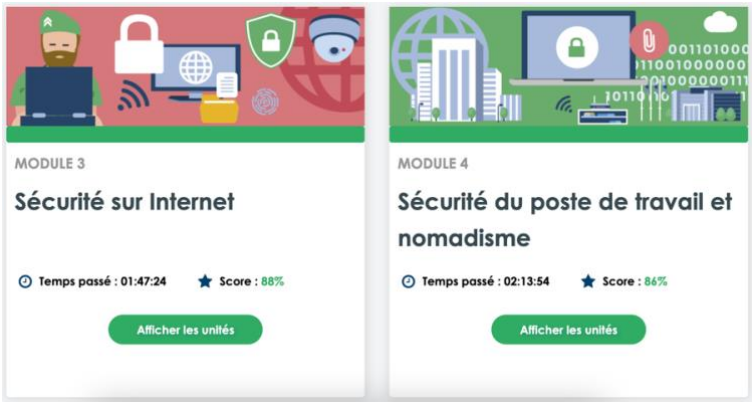
Compte-rendu Mission 10 Cybersécurité



Module : La Sécurité sur Internet

Internet, ce réseau mondial interconnecté, permet la communication et l'échange d'informations à l'échelle planétaire. Reposant sur des protocoles de communication standardisés tels que TCP/IP, il facilite la transmission de données entre des milliards d'appareils. À l'origine développé à des fins militaires, Internet a ensuite été redirigé vers le milieu scolaire.

Les fichiers provenant d'Internet comprennent une diversité de contenus tels que des documents textuels (Microsoft Word), des fichiers audio (MP3), des images (JPEG), des vidéos (AVI), des applications (EXE), et bien plus encore. Accessibles via des liens hypertexte, ces fichiers permettent aux utilisateurs de naviguer et de récupérer des informations depuis des sites web et d'autres sources en ligne. Cependant, la présence de fichiers malveillants rend crucial le fait d'être attentif à ce que l'on télécharge, car ces fichiers peuvent rapidement devenir dangereux, compromettant la sécurité des postes en prenant le contrôle, exfiltrant des données, ou demandant des rançons.

La navigation web, réalisée à l'aide de navigateurs tels que Chrome, Firefox, Safari et Edge, consiste en l'exploration des contenus d'Internet. Chaque navigateur a ses qualités et défauts, mais l'essentiel est de choisir un logiciel régulièrement mis à jour pour garantir son bon fonctionnement.

La messagerie électronique, aujourd'hui au cœur de nos communications, offre un moyen asynchrone de communication via des courriers électroniques. Malgré son utilité, elle est souvent la cible de démarchages indésirables et d'attaques malveillantes. Les protocoles tels que SMTP et IMAP sont utilisés pour envoyer et recevoir des courriers électroniques. Il est essentiel d'adopter des bonnes pratiques pour utiliser sa messagerie de manière sécurisée et se prémunir contre les menaces en ligne.

En coulisses, une connexion web implique plusieurs composants, du navigateur aux serveurs web en passant par des protocoles comme HTTP ou HTTPS. Cette interaction technique utilise des adresses IP, des protocoles de sécurité (SSL/TLS), des serveurs DNS pour la

résolution des noms de domaine, et d'autres éléments pour garantir une transmission efficace des données sur le réseau.

Module : Sécurité du poste de travail et nomadisme

Le deuxième module, se concentrant sur la sécurité du poste de travail et le nomadisme, nous plonge au cœur des principes essentiels de la sécurité informatique personnelle et professionnelle. Structuré en cinq unités, ce module nous permet d'en apprendre plus sur la sécurité informatique au travail et chez soi.

Dans ce premier module, nous remarquons l'importance fondamentale des applications et des mises à jour. Nous apprenons à comprendre le rôle vital des mises à jour, bien plus que de simples correctifs. C'est un processus continu d'amélioration, afin d'éviter la présence de vulnérabilités ou pire encore d'infection de notre ordinateur.

Cette étape nous transporte vers les bases de la sécurité informatique. Nous explorons les options de configuration de base, telles que les paramètres de confidentialité et de sécurité. Nous découvrons comment personnaliser ces paramètres pour répondre à nos besoins spécifiques, élevant ainsi notre niveau de sécurité afin de rendre plus compliqué et plus long les piratages voir de pouvoir ne pas l'être pour donner suite à un niveau de sécurité élevé.

En progressant dans ce module, nous montons d'un cran en abordant des configurations plus avancées. Nous examinons les paramètres avancés de pare-feu, les règles de filtrage des paquets, et d'autres aspects qui ajoutent des couches supplémentaires de protection à notre environnement numérique et qui permettent de réguler le trafic des connexions entrantes sur notre système.

L'étape suivante nous guide à travers le parc des menaces potentielles liées aux clés USB et aux dispositifs de stockage externes. Nous découvrons les risques associés à l'utilisation de ces périphériques. Comment éviter les pièges lorsqu'on les branche, comment scanner les fichiers avant de les ouvrir, toutes ces connaissances deviennent nos outils pour naviguer prudemment dans ce territoire potentiellement dangereux et ainsi éviter tout problème lié à ça même au travail.

Enfin, la dernière étape adopte une approche stratégique avec la séparation des usages. Nous apprenons comment minimiser les risques en délimitant clairement les activités personnelles et professionnelles sur nos machines, renforçant ainsi notre sécurité. Cela permet donc d'éviter toute élévation de privilège non voulu et d'être encore plus protéger qu'avant.

Chaque terme, qu'il s'agisse d'applications, de mises à jour, de configurations, de sécurité des périphériques amovibles, ou de séparation des usages, nous montre bien que le monde numérique est en constante évolution et qu'il est très difficile aujourd'hui de vouloir tout apprendre au vu de la vitesse avec laquelle il se développe.