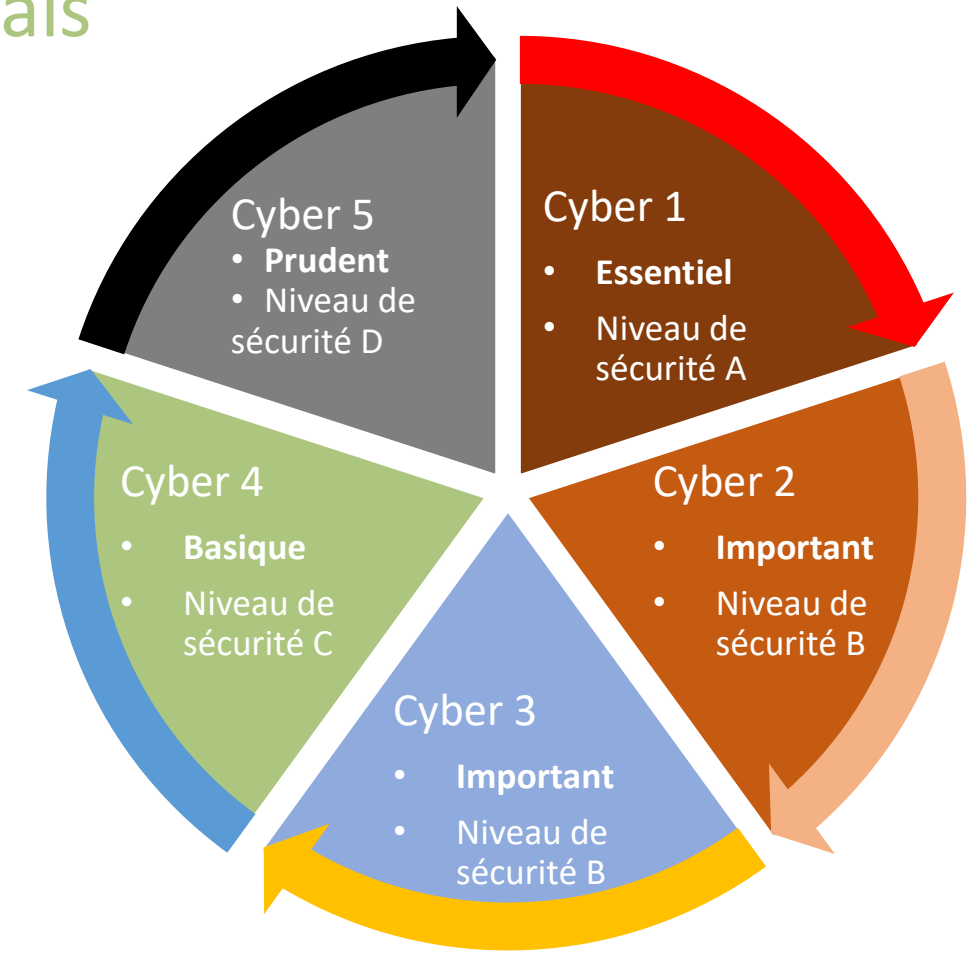
- Les réseaux et systèmes d'informations qui communiquent ou sont reliés d'une quelconque manière avec les zones de sécurité, les espaces sécurisés ou les systèmes

Projet d'AR Cyber: catégories & niveaux de sécurité & cyberfundamentals

AFCN
AGENCE FÉDÉRALE DE CONTRÔLE NUCLÉAIRE

Interconnexion

- Catégories
- Niveaux de sécurité
- Cadre = Cyber fundamentals CCB (*à l'exception de la gestion prudente)



Projet d'AR Cyber : Politique en matière de cybersécurité

- Mesures techniques et organisationnelles appropriées
- Politique de cybersécurité documentée
- À approuver par l'AFCN
- À examiner à des intervalles déterminées par un auditeur accrédité
- L'Agence peut publier des règlements techniques et des recommandations supplémentaires

Projet d'AR Cyber: nommer un Délégué à la Cybersécurité

AFCN
AGENCE FÉDÉRALE DE CONTRÔLE NUCLÉAIRE

- Il faut désigner un Délégué à la Cybersécurité
  - Externe / interne
- La désignation doit être approuvée par l'Agence
  - L'exploitant doit pour ce faire transmettre les données d'identification, la formation et le niveau de formation de la personne
- Désignation du Délégué à la Cybersécurité sur base de:
  - Certificats, attestations, formations professionnelles et/ou diplômes et/ou expérience
- Les connaissances et l'expertise doivent être maintenues à jour grâce à la formation continue.

