Chapitre 1
Introduction

1. Préambule

Les réseaux et les systèmes informatiques deviennent de plus en plus complexes et de plus en plus grands. Ils sont pour certaines entreprises un mal nécessaire et ce qui pourrait être un investissement se transforme en un gouffre. De cette image, découle souvent un très petit intérêt à augmenter le budget de la sécurité informatique. Les administrateurs, eux, ont de nos jours beaucoup de travail et de préoccupations. Ils sont mis sous pression pour obtenir des résultats rapides en matière de déploiement ou de maintenance. Ils n'ont donc pas le temps d'aller dans les détails lors de l'installation d'un produit ou d'une application. Ils sont malheureusement parfois obligés de faire au plus vite puis de s'arrêter au moment où cela fonctionne, sans avoir pris le temps d'en analyser la sécurité avant ou après l'installation. De plus, la sécurité intérieure est souvent négligée au détriment d'une protection d'une éventuelle menace externe.

Pourtant, si la sécurité était parfaite à l'intérieur, que pourrait vraiment faire un hacker externe ?

Différentes études montrent que la sécurité informatique d'une entreprise est dans la plupart des cas aisément attaquable de l'intérieur, mais elles montrent aussi une nette augmentation de ce type d'incidents, que ce soit par des utilisateurs gourmands ou frustrés par le manque de pouvoir ou par des personnes ayant des intentions négatives telles que la vengeance, l'espionnage, le vol ou la destruction d'informations critiques ou privées. La réalité est ainsi, des techniques de hacking sont régulièrement employées à ces fins, les avez-vous constatées chez vous ?

Dans une entreprise, les utilisateurs n'ayant pas de fonction d'administration informatique ont la plupart du temps des droits limités sur leur PC. Et cela a pour but de protéger la machine contre une installation de programme pouvant mettre en danger le réseau ou n'entrant pas dans la politique de sécurité, si bien sûr une telle politique existe. Cela a aussi pour objectif d'éviter à un employé d'être manipulé malgré lui par un pirate interne ou externe. Il est donc normal de ne laisser à un utilisateur que les droits nécessaires à l'utilisation des logiciels prévus par sa fonction.

Toutefois, il existe des outils pour contourner cette attribution de rôle pour à son tour pouvoir tout faire de son PC ou d'un serveur. Il est même possible d'aller plus loin, par exemple, d'obtenir les droits systèmes sur une machine ou de devenir administrateur d'un domaine complet. Certains moyens sont purement techniques et d'autres nécessitent en plus d'agir sur l'humain pour obtenir les autorisations recherchées.

Pour simplifier l'action des pirates, il n'est pas rare de voir des responsables informatiques donner plus de droits que nécessaire, sans pour autant prendre en compte les risques auxquelles ils s'exposent. Il arrive fréquemment que dans une entreprise, tous les utilisateurs soient administrateurs de leur PC, ce qui donne une voie royale pour réaliser des actions de piratage efficaces.

De plus, les mécanismes de sécurité mis en place par Microsoft sont parfois mal compris. Ceux qui sont considérés comme lourds ou intrusifs sont souvent désactivés ou non configurés pour simplifier le travail. Sans ces protections pourtant activées par défaut comme l'UAC (*User Account Control*) ou l'obligation d'avoir une macro signée dans un document Office, il devient enfantin de pirater une machine, comme c'était le cas sous Windows XP.

Vous allez au fur et à mesure découvrir comment prendre le contrôle quand on est un utilisateur avec peu ou pas du tout de droits sur une machine ou un serveur. L'ouvrage apporte aussi des contre-mesures techniques ainsi qu'une réponse en termes de gouvernance sur la problématique de l'internal hacking.

Les entreprises auront ainsi des moyens pour prévenir et empêcher ces attaques avant leur survenue.

2. Décryptage d'une attaque réussie

Lorsque vous partez en vacances, vous commencez en général par choisir la destination ou celle-ci est guidée par votre budget. Puis, une fois la destination validée, vous vous intéressez à l'itinéraire, aux hôtels, jusqu'à nouveau choisir ce qu'il y a de mieux, en rapport qualité/prix. Une fois vos choix faits, vous réservez. Puis, enfin, le jour arrive où vous partez en vacances. Et là, sans vous en rendre compte, vous avez établi un projet en commençant par une phase de reconnaissance. Saisissant une opportunité, vous recherchez encore plus de détails. Voilà la meilleure manière de procéder pour ce type de projet : étudier les opportunités, analyser en détail la ou les éventuelles solutions, pour aller encore plus dans le détail.

Comme la métaphore précédente, l'attaque d'un système se déroule généralement en plusieurs phases. Les premières de celles-ci sont la recherche d'informations et la prise d'empreinte. Comme vous l'aurez compris, c'est le minimum pour la réussite de votre projet. Tous les chefs d'État l'ont bien compris, ils travaillent énormément avec leurs agences de renseignements bien avant qu'un conflit n'arrive sur le terrain. Les premières phrases sont suivies de la phase d'attaque, qui, elle, est élaborée et testée très finement. Copier/coller un script de ce livre ne suffit pas pour réussir dans les meilleures conditions ; pensez à prendre le temps nécessaire pour tester vos futures actions comme les militaires testent un nouveau missile. Puis, une fois l'attaque en cours de progression ou réalisée, il est intéressant de conserver un contrôle sur les systèmes pénétrés, cela réduira le risque de recommencer une nouvelle attaque. On réalise cela grâce à l'installation d'une porte dérobée. Enfin, on efface nos traces, pour laisser les serveurs cibles « aussi propres que vous les avez trouvés en entrant ». L'ennemi ne doit pas savoir que nous sommes passés à l'attaque et il ne doit pas savoir qui l'a fait s'il s'en apercevait.

