le cnam
Bretagne

CYBER

FORMATIONS COURTES

MINISTÈRE
DE L'ENSEIGNEMENT
SUPÉRIEUR
ET DE LA RECHERCHE
Liberté
Égalité
Fraternité

Région
BRETAGNE

À l'ère numérique actuelle, la sécurité informatique est cruciale pour toute organisation. C'est pourquoi le Cnam Bretagne a développé des programmes de formation de haute qualité de courte durée, pour répondre aux besoins de votre entreprise.

Nos formations sont adaptées à différents niveaux de compétences, et elles couvrent une gamme complète de sujets, de la prévention des cybermenaces à la conformité RGPD en passant par la sécurisation des postes informatiques.

RB0E01

PRÉVENTION EN CYBERSÉCURITÉ
RISQUES ET BONS USAGES

Objectifs de la formation

Les usages numériques ont particulièrement évolué avec le recours au télétravail, l'utilisation de nombreux services et objets connectés. Ce contexte a favorisé le développement et la fréquence des cyberattaques de plus en plus professionnalisées. Tout salarié est naturellement confronté à ces menaces, car il est la 1ere porte d'entrée dans le système d'information de l'entreprise.
Cette formation consiste à former vos salariés à la compréhension de la cybermenace afin qu'ils acquièrent de bonnes pratiques et améliorent la protection des données de l'entreprise.

Cas d'usage

- Identifier les enjeux personnels et professionnels en cybersécurité
- Auto-analyser ses pratiques de sécurité
- Comment avoir un mot de passe solide ?
- Commenter et utiliser un coffre-fort numérique pour stocker tous ses mots de passe
- Comment reconnaître les pièges du phishing ?
- Comment se protéger d'une usurpation d'identité ?
- Comment se prémunir contre les fuites de données personnelles ?

Evaluation :

Évaluation des compétences acquises via un questionnaire en ligne intégrant des mises en situation

3h30
en présentiel ou distanciel (en fonction de la programmation)

Prochaine session :
Contacter nos conseillers

Prérequis
aucun

nombre de places mini.
5 personnes

tout public ayant accès à un système d'information (niveau débutant)

445 €
par participant

222,50 €
Tarif EDIH par participant

Programme

Mot de passe
- Temps de résistance d'un mot de passe, autotest
- Vol de mot de passe : risques encourus pour le salarié/son entreprise
- Créer et gérer ses mots de passe : solidité, longueur, diversité, confidentialité
- Utiliser un coffre-fort numérique pour stocker tous ses mots de passe

Hameçonnage ou « phishing »
- La technique du hameçonnage : exemples
- Pourquoi les données intéressent-elles les pirates ?
- Comment reconnaître les pièges ?
- Que faire si l'on est piégé ?

Usurpation d'identité
- Quelle définition ?
- Les conséquences d'une usurpation d'identité suite à un hameçonnage
- Comment s'en protéger ?
- Les peines encourues

Fuite de données
- Qu'est-ce qu'une fuite ou violation de données personnelles ?
- Comment se prémunir contre les fuites de données personnelles ?
- Que faire en cas de fuite ou violation de données personnelles ?
- Violation de données personnelles, les types d'infractions

RB0E02

SÉCURITÉ INFORMATIQUE
RISQUES, CONSÉQUENCES ET MESURES DE PROTECTION

Objectifs de la formation

Quelle soit petite ou de grande taille, toute organisation est soumise au risque cyber. La connaissance et la maîtrise de ce risque sont donc incontournables pour éviter une perte d'activité. L'objectif de cette formation est d'identifier et de comprendre les risques cyber, de les mesurer et de déterminer les actions à mettre en œuvre afin de les réduire.

Cas d'usage

- Quels sont les risques cybersécurité pour mon entreprise ?
- Comment réaliser une analyse de risques ?
- Quelles sont les principales mesures de sécurité à mettre en place ?
- Comment structurer son management à la sécurité de l'information (SMSI) ?
- Comment se préparer à une crise de cybersécurité (PCA / PRA) ?

