Récapitulatif des principaux risques encourus

B

Cette annexe présente un bilan des risques que nous avons identifiés tout au long de l'ouvrage. Elle ne prétend pas à l'exhaustivité. Son principal objectif consiste à :

- donner un aperçu rapide des principales menaces qui pèsent directement sur un poste de travail ou un réseau informatique de taille modeste (pour plus de détails, nous vous renverrons aux chapitres concernés) ;
- identifier les conséquences potentielles sur le système si la menace se réalise ;
- proposer des mesures simples qui permettent de réduire significativement le risque.

Il convient de remarquer que cette annexe est adaptée à la problématique du poste de travail de l'utilisateur individuel et du petit réseau domestique ou d'entreprise. De nombreux aspects concernant les grands systèmes informatiques ne sont pas abordés ici. Si le lecteur souhaite se faire une vision plus complète, il peut se référer à la méthode EBIOS, disponible gratuitement à partir du site de la DCSSI.

Toutefois, le simple suivi des recommandations listées ci-après évitera bon nombre de catastrophes.

Erreurs d'utilisation

Voir le chapitre 1.

Comportement à risque	Conséquences	Mesures
L'utilisateur divulgue son mot de passe à un tiers.	Un inconnu peut alors usurper l'identité de l'utilisateur et s'introduire au cœur du système. * Divulgation, altération et/ou destruction d'informations sensibles (par exemple base des clients). * Ouverture possible de trappes cachées pour que l'attaquant puisse revenir ultérieurement.	Ne jamais donner son mot de passe à quelqu'un, même s'il s'agit en apparence d'un officiel (représentant de la banque, administrateur informatique...).
L'utilisateur choisit un mot de passe faible : « 12345678 », « azertyui », « password », « nathalie »...	Un pirate peut très facilement trouver la valeur du mot de passe et se connecter au système.	Dans tous les cas, choisir un mot de passe robuste (ex. « Fz5#Bs15 »).
Arrêt brutal du système d'exploitation ou d'une application. Interruption brutale d'un processus.	Altération de fichiers système : * Le système entre dans un état incohérent. * Certains fichiers sont corrompus. * Le système d'exploitation est détérioré ou ne démarre plus.	Ne jamais interrompre un processus en cours d'exécution. Ne jamais éteindre brutalement son poste. Quitter les applications proprement.
Suppression involontaire de fichiers situés sur un répertoire réseau.	Suppression définitive : les fichiers ne sont pas envoyés dans la corbeille. Ils ne peuvent être restaurés.	Toujours conserver une copie des données importantes en local. Sauvegarder les lecteurs réseau. Maîtriser les procédures de restauration.
Arrachage intempestif d'une clé USB au cours de l'édition d'un fichier stocké sur cette clé.	Fichier corrompu. Au pire, disparition du fichier.	Ne jamais travailler sur une clé USB.
L'utilisateur ne pense jamais à faire le ménage sur sa machine.	Les fichiers grossissent, finissent par « planter » l'application qui les gère et deviennent inaccessibles (c'est le cas notamment des messageries). Trop d'applications installées sur un poste peuvent entrer en conflit.	Penser à faire le ménage (au moins une fois l'an). Archiver les données anciennes sur supports externes (CD-Rom non réinscriptibles). Archiver la messagerie. Stocker les archives en lieu sûr. Désinstaller les applications dont on ne se sert plus.
Fichiers dotés de noms « à rallonge ».	Ils sont mal gérés par Windows : * mal copiés * pas toujours sauvegardés.	Toujours affecter un nom raisonnable à un fichier (moins de 30 caractères).
Le système affiche régulièrement un message d'erreur et l'utilisateur ne réagit pas.	Certains fichiers système sont peut-être corrompus, exposant l'utilisateur à une interruption de services et/ou à la perte d'informations. Une attaque est possible (un message d'erreur persistant est le symptôme de la présence possible d'un cheval de Troie).	Ne jamais traiter un message d'erreur par le mépris. Il faut résoudre le problème : * Contacter un administrateur. À défaut, se renseigner auprès d'une personne compétente de son entourage. * Faire appel au service d'assistance.
« Plantage » du système d'exploitation ou d'une application en cours d'utilisation.	Perte des données saisies depuis le dernier enregistrement.	Activer les fonctions d'enregistrement automatique.

