Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

DÉLÉGATION INTERMINISTÉRIELLE À L'INTELLIGENCE ÉCONOMIQUE

Formation à la cybersécurité des TPE et des PME

Référentiel pédagogique

Mars 2015

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

Ce document est le résultat d'une réflexion d'entreprises et d'acteurs institutionnels spécialisés dans l'accompagnement et la protection des entreprises en matière de cyber-risques.

À la demande du Premier ministre, ce travail a été piloté par la Délégation interministérielle à l'intelligence économique (D2IE – www.intelligence-economique.gouv.fr), avec le soutien de l'Agence nationale de la sécurité des systèmes d'information (ANSSI – www.ssi.gouv.fr).

Ce référentiel pédagogique est un cahier des charges destiné à aider les organismes de formation à élaborer des offres de stage en cybersécurité au profit des TPE/PME. Il décrit les programmes minimaux à partir desquels les formateurs doivent développer une ingénierie pédagogique permettant de produire des programmes et des contenus adaptés.

Tout organisme souhaitant mettre en place des formations sur la base de ce référentiel est invité à en faire part, pour information, à la D2IE (sec.d2ie@pm.gouv.fr).

ooo

Les Très petites entreprises (TPE) et les Petites et moyennes entreprises (PME) représentent une source importante d'emplois et d'innovations.

Elles évoluent aujourd'hui dans un environnement de plus en plus numérique, qui favorise incontestablement leur compétitivité et leur croissance. Pour autant, les nouvelles technologies de l'information et de la communication (NTIC), lorsqu'elles sont mal maîtrisées, peuvent être à l'origine de vulnérabilités et faciliter les attaques sur l'entreprise.

Pour y faire face, les TPE/PME n'ont pas toujours la possibilité de recruter des profils dédiés à la sécurité informatique. Qui plus est, l'approche qu'elles ont de la gestion des infrastructures informatiques varie en fonction de l'utilisation qui en est faite, de leur taille, du secteur économique et du budget qui y est consacré. De fait, à l'exception de certains secteurs très spécifiques, le niveau de perception et de prise en charge du cyber-risque dans les TPE/PME est aujourd'hui très faible.

Afin de promouvoir un environnement favorable au développement économique et de préserver le patrimoine immatériel de ces entreprises, il convient aujourd'hui, dans une démarche d'intelligence économique, de mettre en place des solutions humaines et techniques adaptées aux spécificités des TPE/PME.

La formation de **référent en cybersécurité** interne au profit des TPE/PME permettra de répondre en partie à ce défi.

Objectif de la formation

L'objectif général de la formation est de faire du participant un « **référent en cybersécurité »** interne.

A la fin du cours, le participant devra être en mesure de :

- maîtriser les enjeux de la cybersécurité pour l'entreprise ;
- identifier et utiliser les outils nécessaires à la protection des informations sensibles (personnelles et professionnelles) sur les différents réseaux.

Pour cela, les compétences attendues à la fin de la formation sont les suivantes :

- identifier et analyser des problèmes de cybersécurité dans une perspective d'intelligence et de sécurité économiques ;
- connaître les obligations et responsabilités juridiques de la cybersécurité ;
- identifier et comprendre les menaces liées à l'utilisation de l'informatique et des réseaux internet, réseaux privés d'entreprises, réseaux publics ;
- mettre en œuvre les démarches de sécurité inhérentes aux besoins fonctionnels ;
- savoir présenter les précautions techniques et juridiques pour faire face aux attaques.

Public et prérequis de la formation

La formation à la cybersécurité est ouverte à l'ensemble des TPE/PME du territoire. Elle doit toucher un public hétérogène au sein de ces TPE/PME. Pour cela, elle comprend sept modules servant à construire un parcours cohérent et destiné aux différents profils que sont les dirigeants, les cadres, les responsables informatiques, etc.

Des connaissances de base faciliteront la compréhension des participants.

Structure pédagogique de la formation

Ce programme s'organise autour d'un bloc de modules communs à l'ensemble des TPE/PME, avec des notions d'ordre général et des modules complémentaires, en fonction de l'utilisation faite du numérique et des profils des TPE/PME.

Chaque module se termine par une évaluation tandis qu'un ensemble de liens vers des ressources complémentaires (sites web, documents, statistiques, etc.) est fourni aux participants désireux d'approfondir certains sujets de cybersécurité.

