La cybersécurité pour les dirigeants

Référentiel de formation

Campus Cyber Nouvelle-Aquitaine

SecNumedu Formation continue

ANSSI

Sommaire

Introduction

Avec l'usage de plus en plus répandu du « tout numérique » et face à des attaques toujours plus nombreuses, l'importance de la cybersécurité n'est plus à démontrer. Arrêt des services essentiels, perte de revenus, vol ou pertes de données, atteinte à la réputation, les conséquences d'une cyberattaque peuvent être désastreuses et menacer jusqu'à la survie même d'une entreprise. Enjeu stratégique majeur, la question de la sécurité numérique ne relève plus uniquement de la cellule informatique mais doit être prise en compte au plus haut niveau de l'entreprise. Les équipes de direction, et particulièrement les dirigeants, doivent s'impliquer dans l'élaboration et la mise en œuvre d'une politique de sécurité, permettant notamment la résilience des activités essentielles en cas de cyberattaque.

Cette nécessité semble désormais admise dans la conscience collective, pourtant, bon nombre d'entreprises, notamment celles de taille moyenne à intermédiaire, ne sécurisent pas de manière suffisante leurs systèmes d'information, pour diverses raisons : méconnaissance de la menace numérique, manque de méthodes, manque de moyens, etc. Les dirigeants engagent pourtant leur responsabilité face aux risques numériques et ont, dès lors, tout intérêt à intégrer ce volet dans leur feuille de route.

De ces constats est née la réflexion autour de la question suivante : comment permettre aux dirigeants d'entreprise de s'approprier les enjeux et les clés stratégiques de la sécurité numérique leur permettant de piloter la mise en place et le maintien d'un dispositif adapté ? La tâche n'est pas simple et n'est jamais achevée, les technologies et les techniques d'attaque évoluant constamment et nécessitant, de fait, une réflexion permanente sur les dispositifs en place.

Le présent référentiel est le résultat de cette réflexion, initiée et pilotée par le Campus cyber Nouvelle-Aquitaine, ayant fait intervenir différents acteurs, publics et privés, travaillant dans le domaine de la cybersécurité, et des dirigeants d'entreprise, non spécialisés dans ce secteur. Il a pour objectif d'aider les organismes de formation dans l'élaboration d'un programme de formation en cybersécurité destiné aux dirigeants d'entreprise. Il présente pour cela les enseignements minimaux à y intégrer afin de permettre à ces derniers d'être en capacité de piloter la mise en place d'une organisation dédiée.

La formation intègre la réalisation de travaux par les apprenants durant les périodes d'autonomie, leur permettant de mettre en pratique les enseignements théoriques et ainsi d'initier les travaux de sécurisation de leur système d'information.

Label SecNumedu-FC

Les formations conformes aux exigences de ce référentiel peuvent obtenir la labellisation SecNumedu-FC. Les formations labellisées sont référencées sur le site de l'ANSSI et peuvent utiliser le logo associé à SecNumedu-FC.

Le processus d'acquisition du label et ses modalités sont présentés sur le site web de l'ANSSI à l'adresse suivante : https://cyber.gouv.fr/labellisation-secnumedu-fc-comment-proceder.

La cybersécurité pour les dirigeants

Objectifs de la formation

La formation vise à permettre aux dirigeants d'entreprise de s'approprier les enjeux et les clés stratégiques de la sécurité numérique et d'être notamment en capacité de :

- Mesurer le risque numérique
- Identifier les risques majeurs pour l'entreprise
- Identifier les actions prioritaires à mettre en place
- Répondre aux exigences en termes de sécurité numérique
- Réagir en cas de crise cyber

Programme

Kick off : exercice de mise en situation de crise / simulation / serious game

Module 1. Mesurer le risque cyber

Introduction
1. Comprendre son activité numérique
2. Le risque numérique : êtes-vous une cible ?
3. Les grands types de menace
4. À quels impacts s'attendre ?
5. Construire ses scénarios de risque et définir son seuil d'acceptation

Module 2. S'organiser et piloter

Introduction
1. Définir un cadre de gouvernance du risque numérique (amélioration continue)
2. Développer une culture de sécurité numérique
3. Définir sa stratégie de sécurité numérique
4. Mettre en place des polices d'assurance adaptées

Module 3. Bâtir sa sécurité numérique et la valoriser

Introduction
1. Bâtir sa protection
2. Orienter sa défense
3. Faire preuve de résilience en cas de cyberattaque
4. Homologuer ses services numériques critiques

Public visé

- Dirigeants d'entreprise (de taille moyenne ou de taille intermédiaire)
- Membres du comité exclusif

Prérequis

Connaissances générales en informatique

Durée de la formation

Minimum 4 demi-journées, espacées d'un mois durant lequel un travail est réalisé par les apprenants dans leur entreprise respective

Nombre de participants

8 à 16 participants

Mode d'apprentissage[1]

Présentiel ou hybride (présentiel et distanciel)

Méthodes pédagogiques

- Cours théoriques
- Travaux pratiques
- Exercice de mise en situation de crise

[1] Les différents modes d'apprentissage sont définis dans la partie « Exigences générales pour la labellisation SecNumedu-FC » p.9.

