Compte rendu du module 3 : Sécurité sur Internet

Internet est un réseau mondial interconnecté qui permet la communication et l'échange d'informations à l'échelle planétaire. Il repose sur des protocoles de communication standardisés TCP/IP, facilitant la transmission de données entre des milliards d'appareils. Internet a été développé au début pour des raisons militaires puis redirigé dans le milieu scolaire.

Les fichiers provenant d'Internet englobent une diversité de contenus tels que des documents textuels(microsoft word),fichiers audio(mp3), des images(JPEG), des vidéos(AVI), des applications(EXE), et bien plus encore. Ces fichiers sont accessibles à travers des liens hypertexte, permettant aux utilisateurs de naviguer et de récupérer des informations depuis des sites web et d'autres sources en ligne.Néanmoins des fichiers malveillants existent et peut très vite devenir dangereux(prise de contrôle de votre poste, exfiltration de vos données ou encore des demandes de rançons)il faut donc faire très attention à ce que l'on télécharge.

La navigation Web est l'exploration des contenus d'Internet au moyen de navigateurs web. Ces logiciels permettent aux utilisateurs de naviguer entre elles, visualiser des pages web, de suivre des liens, d'interagir avec des éléments multimédias et d'accéder à une variété de services en ligne. Les navigateurs populaires incluent Chrome, Firefox, Safari et Edge. Il n'y a pas de bon, mauvais navigateurs, chacun a ses qualités et ses défauts. Il est surtout important de choisir un logiciel maintenu en conditions opérationnelles, c'est-à-dire proposant des corrections et des mises à jour régulières et donc de les appliquées.

La messagerie électronique occupe aujourd'hui une place centrale dans nos moyens de communications, elle offre un moyen de communication asynchrone via des courriers électroniques. Les utilisateurs peuvent envoyer et recevoir des messages, des pièces jointes, et organiser leurs communications de manière structurée sans avoir à se déplacer ou d'attendre que ce ou ces derniers soient disponibles. Les protocoles courants tels que SMTP et IMAP sont utilisés pour envoyer et recevoir des courriers électroniques. L'arrivée des réseaux à diminuer l'usage des courriels dans un cadre privé, mais la messagerie électronique est toujours très utilisée dans la sphère professionnelle. Malheureusement les messageries sont régulièrement ciblées par des démarchages indésirables de sites commerciaux mais aussi par des individus malveillants qui essaient d'obtenir des informations personnels ou faire exécuter différents types de logiciels malveillants(cheval de troie) en utilisant des techniques d'ingénierie sociale ou d'hameçonnage. Il est donc important de connaître les bonnes pratiques à adopter pour utiliser sa messagerie de façon sécurisée.

En coulisses, une connexion Web implique plusieurs composants. Lorsqu'un utilisateur accède à un site, un navigateur envoie des requêtes à un serveur web via des protocoles comme HTTP ou HTTPS. Le serveur répond en fournissant les données demandées. Cette interaction sous-jacente implique des adresses IP, des protocoles de sécurité (comme SSL/TLS), des serveurs DNS pour la résolution des noms de domaine, et d'autres éléments techniques garantissant une transmission efficace des données sur le réseau. Pour résumer, le navigateur doit connaître l'adresse du serveur web correspondant à l'aide d'un ou plusieurs serveurs DNS. Lorsque l'adresse IP est obtenue, le navigateur demande une page du site au serveur web. L'utilisation d'un serveur mandataire (ou proxy) peut vous permettre d'optimiser l'ouverture de pages web déjà consultées, d'améliorer la sécurité de vos navigations et d'empêcher une éventuelle infection.

Compte rendu du module 4:Sécurité du poste de travail et nomadisme

Le choix des applications à installer sur vos appareils informatiques, qu'il s'agisse de postes de travail, de tablettes ou de smartphones, doit être méticuleux, aligné sur les besoins réels, et éviter d'encombrer les systèmes. Il est primordial de privilégier les sources officielles des éditeurs lors du téléchargement et de s'abstenir d'installer des logiciels superflus. Pour maximiser la protection contre les vulnérabilités, il est impératif de procéder rapidement aux mises à jour suggérées par les éditeurs, idéalement dès leur disponibilité, afin de minimiser les impacts potentiels. L'utilisation des paramètres par défaut représente une première couche de sécurité, tandis que l'ajustement avancé des paramètres devrait être réservé à des individus plus expérimentés en matière de règles de filtrage réseau. Cependant, au-delà de toutes ces mesures, le facteur le plus critique demeure la vigilance et la mise en pratique du bon sens en permanence.