MODULE 1 - Cybersécurité : notions de bases, enjeux et droit commun

MODULE 2 - L'hygiène informatique pour les utilisateurs

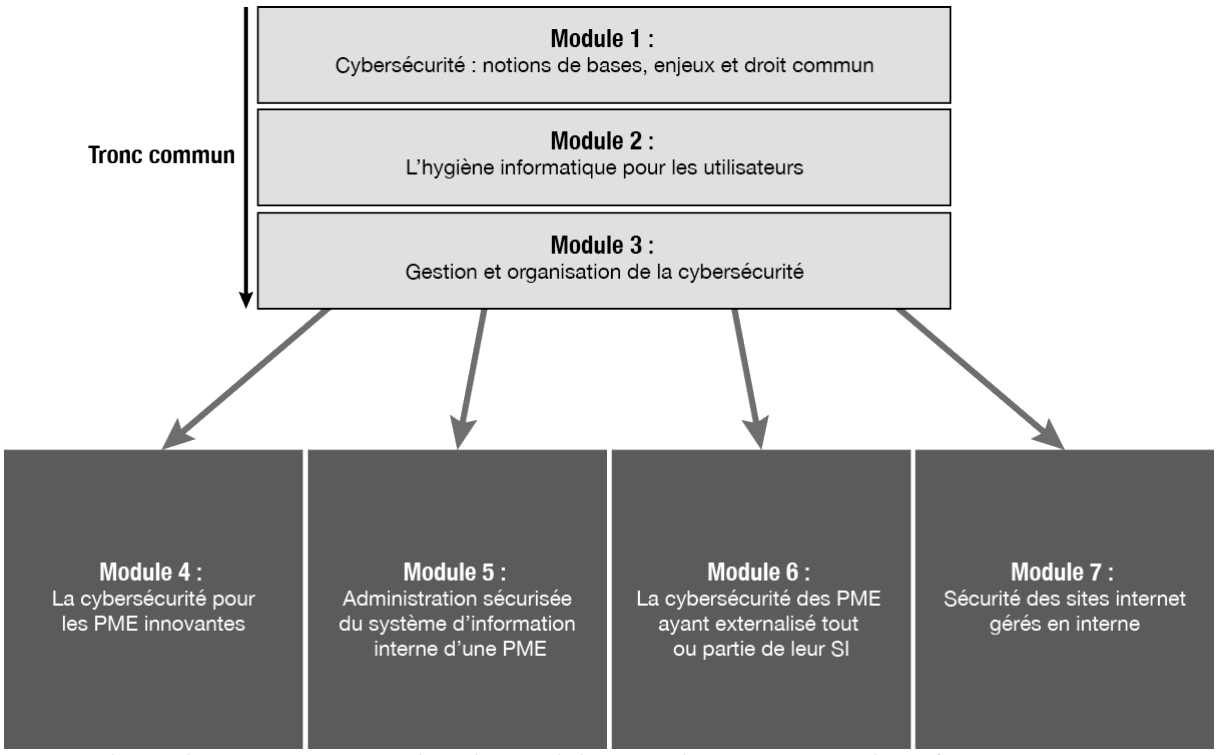
MODULE 3 - Gestion et organisation de la cybersécurité

MODULE 4 - La cybersécurité pour les PME innovantes

MODULE 5 - Administration sécurisée du système d'information (SI) interne d'une PME

MODULE 6 - La cybersécurité des PME ayant externalisé tout ou partie de leur système d'information

MODULE 7 - Sécurité des sites internet gérés en interne



Les volumes horaires présentés dans les modules sont donnés à titre indicatif.

Description détaillée

MODULE 1	Cybersécurité : notions de bases, enjeux et droit commun
Durée	3 heures
Objectifs	▯ Comprendre les motivations et le besoin de sécurité des systèmes d'information (SI). ▯ Connaître les définitions et la typologie des menaces.
Contenu détaillé	▯ Définition de la cybersécurité Sécurité des SI (prévention) + Cyberdéfense (réaction) + Cybercriminalité (sanction) = Cybersécurité ▯ Les enjeux de la sécurité des SI o La nouvelle économie de la cybercriminalité *Les déficiences en matière de cybersécurité peuvent engendrer des pertes financières directes (manque de disponibilité d'un site marchand, par exemple) ou indirectes (espionnage économique sur des appels d'offres, par exemple).* o Panorama des menaces selon une typologie *Panel assez large des différentes menaces (attaques intrusives - injection SQL, passive* – phishing, *destructrices – virus, etc.). Détails sur les* Advanced persistent threat *(APT, Attaque persistante avancée) : rôle des PME dans ces attaques.* o Les vulnérabilités (exemples, détermination, veille) *Vulnérabilité : faiblesse d'un bien, que ce soit à la conception, la réalisation, l'installation, la configuration ou l'utilisation.* o Focus sur l'ingénierie sociale ▯ Les propriétés de sécurité o Présentation du principe de défense en profondeur *Un logiciel spécialisé dans la cybersécurité n'est pas suffisant. La démarche de cybersécurité s'inscrit dans un processus global de sécurité économique (sécurité bâtimentaire, sécurisation des déplacements, contrôle d'accès, etc.). Cf. La sécurité économique au quotidien en 22 fiches thématiques (D2IE).*