Comportement à risque	Conséquences	Mesures
Incident logiciel : découverte en fin de journée que la fonction d'enregistrement ne fonctionne pas.	Perte d'une journée de travail.	Enregistrer le document dès son ouverture, avant de commencer l'édition. Effectuer des enregistrements fréquents.
Incidents réseau survenant lors de transferts massifs de données entre plusieurs machines (serveurs/serveurs, serveurs/clients).	Certains fichiers ne sont pas copiés. D'autres fichiers sont transférés mais restent illisibles. Interruption prématurée du processus de transfert.	Le câblage du réseau doit respecter les normes et les caractéristiques des constructeurs (câbles de bonne qualité, architecture, environnement...). Éviter les perturbations électromagnétiques (chemins de câbles près des néons...) Vérifier systématiquement le déroulement des transferts (comparaison nombre/volume fichiers et répertoires entre source et destination). En cas de rénovation du parc, conserver les anciens serveurs, au moins pendant une période transitoire.
Forcer une application à exécuter des tâches « tordues » augmente le risque de la faire « planter ».	Les fichiers en cours d'édition peuvent être endommagés ou perdus. L'application entre dans un état incontrôlé et peut « planter « le système.	Ne jamais forcer une application à exécuter des tâches pour lesquelles elle n'est pas prévue.
Perte d'un périphérique de stockage amovible (CD-Rom, clé USB, balladeur MP3...).	Perte de données précieuses. Divulgation externe de données confidentielles.	Plusieurs copies de sauvegardes des données stockées sur la clé USB (CD-Rom, disque réseau, disque dur externe, bande...). Chiffrement des fichiers sensibles stockés sur le support (ex. GnuPG).

Sauvegardes

Voir le chapitre 1.

Comportements à risque	Conséquences	Mesures
L'utilisateur ne sauvegarde pas ses données.	Une donnée non sauvegardée finit par disparaître tôt ou tard.	S'assurer que des procédures de sauvegarde ont été définies et sont claires pour les acteurs concernés. Toujours disposer de plusieurs sauvegardes : * bande magnétique (plutôt entreprises) ; * CD-Rom réinscriptible (données récentes) ou non réinscriptible (archives); * disque réseau et disque local ; * disque externe ; * clés USB (uniquement les sauvegardes temporaires avant la sauvegarde sur disque).

Comportements à risque	Conséquences	Mesures
L'utilisateur ne sait pas toujours où sont rangées certaines données importantes : * la messagerie ; * les données gérées par les applications (photos, morceaux de musique...) ; * le bureau ; * les favoris.	Ces données.ne sont pas toujours correctement sauvegardées et finissent par se perdre.	Bien penser la stratégie de sauvegarde. Apprendre où sont rangées ces données précieuses sur le disque. Savoir éventuellement mettre en œuvre les fonctions de sauvegarde proposées par les applications. Si utilisation d'un système de sauvegarde spécifique, définir une politique de sauvegarde prenant en compte les répertoires hébergeant ces données.
Perte/oubli des paramètres vitaux ouvrant l'accès à l'espace de travail (ces paramètres sont souvent mémorisés par le système) : * mots de passe du compte sur la machine ; * paramètres système ; * mots de passe d'accès aux ressources du réseau ; * paramètres d'accès à la messagerie ; * hébergeur...	L'espace de travail de l'utilisateur est inaccessible tant qu'il n'a pas retrouvé ces informations. Perte définitive de l'accès si l'utilisateur travaille sur le seul compte de la machine (compte administrateur) et que le mot de passe n'a été noté nulle part.	Conserver soigneusement dans un lieu sûr les éléments utiles et toutes les données importantes sans lesquels il n'est plus possible de travailler normalement.
L'obésité du système est un facteur de « plantage » et de perte d'information.	Perte de temps. Perte de données vitales.	Définir et mettre en œuvre une procédure d'archivage adaptée. Prévoir des mesures de conservation des archives adaptées aux délais de rétention.

Restauration

Voir le chapitre 1.

Comportement à risque	Conséquences	Mesures
Ignorance du mode opératoire des procédures de restauration.	En cas de perte d'information, les sauvegardes ne sont d'aucun secours.	Définir clairement les procédures de restauration. Se familiariser avec les procédures de restauration. Apprendre à restaurer complètement des données (par exemple une messagerie).
Les données sauvegardées sont inexploitables.	En cas de perte d'information, celles-ci seront irrécupérables.	Toujours vérifier et valider la procédure de sauvegarde.

Pannes

Voir le chapitre 1.

Problème	Conséquences	Mesures
« Plantage » inopiné de la machine en cours de travail. Panne secteur ou extinction intempestive de la machine pour quelque raison que ce soit.	Perte des données saisies depuis le dernier enregistrement. Fichiers en cours d'édition/fichiers système endommagés.	Réseau d'entreprise : alimentation de secours obligatoire sur les serveurs (onduleurs).
Le système ne démarre plus.	Indisponibilité momentanée ou définitive du système et des données qu'il renferme.	Savoir identifier l'origine d'une panne. Se familiariser avec les procédures de récupération du système. Se préparer à réparer un système endommagé : * Savoir activer la dernière bonne configuration connue. * Se familiariser avec le mode sans échec. * Connaître l'existence des plans de récupération offerts par les systèmes d'exploitation et savoir les exploiter.