Projet AR Cyber : rôle du Délégué à la Cybersécurité

AFCN
AGENCE FÉDÉRALE DE CONTRÔLE NUCLÉAIRE

- Doit être étroitement impliqué dans la politique
- Doit être clairement soutenu, notamment en lui fournissant des ressources
- Rend compte directement au dirigeant de l'exploitant
- Informe et conseille l'exploitant et ses employés sur toutes les questions et obligations en matière de cybersécurité nucléaire
- Doit être consulté lors d’incidents et autres décisions importantes

Projet AR Cyber : rôle du Délégué à la Cybersécurité

AFCN
AGENCE FÉDÉRALE DE CONTRÔLE NUCLÉAIRE

- Élabore une politique de sécurité documentée
- Supervise la mise en œuvre et l'observation de celle-ci
- Est la personne de contact pour tout ce qui concerne la cybersécurité nucléaire
- Assure la sensibilisation et la formation de l'ensemble du personnel
- Prépare un rapport annuel et le tient à la disposition de l'Agence à des fins de consultation

Projet d'AR Cyber: Contenu de la politique de cybersécurité

AFCN
AGENCE FÉDÉRALE DE CONTRÔLE NUCLÉAIRE

La politique de cybersécurité est une déclaration des responsables sur :

- Le fonctionnement de la cybersécurité nucléaire
- Cadre des risques cyber nucléaire
- Développement des politiques de cybersécurité nucléaire
- Cybersécurité nucléaire dans le cadre de la conduite du projet
- Formation et sensibilisation
- Détermination des lignes hiérarchiques
- Rôles et responsabilités du DCS
- Conformément à la législation belge
- Moyens budgétaires et humains
- Evalue la politique de cybersécurité nucléaire et l'ajuste au besoin

Projet d'AR Cyber: Exemple contenu de la politique cybersécurité

Le fonctionnement de la cybersécurité au sein de "l'exploitant"

- La cybersécurité au sein de l'organisation est cruciale afin de soutenir la croissance et la continuité de "l'exploitant"
- La cybersécurité est un processus transversal au sein de "l'exploitant"
- La cybersécurité comporte l'intégrité, la disponibilité et la confidentialité mais aussi la limitation des conséquences nucléaires ou radiologiques, conformément à la mission de l'AFCN
- AR cybersécurité nucléaire

Projet d’AR Cyber : contenu du rapport annuel

- Un aperçu général de la situation en matière de cybersécurité, des mesures prises dans ce domaine, de l'évolution au cours de l'année écoulée et des objectifs qui restent à atteindre
- Une sommaire des avis transmis par le Délégué à la Cybersécurité au dirigeant de l'exploitant et des suites qui leur ont été données.
- Un aperçu du travail effectué par le Délégué à la Cybersécurité

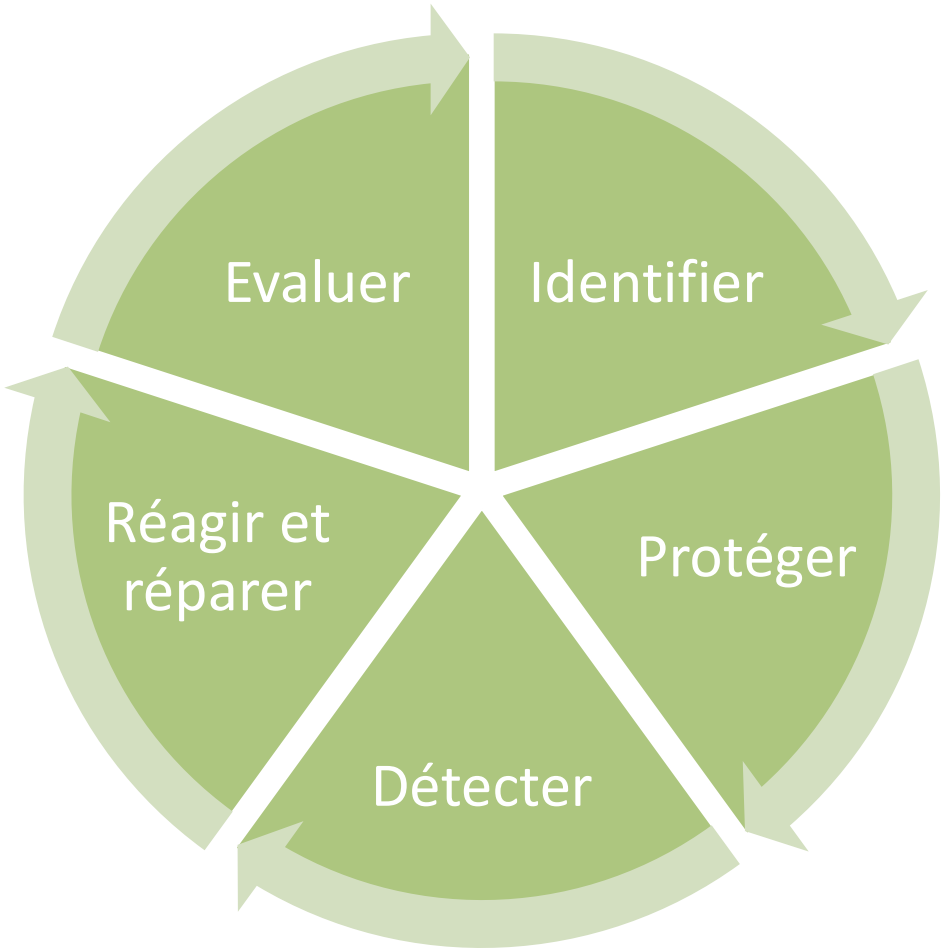
Projet AR Cyber: contenu du rapport annuel