	○ Identification et évaluation des actifs et des objectifs de sécurité *Arriver à identifier précisément le besoin.* *Par exemple, un site internet marchand et un site internet « vitrine » n'ont pas les mêmes besoins en termes de sécurité.* *Critères : disponibilité, intégrité, confidentialité, preuve / traçabilité.* *Ces critères permettent de déterminer le niveau de sécurité des SI.* Aspects juridiques et assurantiels ○ Responsabilités *Quelles sont les responsabilités des entreprises qui n'ont pas assez sécurisé leurs SI ? Quelles possibles actions récursoires vers les prestataires ?* *Réglementation européenne : analyse de risque obligatoire pour une entreprise dès qu'il y a une déclaration à la Commission nationale de l'informatique et des libertés (CNIL).* ○ Préservation de la preuve *Que faire en cas d'attaques informatiques ? Comment préserver la preuve tout en restant opérationnel ? Qui faut-il contacter ? Le rôle de l'huissier.* ○ L'offre assurantielle

MODULE 2	L'hygiène informatique pour les utilisateurs
Durée	3 heures
Objectifs	Appréhender et adopter les notions d'hygiène de base de la cybersécurité pour les organisations et les individus.
Contenu détaillé	Connaitre le système d'information et ses utilisateurs *Faire une cartographie des SI de l'entreprise.* Identifier le patrimoine informationnel de son ordinateur (brevets, recettes, codes source, algorithmes…) *Connaitre la valeur des informations contenues dans son ordinateur pour appliquer les différentes procédures de sécurité en fonction des documents utilisés.* Maîtriser le réseau de partage de documents (en interne ou sur internet) *Identifier précisément les passerelles qui existent entre internet et le réseau interne pour éviter les failles qui permettront / faciliteront une intrusion non détectée.* Mettre à niveau les logiciels *Définir une véritable politique de mise-à-jour des logiciels (Qui est en charge ? À quel moment ? etc.).* Authentifier l'utilisateur *Présentation des différentes méthodes permettant d'authentifier les utilisateurs et ainsi de leur attribuer la méthode qui correspond le mieux aux documents qu'ils utilisent.* *Evoquer les bonnes pratiques pour les mots/phrases de passe (conception, fréquences d'utilisation, etc.).* Nomadisme - Problématiques liées au BYOD *(Bring your own devices)* *Evoquer les risques liés à l'utilisation des terminaux mobiles personnels (PC et/ou Smartphone) dans la chaîne de sécurité de l'entreprise.*

MODULE 3	Gestion et organisation de la cybersécurité
Durée	3 heures
Objectifs	- Appréhender les multiples facettes de la sécurité au sein d'une organisation. - Connaitre les métiers directement impactés par la cybersécurité. - Anticiper les difficultés courantes dans la gestion de la sécurité.

Contenu détaillé	- Présentation des publications/recommandations
	  - Guides de l'ANSSI
	  - Recommandations de la CNIL
	  - Recommandations de la police et de la gendarmerie
	  - Club de la Sécurité de l'information Français, Club des experts de la sécurité de l'information et du numérique (CLUSIF/CESIN), etc.
	  - Observatoires zonaux de la SSI
	  - Les *CERTs* (*Computer emergency response team*)
	  Il s'agit ici de sensibiliser les PME à l'importance de la veille sur les différentes documentations disponibles.
	- Présentation des différents métiers de l'informatique (infogérance, hébergement, développement, juriste, etc.)
	- Méthodologie pédagogique pour responsabiliser et diffuser les connaissances ainsi que les bonnes pratiques internes (management, sensibilisation, positionnement du référent en cybersécurité, chartes, etc.)
	  Insister sur les messages que le référent en cybersécurité doit transmettre aux utilisateurs finaux des PME. Présenter le principe des chartes informatiques que chaque utilisateur doit connaitre.
	- Maîtriser le rôle de l'image et de la communication dans la cybersécurité
	  - Surveillance de l'e-réputation
	  - Communication externe
	  - Usage des réseaux sociaux, professionnel et personnel
	- Méthodologie d'évaluation du niveau de sécurité

	Présentation d'un audit de sécurité (réglementation, avantages, coût etc.). • Actualisation du savoir du référent en cybersécurité *Les découvertes en matière de cybersécurité sont nombreuses, rapides et les méthodes d'attaques évoluent en permanence. Il est donc nécessaire que le référent en cybersécurité connaisse les grandes actualités du domaine.* • Gérer un incident / Procédures judiciaires *Identifier clairement le point de contact dans la PME ainsi que son rôle (lien avec les services de police, résilience du SI de l'entreprise etc.).*

