# CERTITUDE CONTRE PERCEPTION : SECURISER VOTRE ENTREPRISE AVEC LE PLAN DE SURVEILLANCE CONTINUE ET LE CONTROLE D'ACCES RESEAU

KEVIN T MCDONALD, iCEO #27674

## Le niveau d'alerte actuel : Rouge

Le coût d'une simple suspicion d'intrusion est à ce jour d'environ 90 à 305 US $ par enregistrement perdu[1]. Ce chiffre peut être aggravé par la perte d'affaires futures, le coût de localisation, de notification et d'apaisement des personnes impactées et par la perte de productivité subie post-incident. La plus grosse perte de propriété intellectuelle connue a probablement été la perte de technologie nucléaire du Projet Manhattan dans les années 1950. Le projet Manhattan à lui seul a coûté 20 Billions de US$[2]. La victime moderne la plus récente a été TJX avec la perte de données de cartes de crédit clients, le résultat d'une simple connexion au réseau par Wifi, avec un coût estimé de 1,6 billions US$[3]. En ces sombres jours, vous sentez-vous en sécurité ?

## Quel est le profil de sécurité idéal ?

Dans l'environnement actuel, cela dépend en grande partie de l'entreprise. La plupart des modèles de sécurité mis à plat ressemblent au parcours d'une balle de golf. L'information la plus importante est protégée au centre, entourée d'anneaux de sécurité. Chaque anneau peut présenter des obstacles demandant à l'utilisateur de fournir une carte, un code, un mot de passe, une empreinte digitale ou autre identification bio-métrique. Une fois l'accès accordé, il reste encore un risque d'espionnage pouvant contourner complètement le processus. Si l'information protégée est aussi importante que dans les exemples ci-dessus, elle justifie toute l'attention que vous pouvez apporter au problème..

## Quelles sont les menaces auxquelles les entreprises peuvent être confrontées aujourd'hui ?

Pendant la guerre froide, les services de sécurité gouvernementaux ont imaginé des moyens pour lire des données d'équipements électroniques à distance des sources électroniques. Les contre-mesures à ce type d'espionnage sont regroupées dans une catégorie d'équipements connue sous le nom de Contrôle de Tempête. Les Contrôles de Tempête limitent, entourent ou émettent des bruits pour réduire le risque d'espionnage. Les attaques de tempête ne sont pas conçues pour atteindre des cibles de

[1] Source : Infocationweek.com "Security breaches cost $90 to 305 per lost record" Etude Forrester portant sur 28 entreprises ayant connu des intrusions informatiques et ont eu du mal à calculer les dépenses en résultant. Par Sharon Gaudin citant le Rapport Forrester de Khalid Kark (http://www.informationweek.com/news/showArticle.jhtml?articleID=1990002221)

[2] Source Brookings Institute : http://www.brook.edu/FP/PROJECTS/NUCWCOST/MANHATTAN.HTM

[3] Source hackreport.net Inside Job? TJX Hacl loss estimated at 1.6 Billion, Martin Hack, Hack report quoting Protegrity : http://hackreport.net/2007/04/12/inside-job-tjx-cost-of-breach-estimated-at-16-billion/

faible importance, en raison de leur coût et de la sophistication du matériel nécessaire, mais les organismes gouvernementaux, ou à forte valeur financière, ou R&D devraient y songer.

Il existe un certain nombre de rampes d'accès dans les réseaux moyens actuels. Les sites Web sont les cibles les plus sujettes à des attaques. Comme ceux-ci sont complexes et évoluent régulièrement, cela laisse des opportunités d'exploiter les nouvelles failles découvertes et les trous laissés quand de nouveaux programmes sont introduits. Sans techniques de blocage spécifiques, ces sites sont des maillons faibles. Les pirates informatiques vont scanner des milliers de sites à la recherche de faiblesses particulières. Ils peuvent ne pas cibler votre entreprise en particulier, mais il s'agit juste d'un système qui leur paraît vulnérable. Les services de sécurité font référence à cet environnement en termes de menaces, vulnérabilités et contre-mesures. Par exemple, si vous laissez votre maison sans surveillance pendant quelques jours, et que le courrier et les journaux s'empilent, les voleurs vont d'abord essayer d'ouvrir votre porte. La menace est le cambrioleur. La vulnérabilité est le fait que la maison semble inoccupée. Les portes, serrures et alarmes sont les contre-mesures. Si en s'approchant, le cambrioleur voit un signe indiquant la présence d'une alarme, cette contre-mesure supplémentaire pourrait suffire pour qu'il abandonne votre maison pour passer à la suivante.