Ce livre vous aidera dans toutes les tâches de ce processus. Gardez en tête qu'il n'y aura pas de bonne attaque si vous la lancez au hasard. Préparez-vous suffisamment et testez vos techniques, comme un magicien prépare ces tours. Finalement, la réussite de tout projet se base sur une bonne préparation.

3. Décryptage de contre-mesures efficaces

Une contre-mesure efficace est une contre-mesure qui saura contrer si possible plusieurs attaques potentielles, et ce, même si celles-ci n'ont pas encore été forcément détectées comme étant des menaces. La défense doit être portée à 360°. Il ne s'agit pas de fermer une porte à double tour, et de laisser une fenêtre grande ouverte. Il est aussi important d'y ajouter une touche de gouvernance définissant les processus de contrôle, comme contrôler que toutes les portes et les fenêtres soient bien fermées dans votre logement avant de partir en vacances. Cette partie-là n'est pas technique mais belle et bien procédurière. Il reste à bien comprendre les risques techniques et, pour cela, il est indispensable de comprendre les rouages de l'internal hacking pour mettre en place une défense à la hauteur de la menace.

3.1 Analyse de risques réels

Pour se défendre correctement, il faut savoir ce que l'on risque. Se protéger contre l'inconnu est très difficile dans la mesure où l'on ne souhaite pas tout bloquer. L'analyse de risques doit donc prendre en compte les menaces réelles et pas seulement les risques repertoriés par un référentiel, qui la plupart du temps donne volontairement des consignes très générales pour couvrir le maximum de risques. Mais à vouloir se protéger d'un risque flou, on risque de mettre en place des moyens techniques et procéduriers coûteux, longs et complexes, tout cela pour ne pas forcément couvrir le risque réel.

3.2 Considérations techniques

Une défense doit tenir compte des aspects techniques même si cela donne une réponse moins générale ou moins variable à une menace. Il faut, pour préparer de bonnes contre-mesures techniques, utiliser l'analyse de risques (réels) et ainsi répondre par des moyens adaptés. Pensez à comparer les solutions intégrées, souvent gratuites, aux solutions payantes qui n'apportent pas toujours une vraie plus-value. Pensez à couvrir les risques à 360°. Il m'arrive souvent de voir que pour empêcher un utilisateur d'installer un programme sur son PC, le téléchargement est interdit et bloqué grâce à un proxy web. Mais est-ce que lorsqu'on empêche un utilisateur de télécharger, on l'empêche vraiment d'installer une application ? D'autres pensent que si l'utilisateur n'est pas administrateur de sa machine, il ne peut rien installer, mais c'est faux. Il peut installer certains programmes ou utiliser des applications portables. Il peut fabriquer ses propres programmes. Est-ce que le risque, c'est l'installation de programmes ou est-ce que c'est l'exécution d'une application dangereuse ? C'est en pensant à toutes ces choses-là que l'on peut considérer que l'on couvre un risque à 360°.

3.3 Considérations sur la gouvernance

La gouvernance des systèmes est importante. Si vous ne pensez qu'en termes techniques, vous allez passer à côté de certains fondements de la sécurité. Quelques exemples simples, si vous voulez avoir le droit d'utiliser un proxy qui surveille les connexions Internet de vos utilisateurs, vous devez les avertir. Cela peut être fait dans une politique de sécurité, qui inclura le règlement d'utilisation de l'infrastructure informatique. Si la salle serveur devait brûler, est-ce que vous sauriez comment organiser les ressources humaines et informatiques pour remonter le plus rapidement possible un système utilisable par les gens du métier afin qu'ils puissent travailler ? Lorsque quelqu'un quitte la société, que se passe-t-il avec ses fichiers, ses mails, son compte, etc. ? Lorsqu'une attaque par virus est déclarée dans votre réseau, quelles réactions ont les utilisateurs, par quel processus êtes-vous informé, quel système permettra d'endiguer et de résoudre le problème ?

Comme vous l'aurez compris, même si la technique est très importante, elle ne doit pas être le guide pour la mise en place d'une contre-mesure et plus globalement pour l'installation d'une solution informatique. La gouvernance des systèmes vous aidera à prendre en compte les risques mais tiendra aussi compte du métier et des coûts, ce qui donne aussi un résultat beaucoup plus proche du besoin général de l'entreprise qu'une solution réaliste et applicable en termes de sécurité.

4. Quelles actions, pour quel rôle ?

Vous devez, avant de rechercher des informations, savoir en quoi consistent les rôles existants et ce qu'ils permettent de faire dans l'environnement dans lequel vous travaillez.

Il y a globalement trois rôles principaux définis : celui d'administrateur local, qui peut faire quasiment tout sur sa machine, celui d'administrateur du domaine, qui peut quasiment tout faire sur l'ensemble des machines de l'entreprise, et enfin, le plus répandu, celui d'utilisateur, qui est normalement configuré pour simplement utiliser le système qu'on lui met dans les mains, c'est-à-dire pour uniquement réaliser son travail. Il existe des variantes de ces rôles qui sont créés à l'aide de groupes de sécurité et de règles de sécurités spécifiques souvent liées à un rôle métier comme comptable, vendeur, technicien en informatique, etc.

À dire vrai, en contournant l'utilisation classique du système et du rôle que le responsable informatique vous a attribué, on peut aller bien plus loin qu'il ne l'espère.