Configuration du poste de travail

Voir le chapitre 2.

Attaque risquée	Conséquences	Mesures
Accès non contrôlé à la machine de l'utilisateur (par exemple machine libre service ou sans mot de passe).	Accès illicites : * aux données contenues sur la machine ; * au réseau et aux serveurs de l'infrastructure (intranet). Atteinte possible à la confidentialité, l'intégrité et la disponibilité des données et des services. Modification illicite de la configuration du système (par exemple ouverture de trappes cachées pour accroître les possibilités d'accès non autorisés).	Créer des comptes d'utilisateurs et leur affecter des mots de passe robustes. Activer l'écran de veille et protéger la sortie de veille avec un mot de passe robuste. En entreprise : * proscrire toute forme de naïveté ; l'espionnage économique peut venir de l'intérieur (par exemple stagiaire, consultant extérieur, sous-traitant) ; * allouer des droits d'accès aux utilisateurs ; * supprimer les comptes d'utilisateurs ayant quitté la société ; * activer la journalisation des événements ; * auditer l'activité des systèmes et du réseau.

Attaque risquée	Conséquences	Mesures
Connexion non autorisée sur une machine en usurpant l'identité d'un utilisateur reconnu.	Accès illicite à l'espace de travail de l'utilisateur et aux ressouces du réseau. Divulgation externe d'informations sensibles. Altération, modification frauduleuse d'informations utilisateur et système. Atteintes possibles à la disponibilité des données, des services et du système.	Définir des mots de passe robustes : * protéger l'accès aux comptes d'utilisateurs ; * protéger l'accès aux ressources partagées et au réseau. Saisir le mot de passe à l'abri des regards indiscrets. Définir une procédure de changement régulier des mots de passe. En entreprise, auditer l'activité des systèmes et du réseau.
Volumes non formatés NTFS.	De nombreuses fonctions de sécurité ne peuvent être activées, dont : * fonctions plus élaborées d'affectation de droits et de contrôle d'accès aux données ; * fonctions natives de chiffrement EFS.	Penser à formater les volumes en NTFS, si cette opération n'a pas déjà été effectuée en usine.
Exploitation frauduleuse des partages ouverts sur un ordinateur.	Recenser les ressources actives, les réseaux, obtenir une liste valide d'utilisateurs autorisés. Accéder sans autorisation à des ressources partagées. Divulgation externe, modification et/ou destruction de données accessibles sur les partages. Pénétrer une organisation en profondeur.	Définir des mots de passe robustes pour protéger l'accès aux ressources partagées. Inspecter régulièrement les partages actifs et fermer ceux qui ne sont pas nécessaires. Réduire au strict minimum les permissions associées à un partage. Désactiver impérativement les services SMB sur les interfaces avec les réseaux non sûrs (Internet).
Manipulation frauduleuse du registre par un exécutable malveillant.	Contamination de la machine par un virus, un cheval de Troie ou un logiciel espion. Ouverture de canaux cachés. Prise de contrôle de l'ordinateur à distance. Atteinte au bon fonctionnement de l'ordinateur.	Vérifier, maîtriser les permissions associées aux objets du Registre. Ne jamais travailler sous un compte doté des droits administrateur. Vigilance : veiller à installer sur son poste des exécutables de provenance fiable. Un pare-feu logiciel sachant détecter les applications qui tentent de modifier le registre. Un antivirus à jour.
Éplucher l'historique des actions réalisées par un utilisateur sur son poste.	Espionner l'activité de l'utilisateur	Vider les historiques et désactiver les mouchards.
Exploitation malveillante d'une vulnérabilité logicielle.	Système d'exploitation soumis à des requêtes mal formées : * exécution/installation à distance de codes arbitraires ; * prise de contrôle à distance de l'ordinateur.	Procéder à la mise à jour permanente du système d'exploitation et des logiciels installés sur le poste. Un antivirus/antispyware à jour. Réseau d'infrastructure : pare-feu matériel doté de fonctions d'analyse des contenus véhiculés par les protocoles Internet (HTTP, SMTP, DNS...).

Attaque risquée	Conséquences	Mesures
Exploitation malveillante de protocoles peu sécurisés, ou pas sécurisés du tout.	Interception d'informations sensibles (mots de passe) transitant via des flux non chiffrés. Accès non autorisé au poste et à l'infrastructure informatique. Intrusion du réseau.	Désactiver tous les services réputés dangereux ou inutilisés (SNMP, Telnet, TFTP, ICMP...). Opter pour l'utilisation de protocoles sécurisés (par exemple SSH au lieu de Telnet).
Vol de l'ordinateur (menace élevée dans le cas des postes nomades)	Atteinte à la confidentialité de données sensibles. Risque de chantage, d'extorsion de fonds à l'encontre de l'entreprise. Perte de données précieuses.	Ne pas attirer l'attention, transporter l'ordinateur dans une serviette banalisée. Chiffrer les fichiers et/ou les dossiers sensibles : * système natif Windows (EFS) pour un chiffrement de premier niveau ; * utilisation de GnuPG (sécurité forte si gestion rigoureuse) ; * pour les fichiers très sensibles, envisager un produit de sécurité spécialisé avec chiffrement du disque à la volée. Authentification forte de l'utilisateur au démarrage de la machine, avec dispositif matériel externe (cartes à puce, clé USB).