MODULE 4	La cybersécurité pour les PME innovantes
Durée	3 heures
Objectif	- Appréhender la protection de l'innovation à travers les outils informatiques
Contenu détaillé	- Présentation de la protection du patrimoine scientifique et technique de l'entreprise *L'objectif est de présenter les mesures et obligations liées à la préservation du patrimoine scientifique et technique, notamment les dispositifs étatiques (ZRR, classifié de défense, etc.).* - Droit de la propriété intellectuelle lié aux outils informatiques *Il s'agit de donner les moyens nécessaires aux entreprises ayant des données importantes pour connaitre les tenants et les aboutissants des contrats comme l'infogérance, par exemple.* - Cyber-assurances *Présentation d'un domaine nouveau et émergent. L'objectif est de donner les clés nécessaires à une PME dans le cas où elle souhaiterait souscrire à une offre de cyber-assurance.* - Cas pratiques *Présentation de cas de cyber-attaques avérés.*

MODULE 5	Administration sécurisée du système d'information (SI) interne d'une PME
Durée	6 à 9 heures
Objectifs	▯ Savoir sécuriser le SI interne ▯ Savoir détecter puis traiter les incidents ▯ Connaitre les responsabilités juridiques liées à la gestion d'un SI
Contenu détaillé	▯ Analyse de risque (EBIOS / MEHARI) *Définir les besoins auxquels répondre à travers les principes et domaines de la SSI* ▯ Principes et domaines de la SSI afin de sécuriser les réseaux internes *Développement de la notion de défense en profondeur évoquée précédemment.* o Politique et stratégie de sécurité o Gestion des flux, notamment réseaux sans fil / architecture réseaux (cloisonnement du réseau) o Gestion des comptes, des utilisateurs, des privilèges selon le besoin d'en connaître o Gestion des mots de passe o Gestion des mises à jour o Journalisation et analyse o Gestion des procédures o Plan de continuité d'activité (PCA) / Plan de reprise d'activité (PRA) o Virtualisation / cloisonnement ▯ Détecter un incident ▯ Gestion de crise o Traitement technique de l'incident o Procédure organisationnelle et communication o Reprise d'activité ▯ Méthodologie de résilience de l'entreprise ▯ Traitement et recyclage du matériel informatique en fin de vie (ordinateurs, copieurs, supports amovibles, etc.) ▯ Aspects juridiques o Responsabilité en l'absence de conformité des infrastructures o Cyber-assurances

MODULE 6	La cybersécurité des PME ayant externalisé tout ou partie de leur SI
Durée	3 heures
Objectifs	▯ Connaitre les techniques de sécurisation d'une SI, partiellement ou intégralement externalisé
Contenu détaillé	▯ Les différentes formes d'externalisation o Les contrats de services « classiques » o Enjeux du *cloud computing* o *Software as a Service* (SaaS) o Techniques de sécurité lors de l'externalisation (chiffrement des données…) ▯ Comment choisir son prestataire de service ? *Quels sont les points clés, techniques et organisationnels, de sécurité à bien identifier lors du choix d'un prestataire.* *Aborder la notion et le contexte de certification / qualification des produits.* ▯ Aspects juridiques et contrat o Connaitre les bases juridiques pour protéger son patrimoine économique lors de l'externalisation d'un SI *Exemple : qui est propriétaire des données (même après la fin du contrat) ?* o Présentation du référentiel de l'ANSSI *Maitriser les risques de l'infogérance*

MODULE 7	Sécurité des sites internet gérés en interne
Durée	9 à 12 heures
Objectifs	▯ Connaitre les règles de sécurité pour gérer un site internet
Contenu détaillé	▯ Menaces propres aux sites internet ▯ Approche systémique de la sécurité (éviter l'approche par patches) ▯ Configuration des serveurs et services ▯ HTTPS et Infrastructure de gestion de clés (IGC) ▯ Services tiers ▯ Avantages et limites de l'utilisation d'un CMS et / ou développement web ▯ Sécurité des bases de données ▯ Utilisateurs et sessions ▯ Obligations juridiques réglementaires o Le e-commerce o La Loi pour la confiance dans l'économie numérique (LCEN), la Commission nationale informatique et liberté (CNIL), *Payment Card Industry-Data Security Standard* (*PCI-DSS)*

Documentation non exhaustive

La sécurité économique au quotidien en 22 fiches thématiques, à destination des TPE/PME

www.intelligence-economique.gouv.fr/methodes-et-outils/la-securite-economique-au-quotidien

Guides techniques et bonnes pratiques de l'ANSSI

www.ssi.gouv.fr/entreprise/bonnes-pratiques

ooo

Délégation interministérielle à l'intelligence économique
55, rue St Dominique - 75007 Paris
Tél : (33) 1 42 75 58 20 - Contact : sec.d2ie@pm.gouv.fr
www.intelligence-economique.gouv.fr

Maquette et impression : Pôle Conception graphique-Fabrication – DSAF – Mars 2015