AFCN
AGENCE FÉDÉRALE DE CONTRÔLE NUCLÉAIRE

- Un aperçu des initiatives de sensibilisation prises et des campagnes menées afin de promouvoir la cybersécurité
- Un aperçu de toutes les formations suivies et de celles qu'il est prévu de suivre
- Un aperçu des audits internes et externes réalisés en matière de cybersécurité et de leur suivi (plan d'action)

Mesures de cybersécurité nucléaire

AFCN
AGENCE FÉDÉRALE DE CONTRÔLE NUCLÉAIRE



Projet d'AR Cyber: mesures en matière de cybersécurité

AFCN
AGENCE FÉDÉRALE DE CONTRÔLE NUCLÉAIRE

Identificeren (IT/OT/IOT/fournisseurs)

- Inventaire des actifs (matériel informatique, logiciels, information, identités…)
- Classifier les actifs, prioriser, identifier le caractère critique des actifs
- Rôles et responsabilités
- Identification et gestion des risques
- Identification des risques de la chaîne d'approvisionnement
- Communiquer et mesurer la politique de sécurité
- Identifier les vulnérabilités et y remédier
- Documenter et évaluer

Projet d'AR Cyber: mesures en matière de cybersécurité

- Protéger
  - Gestion des accès physiques et virtuels
  - Déterminer les niveaux d'authentification (systèmes, personnes, applications,…)
  - Protection adéquate des réseaux et des applications (pare-feu, VLAN, pare-feu pour applications, ...)
  - Formations prévues dans le domaine de la cybersécurité
  - Encryption de données sensibles au repos et en transit
  - Enregistrement fourni sur les applications, les systèmes,...

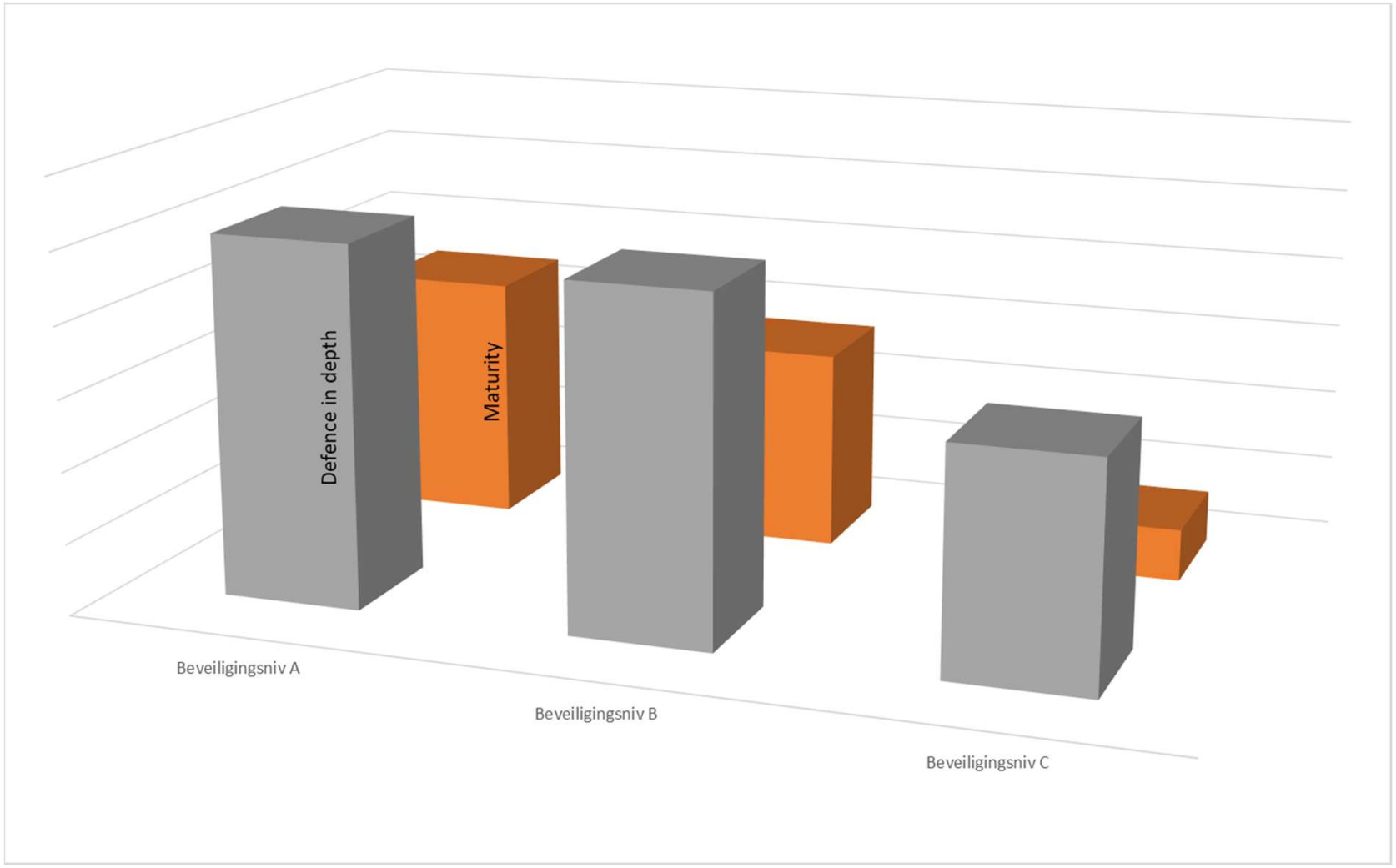
Projet d'AR Cyber: mesures en matière de cybersécurité