Programme détaillé

Prérequis : avoir réalisé le diagnostic de maturité cyber de l'entreprise avec l'outil « mon aide cyber » disponible via le lien suivant : MonAideCyber

Kick-off (1/2 journée) : exercice de mise en situation de crise / simulation / serious game

MODULE 1
MESURER LE RISQUE NUMÉRIQUE

DURÉE : ½ journée

OBJECTIF : Prendre conscience du risque numérique et connaître les divers modes d'attaques et leurs impacts.

CONTENU DÉTAILLÉ :

Introduction

Objectif : adapter le cadre de la formation aux attentes des apprenants.

- Recueil des attentes des apprenants
- Règles et programme

1.1. Comprendre son activité numérique

Objectif : Prendre conscience de la dépendance au numérique de l'activité économique.

- Transformation numérique et nouvelle dépendance
- Introduction du concept de valeur métier et de biens supports
- Cartographier son système d'information et son écosystème

1.2. Le risque numérique : êtes-vous une cible ?

Objectif : Comprendre l'économie de la malveillance numérique et des motivations des attaquants.

- La valeur de la donnée
- Attaque directe et contagion
- Les nouveaux champs de bataille

1.3. Les grands types de menace

Objectif : Connaître les différentes tactiques, techniques et procédures des attaquants.

- Notions de vulnérabilités et de chemins d'attaque
- Les motivations des attaquants
- Les événements redoutés

1.4. À quels impacts s'attendre ?

Objectif : Mesurer les impacts d'une attaque cyber sur l'activité de l'entreprise.

- Les différents impacts d'une attaque cyber (processus, gouvernance, physiques, financiers, réputationnels…)
- L'évolution des impacts (choc initial, souffle et répliques)

1.5. Construire ses scénarios de risque et définir son seuil d'acceptation

Objectif : Être en capacité de décrire au moins un risque critique dans toutes ses dimensions (valeur et bien support, scénario…).

- Identifier les événements redoutés et quantifier leur vraisemblance
- Identifier les scénarios critiques d'attaques cyber
- Quantifier l'impact de ces scénarios et définir son seuil d'acceptation

***Mis à disposition en fin de séance** : méthodologie et cadre d'étude du risque numérique*
***Rendu à la fin de la période d'autonomie :** étude d'un risque critique*

MODULE 2
S'ORGANISER ET PILOTER

DURÉE : ½ journée

OBJECTIF : Être en capacité de mettre en place une organisation adaptée aux risques cyber.

CONTENU DÉTAILLÉ :

Introduction

- Retour sur l'étude de risque du processus critique sélectionné
- Responsabilités du dirigeant

2.1. Définir un cadre de gouvernance du risque numérique (amélioration continue)

Objectif : Piloter le risque cyber.

- Rôle des RSSI / référents cyber / conseillers cyber
- La politique de sécurité des systèmes d'information (PSSI)
- Les obligations réglementaires, les référentiels et la conformité (NIS2, RGPD, etc.)

2.2. Développer une culture de sécurité numérique

Objectif : Faire vivre la politique de sécurité numérique dans l'organisation.

- Placer l'humain au centre du jeu
- Former ses collaborateurs

2.3. Définir sa stratégie de sécurité numérique

Objectif : Construire ses objectifs de sécurité en fonction des risques.

- Définition des objectifs de sécurité
- Choix du référentiel
- Priorité à la sécurité ou à la résilience ?

2.4. Mettre en place des polices d'assurance adaptées

Objectif : Partager le risque cyber résiduel.

- Pourquoi assurer le risque cyber ?
- Comment choisir sa police d'assurance ?

***Mis à disposition en fin de séance** : Plan d'une PSSI et référentiels d'objectifs de sécurité*
***Rendu à la fin de la période d'autonomie** : PSSI (chapitre « Objectifs »)*

MODULE 3
BÂTIR SA SÉCURITÉ NUMÉRIQUE ET LA VALORISER

DURÉE : ½ journée

OBJECTIF : Mettre en place les mesures de sécurité adaptées et faire preuve de résilience en cas d'attaque ou de crise d'origine cyber.

CONTENU DÉTAILLÉ :

Introduction

- Retour sur les PSSI
- Cadrage des objectifs de la demi-journée

3.1. Bâtir sa protection

Objectif : Construire le volet opérationnel de sa politique de sécurité.