Pour garantir la sécurité de vos dispositifs, il est essentiel de mettre en place des configurations supplémentaires en complément des paramètres par défaut. Il devient crucial de créer des comptes distincts avec des niveaux d'autorisation spécifiques, de réaliser des sauvegardes régulières des données, de surveiller les différentes interfaces telles que le Wi-Fi, le NFC, le microphone, etc., et d'activer la fonction de verrouillage automatique sur les matériels. En outre, il est fortement recommandé de ne pas prêter votre téléphone afin d'éviter des altérations non contrôlées de vos données. Ces mesures viennent renforcer la protection globale de vos matériels en ajoutant des couches de sécurité essentielles pour prévenir tout accès non autorisé ou modification indésirable.

Les configurations de base d'un appareil constituent la première ligne de défense pour assurer sa sécurité et sa performance optimale. Ces paramètres essentiels, généralement inclus par défaut, visent à fournir une expérience utilisateur sécurisée dès la mise en service de l'appareil. Voici une synthèse des configurations de base :

-Paramètres Utilisateur : Configurez les préférences utilisateur de base, tels que le fond d'écran, les thèmes, et les langues, pour une personnalisation initiale.
-Réseau et Connexions : Établissez des connexions réseau sécurisées, configurez le Wi-Fi, et assurez-vous que le pare-feu est activé pour contrôler les flux de données.
-Sécurité du Compte : Créez un compte utilisateur avec un mot de passe robuste, et envisagez l'utilisation de l'authentification à deux facteurs pour renforcer la sécurité.
-Mises à Jour Automatiques : Activez les mises à jour automatiques du système d'exploitation et des applications pour maintenir la sécurité en intégrant les derniers correctifs.
-Application de Sécurité de Base : Installez des applications de sécurité de base telles que des antivirus et des logiciels anti-malware pour protéger contre les menaces potentielles.

Au-delà des configurations de base, les configurations complémentaires ajoutent des couches de sécurité supplémentaires et des fonctionnalités avancées pour renforcer davantage la protection de l'appareil. Voici une synthèse des configurations complémentaires à considérer :

-Chiffrement des Données : Appliquez le chiffrement sur le stockage de l'appareil pour garantir la confidentialité des données, particulièrement en cas de perte ou de vol.
-Contrôle d'Accès Réseau Avancé : Utilisez des pare-feu plus avancés pour contrôler finement les communications réseau, renforçant ainsi la sécurité des connexions.
-Authentification Multifactorielle : Activez l'authentification multifactorielle pour renforcer la sécurité des comptes et empêcher l'accès non autorisé.

-Politiques de confidentialité avancées : Configurez des paramètres de confidentialité plus avancés pour limiter la collecte de données par les applications et protéger la vie privée.
-Gestion des Applications : Mettez en place des restrictions d'installation d'applications en n'autorisant que celles provenant de sources fiables.
-Surveillance des Activités Suspicieuses : Utilisez des outils de surveillance pour détecter les activités suspectes et réagir rapidement en cas d'intrusion.
-Chiffrement des Communications : Appliquez le chiffrement sur les communications, en particulier lors de l'utilisation de réseaux publics, pour sécuriser les échanges de données.

En combinant ces configurations de base et complémentaires, les utilisateurs peuvent créer une défense complète contre les menaces numériques, tout en garantissant une expérience utilisateur fluide et sécurisée.

La sécurisation des périphériques amovibles, tels que les supports de stockage, est cruciale pour prévenir la perte de données et garantir la confidentialité. Pour ce faire, il est essentiel de sélectionner des supports fiables et adaptés à la durée de conservation souhaitée, tout en activant le chiffrement pour protéger les données en cas de perte ou de vol.
Créer au moins deux copies de sauvegarde sur des supports distincts offre une redondance de données en cas de défaillance. De plus, mettre en place des paramètres de contrôle d'accès, tels que des mots de passe, restreint l'accès non autorisé. L'utilisation de logiciels antivirus pour des analyses en temps réel lors de la connexion de périphériques amovibles aide à détecter les menaces potentielles.
Il est crucial de sensibiliser les utilisateurs à l'importance de la sécurité des périphériques amovibles, les encourageant à éviter les connexions avec des supports inconnus. En outre, au-delà de la simple suppression, l'application de méthodes d'effacement sécurisé, comme la réécriture multiple des données à l'aide d'outils spécialisés, assure une destruction complète et irréversible des informations.
Enfin, l'établissement de politiques d'entreprise régissant l'utilisation des périphériques amovibles, y compris des restrictions sur les types autorisés et des directives de sécurité, renforce la protection des données stockées sur ces supports. Une approche holistique de la sécurité des périphériques amovibles, intégrant sensibilisation, contrôle d'accès, chiffrement, et politiques d'entreprise, contribue à minimiser les risques potentiels associés à ces dispositifs.