Virus, vers, Troyens et logiciels espions

Voir les chapitres 3 et 4.

Attaque risquée	Conséquences	Mesures
Installation non contrôlée d'un code malveillant au cœur de l'ordinateur (message électronique infecté, exécutable de provenance douteuse...). Lancement automatique de ce code malveillant à chaque démarrage de la machine (par exemple suite à une modification non autorisée du registre).	Le virus est résident. Son pouvoir de nuisance est multiple : * interception des appels système ; * altération, destruction partielle ou totale du système de fichiers ; * transformer la machine en un relais pour lancer des attaques ultérieures (par exemple DDoS-Distributed Deny of Service).	Adopter avant tout un comportement prudent. Ne jamais travailler sous le compte Administrateur. S'assurer que les utilisateurs de la machine disposent d'un accès limité au registre. Pare-feu logiciel capable de détecter les modifications du registre. Un antivirus/antispyware à jour.
Le code malveillant active le téléchargement et l'installation de codes arbitraires à travers des canaux cachés.	Machine sous le contrôle d'une entité distante.	Pare-feu logiciel capable de : * détecter la modification d'exécutables (applications, commandes système) ; * signaler les processus qui tentent de réaliser des actions suspectes (ouvertures de connexions Internet, manipulation d'applications). Un antivirus/antispyware à jour.

Attaque risquée	Conséquences	Mesures
Modification par le code malveillant de certains exécutables présents sur la machine.	Pervertir le fonctionnement de l'ordinateur, servir les intérêts du virus (par exemple désactiver l'antivirus ou son système de mise à jour, intercepter les appels système, modifier les fonctions d'affichage pour camoufler sa présence).	Pare-feu logiciel capable de détecter la modification d'exécutables (applications, commandes système). Un antivirus/antispyware à jour.
Ouverture illicite de ports sur la machine pour recevoir et traiter des commandes lancées par l'attaquant à distance.	Prise de contrôle partiel ou total de la machine à distance. Divulgation externe, altération, destruction d'informations sensibles. Transformation du poste de travail en une base avancée pour lancer une attaque au cœur du réseau (infiltration, saturation des ressources).	Sauvegarde régulière des données. Pare-feu logiciel apte à détecter les comportements suspects des processus. Vigilance de l'utilisateur : inspection régulière de la configuration du pare-feu. Un antivirus/antispyware à jour.
Envoi en masse de messages à tous les utilisateurs répertoriés dans le carnet d'adresses.	Propagation du ver. Contamination possible d'autres utilisateurs. Pollution de la messagerie.	Un antivirus à jour, configuré pour détecter les tentatives d'envoi massif de courriers électroniques.
Observation du comportement de l'utilisateur. Envoi de rapports détaillés à des inconnus. Divulgation des informations sensibles à l'extérieur.	Espionnage.	Toutes les mesures citées précédemment. Un antispyware à jour.

Installation hasardeuse de logiciels « attractifs »

Voir les chapitres 3 et 4.

Attaque risquée	Conséquences	Mesures
Infection de la machine par de multiples chevaux de Troie.	Le PC devient partiellement ou totalement sous contrôle d'une entité extérieure. Le réseau local (domestique ou d'entreprise) est menacé. Divulgation à l'extérieur d'informations sensibles.	Ne jamais installer de logiciels issus d'une source non digne de confiance. Un antivirus/antispyware à jour.

Attaques réseau

Voir les chapitres 5 et 6.