21 h (3 jours)
en présentiel ou distanciel
(en fonction de la programmation)

Prochaine session :
Contacter nos conseillers

2775 €
par participant

1388 €
Tarif EDIH par participant

nombre de places mini.
5 personnes

Toute personne en charge de la sécurisation d'un système informatique ou souhaitant être sensibilisée à la maîtrise des risques cyber, notamment :
- Directeur
- Responsable du Plan de Continuité d'Activité (RPCA - BCM)
- Chargé de gestion de crise
- Responsable opérationnel
- Responsable de la Sécurité des Systèmes d'Information (RSSI - CISO)

Prérequis
aucun

Evaluation :

Évaluation des compétences acquises via un questionnaire en ligne intégrant des mises en situation

Programme

Introduction
- Référentiel général de sécurité (RGS)
- Principes généraux relatifs à la protection des données de la RGPD

Démarche d'homologation de la sécurité
- Précision du référentiel réglementaire
- Délimitation du périmètre
- Diagnostique des besoins de sécurité et du niveau de maturité SSI de l'organisme
- Acteurs de l'homologation

Appréciation des risques
- Approche et limites de l'analyse des risques
- Cadre de l'analyse de risques (ISO 27005 :2018)
- NIST SP 800 30
- MEHARI
- ANSSI EBIOS Risk Manager
- Analyse d'impact relative à la protection des données (Privacy Impact Assessment)
- Analyse de la maturité du SI

Focus sur EBIOS Risk Manager

Périmètre de contrôle et audits

Décision formelle d'homologation

Plan de traitement des incidents et de reprise d'activité
- Principes généraux
- Introduction à la mise en œuvre d'un PCA / PRA (basé sur la norme ISO 22301)
- Procédure d'alertes et de gestion de crise

La maintenance et le suivi de la sécurité des systèmes d'information
- Mise en place d'une démarche d'amélioration continue basée sur la norme ISO 27001
- Veille technique et juridique de la sécurité des systèmes d'information

RB0E03

RGPD
RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Objectifs de la formation

La sécurité des données personnelles est, au-delà d'une obligation légale, un enjeu majeur pour tous les organismes publics et privés, ainsi que pour tous les individus. Tous les organismes sont aujourd'hui touchés par des attaques, quels que soient leur taille et leur secteur. Ces attaques relèvent de la cybermenace et ont des finalités variées allant de l'espionnage au sabotage et passant par la déstabilisation et le profit financier.
Cette formation vise à enseigner par des exemples concrets les principales mesures qu'il convient de mettre en place pour la protection des données.

14h (2 jours)
en présentiel ou distanciel
(en fonction de la programmation)

Prochaine session :
Contacter nos conseillers

1 850 €
par participant

925 €
Tarif EDIH par participant

nombre de places mini.
5 personnes

Toute personne concernée par le traitement de données personnelles (RH, marketing, comptabilité, ...), notamment : DPO, DSI, RSSI, Juriste.

Prérequis
aucun

Cas d'usage

- Quelles sont les contraintes légales de gestion des données pour mon entreprise ?
- Comment initier un chantier RGPD ? Comment structurer ma feuille de route ?
- Comment mettre en œuvre le registre simplifié des traitements ?
- Comment sécuriser mes traitements de données ?

Evaluation :

Évaluation des compétences acquises via un questionnaire en ligne intégrant des mises en situation

Programme

Introduction au RGPD
- Genèse du règlement
- Définitions : Données à caractère personnel, Données sensibles, Traitement, Responsable de traitement, Sous-traitant, Délégué à la protection des données
- Principes de licéité des traitements : finalités du traitement, qualité des données, durée de conservation, base juridique de traitement
- Obligations du Responsable de traitement et du Sous-traitant

Feuille de route pour les traitements
- Cartographie : comment identifier les traitements de données personnelles et leurs supports ?
- Cas de l'anonymisation
- Référencement des traitements dans un registre simplifié pour les TPE
  - Atelier exploitant le modèle proposé par la CNIL
- Garantir la sécurité des données : Approche par les risques
  - Atelier mettant en œuvre l'outil PIA de la CNIL

Sécurisation des traitements
- Rappel de l'obligation du Responsable de traitement
- Introduction à la notion de code de conduite
- Cas de l'informatique en nuage
- Revue des 12 règles essentielles de sécurisation de l'informatique applicables à la protection des données personnelles
- Démonstration de génération de mot de passe robuste au moyen de l'outil Keepass
- Atelier mettant en œuvre le guide de la CPME/ANSSI sur des exemples concrets
- Focus sur les mesures de journalisation
- Focus sur la « pseudonymisation »

Que faire en cas de violation des données personnelles ?