- Détecter
  - Constater les incidents cyber
  - Collecter des informations de connection, reconnaissance de tendances,…
- Réagir et réparer
  - Établir des processus et des critères pour répondre aux cyber-incidents en temps utile
  - Signaler des incidents
  - Analyser les incidents
  - Limiter les conséquences des incidents
  - rétablissement les incidents

Projet d'AR Cyber: mesures en matière de cybersécurité

- Evaluer
  - Evaluer périodiquement les politiques de cybersécurité
  - Organiser des exercices avec des attaques et des scénarios réels et ajuster la réponse
  - Evaluer périodiquement les renseignements sur les menaces

Niveau de sécurité vs defence in depth



Q&A

AFCN
AGENCE FÉDÉRALE DE CONTRÔLE NUCLÉAIRE

Projet d'AR Cyber Procédure d'agrément

L'exposé des motifs de la loi indique en ce qui concerne la procédure d'agrément:

Il conviendrait que cette procédure prenne en compte les évolutions rapides des techniques, par exemple en assurant surtout une obligation de maintenir des niveaux de sécurité plutôt qu'en se focalisant sur la stricte conformité à un dossier de demande d'agrément qui s'avérerait vite obsolète.

Projet d’AR Cyber Procédure d’agrément

AFCN
AGENCE FÉDÉRALE DE CONTRÔLE NUCLÉAIRE

- Réaction rapide à l'évolution technique
- Agrément de la **politique cybersécurité**
- Pour les nouveaux exploitants: couplée à:
  - Soumission demande d’agrément avec le plan de sécurité RAMAS
  - Soumission demande d’agrément avec le système de sécurité physique
- Pour les exploitants existants: mesures transitoires

Mesures transitoires

- Cyber-4: après 24 mois, élaboration de la politique, si implémentée = agréé (impact NIS 2)

- Cyber-3 et Cyber-2 et Cyber-1:
  - Introduire la demande d'agrément après 18 mois (politique)
  - 6 mois après l'introduction: approbation de la politique par l'AFCN
  - Maximum 3 ans pour implémentation totale
  - Suivi de l'implémentation via le rapport annuel du délégué et les audits internes/externes

Entrée en vigueur

- Par étapes
- Les exploitants nucléaires d’abord: Cyber-1 et Cyber-2
- Plus tard, les autres: dépendant de l’implémentation de la NIS 2

Way forward

- Semaine prochaine: publication des projets de texte sur le site web de l'AFCN
  - Projet AR
  - Projet rapport au Roi
- Formulaire de feedback formel
- Feedback au plus tard le 31/05/2024 à l'adresse cyber@fanc.fgov.be
- Traitement des commentaires
- Feedback (individuel et global)
- Terminer le projet d'AR Cyber avant fin 2024
- Processus d'approbation formelle

Presentation CCB

Q&A

AFCN
AGENCE FÉDÉRALE DE CONTRÔLE NUCLÉAIRE

AFCN
AGENCE FÉDÉRALE DE CONTRÔLE NUCLÉAIRE

Merci !