Attaque risquée	Conséquences	Mesures
Un protocole de communication, quel qu'il soit, peut être détourné pour véhiculer un flux malveillant.	Attaques en tous genres du poste utilisateur. Attaques en tous genres du réseau informatique (domestique ou entreprise).	Fermer systématiquement sur la machine tous les services inutiles. Désactiver systématiquement les services dangereux sur toutes les interfaces avec les réseaux non sûrs (NetBIOS, SNMP, ICMP, Telnet, TFTP). Pare-feu indispensable dès que le poste ou le réseau est relié à un réseau non sûr : * pare-feu logiciel sur chaque poste (contrôle des flux entrants et sortants, de l'intégrité et du comportement des applications) ; * pare-feu matériel en entrée de site doté de fonctions d'analyse de contenus. Un antivirus/antispyware à jour.
Présence d'un accès à distance aux systèmes et réseaux locaux (ressources partagées, accès non protégés, télé-maintenance, externalisation des sauvegardes).	Risque accu de pénétration extérieure du réseau et des systèmes informatiques. Vol, modification et/ou destruction de données. Saturation des ressources système et réseau (déni de service).	Désactiver tout lien « remote » permanent. Tout échange entre un poste extérieur (nomade, sauvegarde externe, télé-maintenance) doit impérativement : * emprunter un canal établi à la demande ; * passer par un tunnel chiffré (lien de type VPN) ; * s'effectuer au sein d'une communauté d'utilisateurs clairement identifiés ; * débuter par une authentification forte de l'utilisateur distant, basée sur des moyens cryptologiques implémentés dans un dispositif matériel (carte à puce, clé USB).
Poste nomade plus exposé en dehors du périmètre de l'entreprise.		Être sensibilisé aux attaques informatiques et aux comportements dangereux qu'il faut éviter. Pare-feu logiciel indispensable (contrôle étroit des flux échangés et des applications demandant l'accès à Internet). Un antivirus/antispyware à jour.

Menaces liées aux codes mobiles

Voir le chapitre 7.

Attaque risquée	Conséquences	Mesures
Installation non contrôlée de codes mobiles malveillants sur le poste (par exemple via la consultation de pages HTML à partir de sites peu dignes de confiance).	Rapatriement/installation non contrôlée de codes mobiles sur le poste (ActiveX, applets Java, Javascript), en provenance d'horizons multiples sur Internet. Ouverture de trappes cachées. Accès illicite au système de fichiers (divulgation externe, altération et/ou destruction de données). Accroissement de la vulnérabilité du poste face aux attaques. À terme, contamination assurée du poste par une multitude de codes furtifs, Troyens ou logiciels espions.	Vigilance de l'utilisateur. Configurer le navigateur pour désactiver systématiquement tous les codes mobiles, Java et JavaScript, à l'exception des sites identifiés nominativement par l'utilisateur. Sur ces sites, autoriser uniquement les composants qui représentent potentiellement le moins de risques pour l'ordinateur : * composants authentifiés avec « Authenticode ». * composants reconnus « Sûrs pour l'écriture de scripts ». Refuser tous les autres.
Le code mobile établit et entretient des communications illicites avec des sites dangereux via les protocoles autorisés du pare-feu. Il établit des de tunnels chiffrés (non contrôlables par un pare-feu) entre le poste utilisateur situé au cœur du réseau et un site distant arbitraire.	Le pare-feu devient inopérant face aux protocoles de haut niveau encapsulés à l'intérieur de protocoles standards (HTTP, SMTP, DNS). Le pare-feu ne sait pas filtrer les protocoles chiffrés. Intrusion sur poste à travers le pare-feu. Toutes les opérations sont envisageables : * rapatriement d'autres codes malveillants ; * accès au système de fichiers (divulgation externe, altération, destruction de données) ; * contrôle à distance des actions de l'utilisateur...	Un pare-feu logiciel sachant détecter les comportements suspects des applications et les tentaives d'ouvertures de ports. Inspection régulière de la configuration du pare-feu (vérification des communications sortantes autorisés). Interdire a priori toutes les communications entrantes, en particulier la messagerie instantanée. Un antivirus/antispyware à jour.
Exécution en local de commandes lancées à distance par un site pirate (protocole spécifique transitant via les flux non filtrés par le pare-feu).	Exécution à la demande d'opérations voulues par le pirate : * divulgation externe de fichiers confidentiels ; * saturation du réseau local (domestique ou d'entreprise) ; * téléchargement à distance d'autres exécutables...	Vigilance de l'utilisateur : * éviter à tout prix de se retrouver dans cette situation (appliquer les mesures précédentes) ; * inspection de la configuration du pare-feu ; * suivi des processus ; * exploitation des journaux du pare-feu. Pare-feu logiciel capable de détecter et de contrôler : * l'installation de nouvelles applications ; * les modifications du registre ; * les actions suspectes.

Menaces directement liées aux problèmes de la navigation sur le Web

Voir le chapitre 7.