RB0E04

SÉCURISER UN PARC INFORMATIQUE
BONNES PRATIQUES

Objectifs de la formation

La transformation numérique des entreprises et collectivités permet d'optimiser des processus et rapprocher les entreprises de leurs clients ou usagers. Mais cette transformation s'accompagne de risques cyber qui ne cessent de s'intensifier. Il faut s'en protéger à tous les niveaux et mettre en place de bonnes pratiques techniques pour sécuriser le système d'information de son entreprise.
Cette formation vise à enseigner par des exemples concrets les principales mesures qu'il convient de mettre en place pour sécuriser ses postes informatiques.

Cas d'usage

- Quels sont les menaces et les risques ?
- Quels sont les principes fondamentaux de sécurité ?
- Comment sécuriser un poste de travail, sa messagerie, gérer le nomadisme, l'usage du cloud ?
- Comment sécuriser la pratique du nomadisme ? La messagerie ? L'usage du Cloud ?
- Comment réagir en cas de cyberattaque (techniquement et légalement) ?

Evaluation :

Évaluation des compétences acquises via un questionnaire en ligne intégrant des mises en situation

14h (2 jours)
en présentiel ou distanciel
(en fonction de la programmation)

Prochaine session :
Contacter nos conseillers

1 850 €
par participant

925 €
Tarif EDIH par participant

nombre de places mini.
5 personnes

Toute personne assurant le rôle d'administrateur système ou réseau au sein de sa PME ou ayant un niveau technicien informatique et souhaitant connaître les règles de bases de protection d'un poste informatique.

Prérequis
aucun

Programme

Les bases de la cybersécurité
- Gestion de la sécurité informatique
- La P.S.S.I.
- L'inventaire, les documentations, manuels et charte de sécurité
- Connaître le parc informatique ainsi que les actifs métiers

Sécuriser les postes de travail
- Chiffrement du disque dur avec BitLocker
- L'importance de l'authentification
  - Risque et bonnes pratiques sur les mots de passe
  - Conteneur de mots de passe (KeePass)
  - L'authentification multifacteurs
  - Mise en place d'une authentification par certificats
  - Les demandes d'élévation de privilèges (UAC)
  - Infrastructure de gestion de clés et PKI
- Savoir gérer les autorisations
  - Gestion de politiques de sécurité (ACL)
  - Les applications non désirées (unwanted application)
  - Blocage d'applications (AppLocker)
  - Surveillance et cloisonnement de certaines applications (AppLocker)
- Surveillances des PC
  - La journalisation des évènements
  - Les antivirus (Windows Defender)
- Sécuriser la messagerie
  - Former le personnel au phishing
  - Les logiciels Antivirus / Anti-Spam et anti-phishing
- La gestion des sauvegardes

Sécuriser les réseaux
- Panorama de techniques malveillantes (vol de session, usurpation d'IP, scan réseau, etc.)
- Rappels sur les réseaux
  - @Mac, @IP, Routage, ICMP, DHCP, DNS)
  - Sécurité des protocoles (http, FTP, Telnet, etc.)
  - Segmentation réseau : les VLANs
- Protéger son réseau
  - Filtrer les réseaux avec les Pare-Feu
  - Ruptures de protocoles avec les Proxy
  - Les bastions
  - Les DMZ

Le nomadisme
- Risques d'accès physique
- Les risques des wifi publics et réseaux
- L'usage des VPN (le full-tunneling)

RB0E05

SAVOIR GÉRER UNE CRISE

Objectifs de la formation

Les spécificités liées à la problématique cyber démontrent la nécessité de se préparer à une attaque en formalisant les attaques passées afin d'en reconnaître des « patterns » et en organisant des exercices afin que chaque auditeur puisse en comprendre les enjeux ainsi que le rôle qu'il va devoir jouer sur l'ensemble de la chaîne de sécurité dans le cadre d'une crise cyber.