Les usages et les mesures de sécurité associés aux environnements professionnels et personnels sont différents, c’est pourquoi il est fortement conseillé de séparer le matériel utilisé.De plus,selon l’ANSSI, les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, smartphone, etc.) personnels et professionnels. Il est donc vivement recommandé de séparer les usages personnels des usages professionnels : -Ne jamais utiliser vos équipements personnels pour travailler sur des projets sensibles. -Ne pas héberger de données professionnelles sur vos équipements personnels (clé USB, téléphone, etc.) ou sur des moyens personnels de stockage en ligne. -Éviter de connecter des supports amovibles personnels (clés USB, disques durs externes, etc.) aux ordinateurs de l’entreprise. -Respecter le cloisonnement (c’est-à-dire les infrastructures physiques et informatiques) mis en place par votre service informatique.

Définitions

-Botnet : réseau de terminaux infectés par un/des malwares , souvent à utilisation malveillante.

-Rançonnement : attaque malveillante à but de nuire au bon fonctionnement de leur terminaux afin de couper leur activité. Les pirates demandent alors une rançon en contrepartie d'un arrêt de l'attaque. Pour effectuer cette attaque, les pirates utilisent un rançongiciel.

-La défiguration de site (aussi parfois vu sous le terme « défacement » par anglicisme) consiste à modifier une partie d'un site web, affichant alors des éléments choisis par le pirate.

-MalVertising : le pirate intégrera du contenu malveillant sur des fausses publicités en ligne pour essayer de piéger les visiteurs de sites web sans passer par le propriétaire du site en question.

-l'ingénierie sociale (plus connue sous son nom anglais « social engineering ») désigne l'ensemble des attaques informatiques mettant l'accent sur les vulnérabilités humaines.Elle est souvent utilisée par les pirates pour arriver à leurs fins en parallèle d'attaques plus techniques. Ils ont recours à de nombreuses ruses qu'il convient de savoir déjouer autant que possible.

-L'hameçonnage ou le phishing consiste à obtenir du destinataire d'un courriel, d'apparence légitime, qu'il transmette ses coordonnées bancaires ou ses identifiants de connexion à des services financiers, afin de lui dérober de l'argent.

-Un fichier n'est fondamentalement qu'une suite de 0 et de 1 compréhensibles par l'ordinateur.

-L'extension, c'est le suffixe du nom du fichier, La convention veut que l'extension du fichier corresponde à son format, cela permet non seulement d'identifier rapidement le format du fichier mais aussi de lui associer un logiciel par défaut (c'est-à-dire le logiciel automatiquement choisi pour l'ouvrir).

-Internet désigne le réseau informatique qui relie par le biais du protocole de communication IP (Internet Protocol) des millions d'ordinateurs à l'échelle mondiale.

-Le World Wide Web ou Web désigne une des utilisations possibles d'Internet. Il a été inventé plusieurs années après Internet et désigne un système hypertexte public qui fonctionne sur Internet et permet de consulter des pages web et de naviguer entre elles via des hyperliens.

-L'objectif du « typosquatting » est de réserver un nom dont la typographie est proche d'un site officiel pour tromper l'utilisateur ou nuire à l'entité.

-Un cookie est un objet associé à un site web stocké sur l'ordinateur, qui permet à ce site de stocker des informations relatives au client et de récupérer ces informations lors d'une visite ultérieure du client.

-Navigation privée permet de limiter les traces de navigation laissées sur l'équipement lors de notre passage, mais attention elle ne préserve pas des menaces et on est encore loin de l'accès totalement anonyme sur le grand réseau Internet !C'est d'ailleurs généralement rappelé lors de l'activation de ce mode : votre fournisseur d'accès ou votre entreprise dispose toujours de traces des sites auxquels vous accédez.

->Un pourriel est une communication électronique non sollicitée.

-Le DNS (Domain Name System) est le nom d’un service hiérarchique distribué jouant le rôle d’annuaire pour Internet.

-vulnérabilité: une faille dans la conception, l’exécution ou la gestion d'un système informatique.

-Les « black hats » qui cherchent des failles pour les exploiter à des fins de malveillances ou de profits.

-Les « white hats » qui cherchent des failles pour les remonter aux éditeurs et fabricants afin qu’ils améliorent leurs outils.

-Pare-feu : blocage des connexions entrantes et sortantes du réseau.