Attaque risquée ou comportement dangereux	Conséquences	Mesures
Consultation de pages HTML dynamiques.	Rapatriement possibles de codes mobiles en provenace d'horizons très différents.	Voir section « Menaces liées aux codes mobiles ».
Téléchargement/installation/utilisation par l'internaute d'exécutables et applications d'origines les plus diverses (utilitaires, jeux).	L'ordinateur devient un cheval de Troie au cœur du réseau informatique (domestique ou entreprise). Infiltration du réseau informatique. Attaque par saturation des ressources (Déni de service).	Vigilance accrue de l'utilisateur : * sensibilisation de l'utilisateur aux risques pesant sur le système d'information, aux méthodes d'attaque, aux problèmes de sécurité potentiels ; * définition et suivi de la charte pour une utilisation sûre de l'outil informatique. Pare-feu logiciel et/ou matériel en entrée de site : * règles de filtrage adaptées ; * détection des tentatives de connexion suspectes vers Internet. Suivi de l'activité du réseau (volume des flux, origine).
Attaque par langage de script d'un site distant (Cross Site Scripting) : visitant un site de confiance, l'utilisateur est redirigé à son insu vers un site pirate au moment de livrer des informations sensibles.	Divulgation d'informations sensibles.	Vigilance de l'utilisateur : toujours vérifier l'authenticité d'un site avant de livrer des information sensibles.
Exploitation malveillante des vulnérabilités du navigateur (débordements de tampons).	Prise à distance du contrôle de l'ordinateur. Installation à distance de codes arbitraires sur le poste de l'utilisateur.	Maintenir systématiquement à jour les système d'exploitation et applications. Un antivirus/antispyware à jour.
Phishing : stratagème bien huilé conçu pour piéger l'utilisateur trop crédule.	L'utilisateur trop confiant dévoile ses codes secrets à un tiers.	Sensibilisation de l'utilisateur aux problèmes classiques de « social engineering » (baratinage). Ne jamais répondre à un message où l'on demande à l'utilisateur d'entrer ses codes secrets (même si le message semble provenir d'une source de confiance). C'est un faux dans tous les cas.
Détournement des protocoles mal gérés par les pare-feux.	Infiltration du réseau local. Injection à distance de codes malveillants. Chantage, racket.	En milieu professionnel, éviter systématiquement les sites peer-to-peer et les messageries instantanées. Éviter systématiquement tous les sites mafieux (pornographie, pédophilie).

Cookies

Voir le chapitre 7.

Attaque risquée	Conséquences	Mesures
Vol des cookies sur la machine de l'internaute.	Les informations personnelles de l'internaute sont connues du pirate. Usurpation de l'identitité de l'internaute par le pirate. Rejeu par le pirate d'une session de navigation de l'internaute (sur un site bancaire par exemple).	Configurer le navigateur pour désactiver systématiquement tous les cookies, à l'exception des sites identifiés nominativement par l'utilisateur. Refuser les cookies permanents. Effacer tous les cookies de l'ordinateur.

Messagerie

Voir le chapitre 8.

Attaque risquée	Conséquences	Mesures
Réception d'un message porteur de virus en pièce jointe. L'utilisateur effectue un clic malheureux sur la pièce jointe.	La machine est infectée par le virus.	Ne jamais ouvrir la pièce jointe d'un message, à moins d'être absolument sûr de sa provenance (attention à l'usurpation d'identité !). Un antivirus/antispyware à jour. Filtrage de contenus actifs sur le pare-feu logiciel ou le pare-feu matériel en entrée de site (blocage des fichiers .zip, .exe, .com, .src, .lnk, .bat, .vbe, .js, .vbs, .cmd, ou .cpl).
Réception d'un message porteur d'un virus sachant exploiter une vulnérabilité du client de messagerie ou du navigateur.	La machine est infectée par le virus, sans qu'il y ait forcément intervention de l'utilisateur.	Tenir son client de messagerie et son navigateur à jour. Suppression immédiate des messages de provenance inconnue, sans les ouvrir. Un antivirus/antispyware à jour.
Réception d'un message émanant d'une « source officielle », demandant à l'utilisateur de saisir des informations personnelles.	Divulgation de codes secrets à des inconnus. Ce type de message est un faux (phishing).	Ne jamais répondre à un message demandant à l'utilisateur de saisir des informations personnelles.
Flux de messagerie non chiffrés (courrier électronique et messageries instantanées).	Divulgation d'informations confidentielles à des tiers.	Chiffrer la messagerie avec des mécanismes fiables (GnuPG, utilisation des certificats...). Si la messagerie ne peut être chiffrée, s'abstenir d'échanger des informations confidentielles par ce canal.
Messagerie chiffrée par le fournisseur.	Divulgation d'informations confidentielles : le niveau de sécurité dépend du niveau de confiance accordé au fournisseur.	Si les messages sont potentiellement sensibles (cadre dirigeant d'une entreprise), opter pour un fournisseur de confiance (un fournisseur national traitant les messages sur le territoire national).

Spams

Voir le chapitre 8.