Cas d'usage

- Comment mettre en place une organisation de prévention et de gestion de crise ?
- Comment réaliser des plans de défense, PRA, PCA, PCI, PRI, fiches réflexes, etc. ?
- Comment identifier les compétences utiles à la gestion de crise et savoir les mobiliser, utiliser au mieux les plans élaborés au fur et à mesure du déroulement du scénario ?
- Comment se coordonner entre les équipes techniques et managériales ?
- Comment rendre compte aux instances étatiques (déclaration d'incident, couverture médiatique) et internes (ensemble des équipes, gouvernance et membres d'autres cellules) ?

14h (2 jours)
en présentiel ou distanciel
(en fonction de la programmation)

Prochaine session :
Contacter nos conseillers

1 850 €
par participant

925 €
Tarif EDIH par participant

nombre de places mini.
5 personnes

Toute personne en charge de la sécurisation d'un système informatique ou souhaitant être sensibilisée à la maîtrise des risques cyber, notamment :
- Directeur
- Responsable du Plan de Continuité d'Activité (RPCA - BCM)
- Chargé de gestion de crise
- Responsable opérationnel
- Responsable de la Sécurité des Systèmes d'Information (RSSI - CISO)

Prérequis
aucun

Evaluation :

Évaluation des compétences acquises via un questionnaire en ligne intégrant des mises en situation

Programme

Introduction au RGPD

Introduction à la modélisation de la menace

Cycle de la Threat Intelligence

Organisation d'une cellule de crise
- Planifications
  - Politique de sécurité, plans de défense, SMCA
  - Continuité d'activité (PCA, PCO, PGC, PRA) et continuité informatique (PCI, PRI)
- Méthodologie de gestion de crise
  - Qu'est-ce qu'une crise ? Typologies de crises
  - Gestion d'incidents et gestion de crise
  - Mécanismes de prise de décisions
- Décisions en situation de crise
  - Étude d'une crise pour en tirer des enseignements
  - Passage en crise : réunion et ordres de déclenchement, mise en configuration de crise, décisions
- Coordonner la communication de crise

Exercice de crise
- Coordonner les équipes
- Réaliser les déclarations légales nécessaires en fonction de la situation simulée et de la législation applicable
- Gérer les phases de réaction immédiate et d'investigation

Rétrospective sur le déroulé de l'exercice
- « Déconfliction » : facteurs, conduite, compte-rendu
- Compte rendu et modélisation de l'attaque effectuée
- Adaptation de l'organisation et des procédures dans un processus d'amélioration continue

RB0E06

COMPRENDRE LE CONTEXTE DE LA CYBERSÉCURITÉ

Objectifs de la formation

Les petites et moyennes entreprises ainsi que les collectivités sont de plus en plus ciblées par des cyberattaques, souvent parce qu'elles peuvent être perçues comme ayant moins de défenses robustes comparées aux grandes entités.
Ces attaques peuvent entraîner des pertes financières significatives, des dommages à la réputation, voir la disparition de l'entreprise.
La prise en compte de ce risque supplémentaire est difficile : ce domaine est récent et reste abstrait ou énigmatique pour la grande majorité de la population. Cela nécessite donc de mobiliser plusieurs compétences notamment dans le secteur juridique, de la gouvernance et technique.
Aussi cette formation a pour objectif de donner une vision générale des problématiques liées à la cybersécurité afin d'en comprendre les risques, les enjeux ainsi que les dispositions à mettre en œuvre pour se protéger des attaques.

Cas d'usage

- Comprendre les risques des cyberattaques pour une PME ou une collectivité locale
- Acquérir le vocabulaire fondamental
- Connaître les principes fondamentaux de sécurité de l'information
- Connaître le contexte juridique et les obligations légales
- Comprendre les dispositifs à mettre en place pour se protéger

Evaluation :

Évaluation des compétences acquises via un questionnaire en ligne

3h30
en présentiel ou distanciel (en fonction de la programmation)

Prochaine session :
Contacter nos conseillers

Prérequis
aucun

nombre de places mini.
5 personnes

tout public

445 €
par participant

222,50 €
Tarif EDIH par participant

Programme

Introduction à la cybersécurité

Les risques liés à la cybersécurité liés aux PME et collectivités

Comprendre par l'exemple les plus courantes des attaques informatiques

- Piratage des comptes
- Le Phishing
- La fraude au virement bancaire (et fraude au président)
- Les Ransomwares