## Menaces principales

**Systèmes non patches :**
Au cours d'une semaine normale, on peut compter des dizaines à des centaines de nouvelles découvertes de failles dans les programmes informatiques. Si ces failles ne sont pas sécurisées, certaines personnes sur le net essaieront de les utiliser pour avoir accès aux réseaux. Comme les informaticiens n'ont généralement pas le temps ou l'occasion d'installer les mises à jour des programmes ou équipements informatiques (appelés des patchs) qui vont immédiatement sécuriser le système, il y a des chances pour qu'un pirate informatique remarque les systèmes vulnérables et exploite cette vulnérabilité. Le seul défi pour le pirate informatique est de trouver ces systèmes.

**Réseaux publics :**
Une demande Web peut transiter par 15 routeurs ou plus, chacun d'eux pouvant être infecté par un tiers sans que l'hôte soit au courant. Une fois à l'intérieur, tout le trafic passant par un routeur peut être capturé par un acteur sophistiqué. Cette facilité d'attaque, due au grand nombre de systèmes non recherchés, présente le plus haut degré de menace aujourd'hui. Comme les pirates ont tendance à attaquer les cibles opportunes, à la recherche des faiblesses, les entreprises les moins préparées devraient être attaquées avant les cibles plus complexes.

**Accès sans fil :**
Avec le progrès et la popularité des transmissions de données par les systèmes sans fil WiFi, WiMax, GSM et EVDO, les attaques sont encore plus faciles, car les cartes d'ordinateurs portables ont des faiblesses qui peuvent être attaquées sans même se connecter sur les sites des entreprises. Un ordinateur portable non sécurisé peut être corrompu par des programmes furtifs qui vont faire de l'ordinateur un véritable esclave du pirate informatique. L'ordinateur portable va régulièrement vérifier s'il a reçu des ordres du pirate informatique. Selon ces instructions, il peut résulter de nombreux scénarios négatifs.
Le concentrateur (hub) des systèmes sans fil est également vulnérable en cas de mauvaise configuration ou de faible cryptage qui peut être forcé très rapidement. Ces hubs sont déployés par de

nombreux informaticiens car ils ne sont pas coûteux et que l'on pense généralement que le risque baisse car il faut une certaine proximité physique par rapport au réseau pour avoir accès au trafic. C'est cependant exactement la technique utilisée par un pirate informatique pendant six mois pour capturer des numéros de cartes de crédit de clients dans l'attaque contre TJX. Le réseau peut être complètement protégé de toutes les autres manières possibles, le pirate contourne toute cette sécurité simplement grâce à un seul hub WiFi faiblement protégé. C'est comme d'avoir un passeport diplomatique sur votre réseau : pas de file d'attente, pas de contrôle des bagages.

## La Fonction d'audit en informatique : interne ou externe

Généralement on procède à un audit de sécurité en même temps que l'audit comptable annuel, pour s'assurer que les protections minimales sont en place et fonctionnent. Ces audits sont souvent réalisés par des cabinets d'audits informatiques externes détachés par les cabinets d'audits comptables publics. Utilisant Sarbanes-Oxley, BASEL, HIPAA ou Gram-Leach Bliley pour vérifier la conformité des entreprises, ces audits concernent les restaurations de données et les « bonnes pratiques » informatiques. Cependant, comme ce sont des contrôles annuels et que les informaticiens les considèrent comme des services externes imposés plutôt que des demandes de contrôle demandées en interne, on peut encore faire face à une certaine résistance et à des efforts minimum pour adopter ces standards comme des références internes.