Attaque risquée	Conséquences	Mesures
Découverte d'adresses valides de messagerie, stockage de ces adresses dans des listes de spam.	L'internaute est bombardé de spams.	Ne jamais publier, telle quelle, son adresse de messagerie sur une page web. La publier sous forme d'image. Ne pas affecter à cette image de lien de type « mailto:monAdresse » ! Se faire attribuer des adresses « jetables » pour réaliser les opérations qui nécessitent une adresse électronique. Se faire attribuer des addresses difficiles à deviner (comme ast_784@barycentre.fr).
Bombardement de l'internaute.	Encombrement de la messagerie, gêne à l'utilisation. Risque accru de contamination du poste par un code malveillant (virus, ver, cheval de Troie, logiciel espion). Exposition plus élevée au phishing.	Ne jamais ouvrir un message non sollicité. Utilisation de clients de messagerie dotés de filtres antispam performants (Thunderbird). Lorsque le problème devient incontrôlable : * changer d'adresse de messagerie et repartir sur un bon pied (suivre les mesures ci-dessus). Envisager à l'extrême limite l'acquisition d'un produit spécialisé antispam. Un antivirus/antispyware à jour.

Menaces liées au Wi-Fi

Voir le chapitre 4.

Attaque risquée	Conséquences	Mesures
Écoute du trafic échangé par voie radio entre le poste utilisateur et le point d'accès.	Atteinte à la confidentialité des données échangées.	Sécurisation SSL/HTTPS entre le poste et le site distant. Activation du chiffre WPA2 (à la rigueur WPA) entre le poste et le point d'accès.
Accès illicite au poste utilisateur par la voie radio.	Accès au système de fichiers de l'utilisateur avec toutes les conséquences qui en découlent (divulgation externe, altération et/ou destruction de données). Infiltration du réseau informatique « par la voie des airs », en dépit des éventuelles protections du réseau filaire (pare-feu, DMZ, etc.).	Désactiver l'accès Wi-Fi tant que l'on ne s'en sert pas. Pare-feu logiciel indispensable sur le poste, avec contrôle de l'activité des applications. Activation du chiffre WPA2 (à la rigueur WPA)) entre le poste et le point d'accès. Un antivirus/antispyware à jour.

Glossaire

Il est important de bien connaître les différents types d'attaques qu'un pirate est susceptible de lancer à l'encontre de votre machine. Ainsi vous sera-t-il plus facile de mettre en place les solutions adéquates pour protéger vos données.

Références **Attaques**

Le lecteur désireux d'en savoir-plus sur les attaque pourra se référer à l'ouvrage suivante :

📖 *Halte aux Hackers 4éme édition*, Éditions Eyrolles, 2003.

- **Attaque de l'homme du milieu**

  Man in the middle, attaque du singe intercepteur

  Lorsque deux machines échangent des informations via un réseau de télécommunication, le pirate s'insère entre elles à leur insu et réussit à intercepter, voire modifier leur messages. Se faisant passer pour l'une des parties, il peut obtenir de précieux renseignements.

- **Attaque cryptologique par force brute**

  En possession d'un morceau du message chiffré, le pirate essaie toutes les clés possibles jusqu'à tomber sur le message en clair correspondant. Si votre clé a une longueur de 40 bits, le pirate devra effectuer 2^{40} opérations pour essayer toutes les clés (en moyenne, la moitié suffira). Avec la technologie actuelle, casser une clé de 40 bits est très faisable. En revanche, si vous utilisez une clé de 128 bits, il faudrait en théorie « mouliner » pendant une durée supérieure à la durée de vie de l'Univers.

- **Balayage de ports**

  Connaissant l'adresse IP d'une machine, l'attaquant essaye d'entamer une session TCP sur chacun de ses 65 535 ports. Les réponses obtenues le renseignent sur les applications de communication qui « tournent » sur cette machine. Un balayage est souvent suivi d'une attaque plus précise visant un service actif spécifique.

- **Commande NBNS pour connaître des noms valides de domaines et d'utilisateurs**

  ```
  net view /domain:NomDeDomaine
  ```

- **Commandes SMB pour établir une connexion nulle avec un partage masqué**

  ```
  net use \\NomDeMachine\IPC$ "" /u:""
  net use \\NomDeMachine\C$ "" /u:""
  net use \\NomDeMachine\Admin$ "" /u:""
  ```

- **Commande telnet pour connaître une version de logiciel**

  En lançant la commande `telnet www.votreSiteWeb.com 80`, le pirate reçoit un message d'erreur mentionnant le nom et la version du logiciel de votre serveur web.