Que dit le droit ? Dispositifs législatifs et obligations légales

- Principes fondamentaux de la République numérique de 2016
- Loi Godfrain relative à la fraude informatique
- LPM et RGPD
- CNIL, Commission nationale informatique et libertés
- ANSSI, Agence Nationale de Sécurité des systèmes d'information
- Cybercriminalité et infractions pénales
- NIS et NIS2

Les grands principes de la protection cyber

RB0E07

TECHNIQUES D'OSINT
POUR UN CONTEXTE SPÉCIFIQUE

Objectifs de la formation

À l'issue de la formation, les participants seront capables de :
- Maîtriser les techniques avancées de recherche d'informations accessibles en ligne (Open Source Intelligence - OSINT).
- Utiliser des outils spécifiques pour collecter, analyser et exploiter des données issues de sources ouvertes, y compris les moteurs de recherche, les réseaux sociaux et les bases de données en ligne.
- Appréhender les enjeux de la veille concurrentielle et sécuritaire dans un contexte professionnel.
- Identifier et évaluer les menaces potentielles pour les organisations à partir de données accessibles au public.
- Mettre en œuvre des pratiques de cybersécurité basées sur les résultats d'investigations OSINT pour anticiper les risques.
- Adopter une approche éthique et légale de l'utilisation des données ouvertes.

Cas d'usage

- Analyse de risques pour les PME et collectivités locales : utilisation de l'OSINT pour identifier les menaces spécifiques pesant sur une organisation, telles que la fuite de données sensibles ou l'exposition involontaire d'informations stratégiques.
- Veille concurrentielle : collecte d'informations sur les concurrents pour anticiper leurs stratégies, comprendre leur positionnement et adapter son offre de services.
- Surveillance des réseaux sociaux : détection de signaux faibles sur les plateformes sociales pouvant impacter la réputation de l'organisation ou révéler des comportements suspects.
- Identification de vulnérabilités techniques : recherche de failles sur des sites web ou systèmes d'information exploitables par des acteurs malveillants.

14h (2 jours)
en présentiel ou distanciel (en fonction de la programmation)

Prochaine session :
Contacter nos conseillers

Prérequis
aucun

nombre de places mini.
5 personnes

Toute personne étant sensibilisée au monde du numérique

1 850 €
par participant

925 €
Tarif EDIH par participant

Programme

- Techniques de recherche sur Internet (moteurs de recherche, dorks, contenu archive, ...)
- Techniques de recherche sur les réseaux sociaux (50CMINT)
- Techniques de recherche géospatiales (GEOINT)
- Techniques d'analyse d'image (IMINT)
- Techniques de recherche de données techniques Rees a des sites-web (RECON)

Format

- Contenu théorique présente de manière didactique et interactive
- Démonstrations
- Travaux pratiques représentatifs du contexte vise (min 1j)

Evaluation :

Évaluation des compétences acquises via un questionnaire en ligne

NOUS CONTACTER

Cnam Bretagne
tél. : 02.57.52.05.48
brest@cnam-bretagne.fr

LE CNAM BRETAGNE VOTRE PARTENAIRE DE FORMATION EN BRETAGNE

DES FORMATIONS COURTES, CIBLÉES ET EFFICACES

CONSEILS PERSONNALISÉS POUR VOTRE ENTREPRISE

Nos conseillers dédiés sont à votre service pour vous guider dans toutes les étapes du processus de formation. De la prise en charge au financement, bénéficiez d'une écoute attentive et de conseils sur-mesure adaptés à votre entreprise.

DES FORMATIONS TOURNÉES VERS L'OPÉRATIONNALITÉ

Nos formations courtes sont rigoureusement conçues pour maximiser l'efficacité et l'impact sur votre activité. Des cas pratiques pertinents et des échanges d'expérience riches qui reflètent les défis réels de votre secteur sont proposés.

ACCESSIBILITÉ HANDICAP

Le Cnam Bretagne est engagé dans une démarche de progrès en matière d'accueil des personnes en situation de handicap. Notre référent se tient à votre disposition pour en échanger dès maintenant.

www.cnam-bretagne.fr

version - août 2024