Formation:
Introduction à la Directive NIS2

Public cible
Responsables IT, cadres, et décideurs des villes et communes

Durée
8 heures (dont 2 heures d'exercice pratique sur le cyber range)

Effectif
De 6 à 15 participants par session

Lieu
Centre d'Excellence en Cybersécurité de Nexova, Rue des Etoiles 140, 6890 Libin (Belgique)

Prochaine date
14 mars 2025

Objectif :

Comprendre les exigences de la directive NIS2 et leur application pratique pour les administrations locales.

Programme:

1. La formation débute par une présentation générale de la directive NIS 2. Le contexte, les objectifs et les raisons de son introduction sont expliqués, ainsi que son applicabilité aux villes et communes.
2. Les exigences de conformité sont ensuite détaillées. Cela inclut les obligations organisationnelles et techniques, comme la gestion des risques, la mise en place de mesures de sécurité et la notification des incidents de cybersécurité. Un accent particulier est mis sur les implications pratiques pour les administrations locales.
3. L'exercice pratique sur le cyber range permet aux participants de simuler la gestion d'un incident de cybersécurité. Ils appliquent les processus de notification, testent leurs capacités de réponse et identifient les faiblesses dans leur organisation.
4. Pour conclure, les impacts organisationnels de la directive NIS 2 sont abordés. Les participants travaillent sur l'élaboration d'un plan d'action concret pour se conformer à la directive, en définissant les responsabilités et en priorisant les mesures nécessaires.

Formation:
Hygiène numérique

Public cible
Employés et responsables des administrations communales

Durée
4 heures

Effectif
De 6 à 15 participants par session

Lieu
Centre d'Excellence en Cybersécurité de Nexova, Rue des Etoiles 140, 6890 Libin (Belgique)

Prochaine date
18 avril 2025

Objectif :

Sensibiliser les participants aux bonnes pratiques pour réduire les risques de cybersécurité dans leurs activités professionnelles quotidiennes.

Programme:

1. L'introduction à la cybersécurité explique pourquoi il est essentiel pour les villes et communes de s'intéresser à la cybersécurité. Les menaces spécifiques aux administrations publiques y sont abordées, mettant en lumière leur vulnérabilité face à certaines attaques.
2. Les bases de l'hygiène numérique couvrent des pratiques fondamentales, comme l'importance de créer et gérer des mots de passe sécurisés, la reconnaissance des faux mails et fichiers suspects, ainsi que la mise à jour régulière des logiciels et la gestion des accès utilisateurs.
3. À travers des exemples pratiques et une analyse d'incidents réels, les participants découvrent les erreurs fréquentes commises par d'autres organisations, afin d'apprendre à ne pas les reproduire.
4. La session se termine par l'élaboration d'un plan d'action personnel pour appliquer les bonnes pratiques au quotidien. Les outils disponibles pour améliorer la cybersécurité individuelle sont également présentés.

Formation: **Sensibilisation au phishing**

Public cible
Agents communaux et responsables de service public

Durée
4 heures (dont 2 heures d'exercice pratique sur le cyber range)

Effectif
De 6 à 15 participants par session

Lieu
Centre d'Excellence en Cybersécurité de Nexova, Rue des Etoiles 140, 6890 Libin (Belgique)

Prochaine date
16 mai 2025

Objectif :

Apprendre à reconnaître, prévenir et réagir face aux attaques de phishing.

Programme:

1. La première partie de la formation se concentre sur la compréhension du phishing. Elle détaille ce qu'est une attaque de phishing, les typologies les plus courantes et les techniques utilisées par les cybercriminels pour tromper leurs victimes.
2. Un focus particulier est fait sur l'impact des attaques de phishing dans les administrations publiques. Des exemples concrets montrent comment un simple email frauduleux peut perturber le fonctionnement d'une organisation, voire compromettre ses données sensibles.
3. La partie pratique, réalisée sur le cyber range, consiste en une simulation réaliste d'une attaque de phishing. Les participants doivent identifier les signes d'une tentative d'escroquerie, apprendre à réagir correctement et signaler les emails suspects.
4. Enfin, un débriefing collectif permet d'analyser les résultats de l'exercice. Les erreurs courantes sont mises en évidence et des recommandations claires sont partagées pour éviter les pièges à l'avenir.