- **Commande TFTP pour accéder à des informations sensibles**

  ```
  get configFichier.cfg
  ```

- **Cross Site Scripting (XSS)**

  Attaque d'un site distant via un langage de script : l'utilisateur charge la page web d'un site de confiance, au sein de laquelle un pirate est parvenu – de diverses manières, les moyens ne manquent pas ! – à injecter un script malveillant. Ce script est alors exécuté par le navigateur de l'utilisateur. Généralement conçu pour rediriger vers le site du pirate, l'utilisateur est invité à saisir des informations confidentielles (son nom, son mot de passe, etc.), qui tombent désormais en possession du pirate.
- **Débordement de tampon**

  Le pirate provoque l'exécution d'un code malveillant en envoyant à un programme légitime une commande contenant trop de données. S'il provoque un débordement de tampon, le pirate peut accéder au répertoire racine de la machine avec des droits administrateur.
- **Déni de service distribué**

  Distributed Deny of Service (DDoS)

  Attaque par inondation dirigée contre un ordinateur ou un réseau d'ordinateurs (par exemple les serveurs d'une entreprise). Réalisée par des milliers d'ordinateurs agissant de concert (généralement par l'intermédiaire d'Internet), cette attaque vise à saturer les ressources des serveurs de la victime afin de les rendre indisponibles.
- **Détournement des protocoles chiffrés**

  Un cheval de Troie préalablement installé établit une communication chiffrée avec le pirate, grâce à laquelle ce dernier peut prendre possession de la machine distante à l'insu du pare-feu.
- **Écoute Wi-Fi**

  Grâce au Wi-Fi, le pirate peut écouter tout ce que vous échangez, pénétrer sur votre machine, et même infiltrer votre réseau si votre machine y est branchée.
- **Encapsulation de protocole**

  Le pirate utilise un protocole autorisé par le pare-feu (HTTP, DNS, FTP, SMTP...) pour transporter un autre protocole aux fins moins avouables, qu'un cheval de Troie préalablement infiltré saura exploiter.
- **Exploitation du TTL (Time To Live)**

  Le pirate envoie un message constitué de plusieurs paquets. Le premier paquet a un TTL de 1, le deuxième de 2, le troisième de 3, etc. Chacun des routeurs situés sur la route du message vers son destinataire renvoie alors un message ICMP `TIME EXPIRED`, informant ainsi le pirate à la fois de son existence et de son adresse IP. Comme il y a de grandes chances pour que le dernier routeur sur le chemin soit

celui d'entrée du réseau abritant le destinataire, le pirate sait maintenant vers quelle machine tourner son attaque.

- **Injection SQL**

  Un site s'appuyant sur une base de données relationnelle reçoit comme commandes des requêtes SQL. Si les paramètres de ces requêtes ne sont pas correctement contrôlés, le pirate peut les modifier pour s'octroyer le contrôle total sur la base.

- **IP spoofing**

  Usurpation d'adresse IP.

  Le pirate utilise frauduleusement l'adresse IP d'une machine « autorisée » et se fait passer pour elle pour obtenir des informations confidentielles.

- **Phishing**

  Le terme « phishing », ou « hameçonnage » en français, est issu de la contraction de deux termes : « phreaking », le piratage des centraux téléphoniques, et « fishing », aller à la pêche. « En informatique, l'hameçonnage, ou phishing en anglais, est un terme désignant l'obtention d'informations confidentielles (comme les mots de passe ou d'autres informations privées), en se faisant passer auprès des victimes pour quelqu'un digne de confiance ayant un besoin légitime de l'information demandée. »

  http://fr.wikipedia.org/wiki/Phishing

- **PHF**

  Attaque aujourd'hui dépassée, lorsque le serveur web recevait la commande suivante :

  ```
  /cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
  ```

  il renvoyait tout bonnement au pirate le fichier contenant la liste des identifiants utilisateurs et des mots de passe chiffrés (pour le pirate averti, retrouver ensuite les mots de passe en clair n'était pas très compliqué).

- **Ping de la mort**

  Cette attaque consistait à envoyer des paquets IP trop grands (plus de 65 536 octets) pour faire « planter » une machine distante. Avec les systèmes actuels, elle est désormais obsolète.

- **Téléchargement de codes mobiles**

  Le pirate télécharge télécharge sur votre poste, en même temps que les pages web, de façon transparente et totalement à votre insu, des codes exécutables de toutes sortes, dont des codes malveillants.

- **Violation de répertoires**

Directory traversal

Lorsqu'un programme s'exécute sur un serveur, il le fait avec des droits restreints à certains répertoires seulement. Par diverses ruses, le pirate réussit à en « sortir » et à obtenir l'accès à des répertoires sensibles de la machine, d'où il peut provoquer de gros dégâts.

- **Vol de session**

  TCP hijacking.

  Lorsque deux machines initient une session TCP, le contrôle d'authentification n'est effectué qu'à l'ouverture de la session. En jouant habilement sur les numeros de séquence, le pirate peut détourner la session et prendre le contrôle de la connexion.

- **Wardriving**

  Écoute Wi-Fi

  Le pirate se déplace en voiture avec un matériel spécial pour tâcher de capter les réseaux Wi-Fi qu'il pourrait infiltrer.