- Construction d'un parcours progressif de sécurisation (du diagnostic initial à la conformité)
- Le choix des mesures de sécurité

3.2. Orienter sa défense

Objectif : Comprendre la nécessité de l'évolution des postures de sécurité.

- La veille (renseignement sur la menace et les vulnérabilités) : présentation des acteurs et solutions, intégration dans la posture de sécurité
- Anticiper sa réponse : les PRA et PCA

3.3. Faire preuve de résilience en cas de cyberattaque

Objectif : S'approprier les méthodes de gestion de crise d'origine cyber.

- La cellule de crise : composantes et dynamique
- Les relations avec l'écosystème (ACYMA, ANSSI, CERT régionaux ou sectoriels, CSIRT, autorités, assureurs)
- Le recours à des prestataires (PASSI, PAMS, PDIS, PRIS)
- L'entraînement et les exercices

3.4. Homologuer ses services numériques critiques

Objectif : Décrire les processus d'homologation et leur importance.

- Les référentiels de certification et d'homologation
- L'homologation, une expression de l'engagement raisonné du dirigeant

3.5. Valoriser ses investissements en sécurité numérique

Objectif : Souligner l'importance de la confiance numérique au sein de la chaîne de valeur.

- Le retour sur investissement : quantification financière du risque cyber
- Le développement de la confiance numérique : les preuves de confiance

Mis à disposition en fin de séance *: référentiel de conformité NIS2*
Rendu à la fin de la période d'autonomie *: positionnement initial et stratégie de conformité (NIS2)*

Exigences générales pour la labellisation SecNumedu-FC

- Un descriptif de la formation est disponible sur la page web de l'organisme de formation et détaille notamment :
  - le programme de la formation
  - le volume horaire
  - le nombre d'apprenants (minimum et maximum)
  - le mode d'apprentissage (présentiel, distanciel ou hybride)

- La formation comprend différents supports et notamment :
  - un support de cours pour les apprenants
  - un support de cours formateur (diaporama)
  - un formulaire d'évaluation de la formation
  - des guides méthodologiques pour les apprenants
  - des modèles de documents utilisables par l'apprenant lors de la mise en pratique des enseignements acquis dans l'entreprise

- La pédagogie d'enseignement employée comprend différentes méthodes :
  - méthode affirmative connue aussi comme méthode magistrale (le formateur « dit »)
  - méthode interrogative favorable aux échanges entre formateur et apprenants (le formateur « fait exprimer »)
  - méthode démonstrative où se succèdent démonstrations et exercices de mise en œuvre (le formateur « fait » et « fait faire »)

- La durée indiquée pour chaque module constituant le minimum requis, les organismes sont libres d'adapter cette durée en fonction de leur programme de formation et du niveau des apprenants mais elle ne pourra être inférieure à la durée préconisée.

<u>Exigences relatives au mode d'apprentissage</u>

La formation peut s'effectuer intégralement en présentiel ou en mode hybride, selon les modalités définies ci-après.

➢ Mode présentiel

Les apprenants et formateur(s) sont réunis dans une même salle de classe, durant toute la formation. Ce mode d'apprentissage est obligatoire pour les modules 2 et 3 de la formation.

➢ Mode distanciel ou hybride

Seul le module 1 peut être dispensé à distance, à condition de respecter les conditions suivantes :

- La formation est synchrone, ce qui signifie que les cours intègrent l'ensemble des apprenants et le formateur en direct pendant toute la durée des cours.

- Le formateur et les apprenants peuvent communiquer avec l'ensemble du groupe en permanence pendant toute la durée des cours.
- Les apprenants en distanciel disposent d'une connexion à internet ainsi que les outils permettant les interactions avec le reste du groupe et les formateurs (caméra, micro).
- Le formateur dispose :
  - d'un outil de visioconférence / formation à distance, permettant la gestion de groupes et la création de salles virtuelles. Le formateur est formé à l'utilisation de cet outil.
  - d'une salle virtuelle et d'une visioconférence configurées et préparées en amont de la formation.
  - d'une bonne qualité audio : le formateur est audible par tous, quel que soit l'endroit où il se trouve, y compris lorsqu'il se déplace dans la salle (l'utilisation d'un micro-cravate est suggérée).

- La salle de formation dispose d'un second écran permettant de projeter les caméras des stagiaires à distance. De la même manière, une caméra permet aux apprenants à distance de voir la salle, ainsi tous les stagiaires se voient et peuvent créer des interactions.
- Une seconde caméra filme le formateur et l'endroit où il se trouve. De cette manière, les stagiaires à distance peuvent voir l'ensemble de la gestuelle et des supports pédagogiques utilisés (tableau blanc…) par le formateur. La vue du formateur est projetée sur l'écran des stagiaires à distance.