



Cybersécurité

Ref 8920180

Cybersécurité

Formations courtes

Approfondissement

1 jour (7 heures)

Paris

Réagir aux failles de sécurité et les anticiper

Qu'elles proviennent d'une erreur, d'une négligence ou de procédés illicites, les failles de sécurité représentent aujourd'hui l'une des préoccupations majeures des organismes privés ou publics. Piratage des systèmes de traitement automatisé de données, vol de données personnelles, perte d'informations confidentielles et stratégiques, les enjeux sont importants et lourds de conséquences sur le plan financier.

Objectifs

Identifier les différentes formes de cyberattaques

Mettre en œuvre les actions suite à une attaque informatique

Mettre en place les mesures pour prévenir les attaques informatique

Pour qui ?

Juristes et responsables juridiques
Responsables informatiques, compliance
et sécurité

Prérequis

Avoir des connaissances sur les aspects
juridiques du digital ou avoir suivi "
Maîtriser le cadre juridique du digital "
(code 20026)

Code dokélio : 53249

Compétences acquises:

Programme

Recenser les différentes atteintes possibles du système de traitement automatisé de données (STAD)

Identifier les conditions préalables

- La notion de STAD
- Le " maître du système "
- La question de la protection du STAD

Cerner les infractions d'atteinte à un système de traitement automatisé de données

- L'accès frauduleux
- Le maintien frauduleux
- L'atteinte à l'intégrité du système
- L'atteinte à l'intégrité des données
- L'association de malfaiteurs informatiques
- La détention d'un programme informatique conçu pour commettre une atteinte à un STAD
- La tentative
- Les peines complémentaires encourues
- Les atteintes aux STAD vues par les législations européennes

Intégrer l'infraction spécifique de vol d'informations

- Le cadre légal
- La problématique du vol d'informations

- Les aménagements jurisprudentiels
- De nouvelles armes juridiques

Étude de cas : analyse de cyberattaques fréquemment rencontrées

Réagir face à une cyberattaque

Déposer une plainte auprès du procureur de la République

Exercice d'application : rédaction du plan détaillé de la plainte

Notifier la violation de données personnelles à la Commission nationale de l'informatique et des libertés

Gérer la communication

- Mettre en place un plan média : communiqué de presse, bandeau sur le site internet, communication sur les médias sociaux, Facebook et Twitter, script de réponse aux questions des journalistes
- Préparer un communiqué destiné aux clients

Exercice d'application : rédaction d'un communiqué aux clients dont les données personnelles ont été volées

Gérer l'aspect assurantiel

Prévenir le risque de cyberattaque par la mise en place d'actions préventives

Sécuriser les systèmes d'information contre les risques externes

Sécuriser des systèmes d'information contre les risques internes

- Mettre en place une charte informatique destinée aux salariés, administrateurs et prestataires externes
- Mettre en place une charte d'utilisation du réseau Wi-Fi

1120€ HT

S'inscrire

Prochaines sessions

Paris

02 déc. 2019

02-12-2019

02-12-2019

20 mai 2020

20-05-2020

20-05-2020

09 déc. 2020

09-12-2020

09-12-2020

[Nous contacter](#)