Alors que les sociétés adoptent des philosophies d'entreprise plus proactives, tels Six Sigma et CMM5, la tendance à passer d'un mode réactif à un mode proactif a finalement atteint la masse critique en informatique. La pression porte maintenant sur l'adoption d'un audit informatique interne pour générer une surveillance continue plutôt que discrète, en instaurant par exemple des procédures de comportements standards au lieu de n'afficher de bons comportements que lors des contrôles.
Mais il y a encore une certaine résistance face à l'audit interne, car il s'agit toujours d'un rôle d'inspection. La qualité doit émaner de l'intérieur du système, et non pas le contrôler. Afin de parvenir au niveau supérieur, je recommande d'instaurer un Plan de Surveillance Continue plutôt qu'un audit interne. Un PSC pratique des exercices pour découvrir les éventuelles faiblesses du système. Un exercice est différent d'un test d'audit. Un test donne des résultats de succès ou d'échec, et attribue de mauvaises notes aux entreprises ayant des problèmes. En pratiquant des exercices, tout le monde partage le même objectif, qui est de détecter les faiblesses. Accorder des récompenses pour les faiblesses détectées est une arme bien plus puissante que la conduite de test d'audit. En instaurant le Plan de Surveillance Continue dans un cadre défini, la fonction d'audit n'est pas considérée comme un adversaire par le personnel interne de l'entreprise.
Cela évite également une source potentielle de conflits entre la direction et les services informatiques. Comme les informaticiens aiment toujours être à la pointe, la direction pense souvent qu'ils demandent toujours plus que le nécessaire. Si la demande émane d'un parti indépendant, elle peut être considérée comme fiable. "Il faut remplacer leur gadget pour éviter les problèmes rencontrés par XYZ le mois dernier". Lorsque les achats sont visés par le PSC, on peut s'assurer que cet achat sera lui aussi inclus dans le plan de surveillance et que les plans de continuité peuvent être mis à jour pour inclure les nouvelles ressources informatiques.

## La technologie à la rescousse

En conjonction avec le PSC, on peut également déployer des systèmes de surveillance. La nouvelle génération de pare-feux est appelée systèmes de Contrôle d'Accès Réseau (CAR). Un CAR est un pare-feux intelligent qui pré-enregistre tous les périphériques sur le réseau. Si un nouveau périphérique est connecté, le CAR vérifie son profil. Si le profil ne correspond pas à un dossier pré-existant, le périphérique est isolé en mode "invité". Le mode "invité" peut autoriser des impressions réseau ou des consultations Internet, mais refuse l'accès aux serveurs de l'entreprise. Les responsables de sécurité, une fois alertés de la présence du nouveau périphérique, peut vérifier s'il s'agit d'un visiteur, d'un nouveau PC d'entreprise ou d'un mauvais garçon tentant d'accéder au réseau. Si le périphérique est identifié comme le nouveau Blackberry du DAF par exemple, le profil va être mis à jour et la prochaine fois que le Blackberry accèdera aux e-mails, l'accès pourra lui être accordé. Si l'utilisateur du Blackberry est inconnu, il est relégué à l'accès "invité", avec un faible taux relatif d'accès à des informations sensibles. Cette technologie a été commercialisée sous le label "Network Admission control" (NAC) par Cisco et "Network Access Protection" (NAP) par Microsoft. Les principes de base restent les mêmes, il s'agit de prouver qui vous êtes avant de vous autoriser l'accès au réseau pour des fonctions autres que basiques.
Une autre technologie, la gestion de patch, peut également être déployée avec le NAC. Un gestionnaire de patch vérifie chaque paquet du réseau, détermine s'il représente la vulnérabilité détecté par le NAC et le modifie pour éliminer la faiblesse. Le serveur original conserve le problème, mais le Gestionnaire de Patch empêche son exploitation. Les informaticiens peuvent patcher le serveur lors des cycles normaux de maintenance sans compromettre la sécurité.
Toutes ces techniques commencent à converger vers des équipements plus sophistiqués. La nouvelle génération permettra une mise à jour automatique, le téléchargement de nouveaux profils pour prendre en compte les nouvelles menaces, les nouveaux virus et les nouveaux types de périphériques dès qu'ils sont disponibles.

En conclusion, en confiant tout d'abord la sécurité de l'entreprise au Plan de Surveillance Continue et en déployant la nouvelle génération de surveillance réseau telle le NAC, l'entreprise peut adopter un profil pro-actif avec moins de résistance de la part des personnes impliquées en interne. Cela peut mener le Service informatique au niveau supérieur, où le nombre de systèmes vulnérables diminue et où il peut reprendre un rôle central de création de valeur ajoutée pour l'entreprise.

**KEVIN T MCDONALD**

**A propos de CEO Europe** (www.ceo-europe.com)
A travers la solution de Management on demandT, CEO Europe garantit le développement d'un nouvel environnement de coopération flexible et réactif entre les sociétés, les actionnaires et les dirigeants dans un contexte international. CEO Europe propose aux entreprises, en moins de 3 semaines, un service de management de transition et de recrutement de plus de 9500 cadres dirigeants certifiés « iCEO™» avec tous un profil d'entrepreneurs disposant au minimum de 15 années d'expérience, basés dans plus de 168 pays en Europe, en Amérique du nord et en Asie.