Le rôle des gestionnaires contre l'espionnage industriel

La Boule de Cristal du CRIM
Montréal, 17 février 2006

M. E. Kabay, PhD, CISSP-ISSMP
Professeur associé en sécurité informatique
Directeur de la maîtrise en sécurité informatique
Université Norwich
Northfield, Vermont, É.-U.

Sujets de discussion

- C'est quoi le problème?
- Le contexte
- Exemples de l'espionnage
- L'embauche
- La gestion du personnel
- Congédiement d'un employé

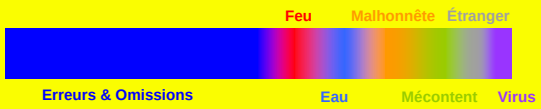
C'est quoi le problème?

C'est quoi le problème?

- Les êtres humains sont au coeur d'assurance de l'information
- Les employés en qui nous avons confiance peuvent contourner les contrôles normaux de la sécurité informatique
- Les personnes malhonnêtes sont experts à convaincre les autres de leur prêter confiance
- Qui a l'accès *physique* aux systèmes informatique possède le contrôle pratiquement complet des ressources

Les dangers avant 1993

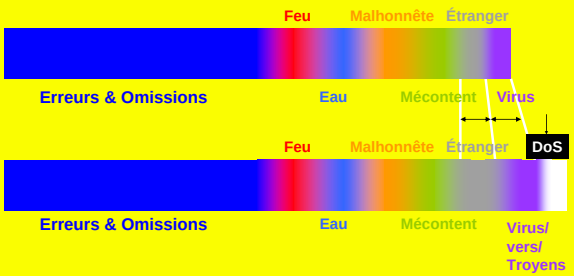
Menaces contre les systèmes informatiques et les données *avant* l'explosion Internet



- Frontières floues
  - information non fiable
- Problèmes statistiques
  - les bris de sécurité passent inaperçus
  - peu de rapportage systématique
  - aucune banque de données centralisée

Les dangers après 1993

Menaces contre les systèmes informatiques et les données *après* l'explosion Internet



Exemples de l'espionnage industriel

- GM vs VW (1993-1997)
- TAXOL (1997)
- Gillette vs Warner-Lambert et al. (1997)
- Joy Mining Machinery vs United Mining Cable (1997)
- Les déchets de Microsoft (2000)
- Echelon (2000)
- Barksdale (2001)
- Acuson vs Bell Imaging (2000)
- Lucent vs Datang Telecom (2001)
- Ericsson vs Russie (2003)
- Troyen en Israël (2005)

GM vs VW (1993-1997)

- Entre 1993-1997, José Ignacio de Arriortua a été impliqué dans un scandale d'espionnage industriel
- 1992: Il avait été nommé directeur de la division Opel de GM
- 1993: Lopez et 7 collègues quittent Opel/GM pour travailler chez VW
- 1993: Opel accuse Lopez d'avoir volé des boîtes entières de documents confidentiels
- 1997: règlement extrajudiciaire, secret

TAXOL (1997)

- deux taiwanais arrêtés pour espionnage
  - cherchaient détails de production de *Taxol*
  - drogue contre le cancer ovarien
  - valeur dans les milliards$
- essayaient de soudoyer un savant de Bristol-Myers Squibb
  - l'employé l'a rapporté à ses patrons
  - le FBI a supervisé l'investigation
- les deux agents ont été arrêtés

Gillette vs Warner-Lambert *et al.* (1997)

- Steven Louis Davis
  - entrepreneur pour la cie. Gillette
  - projet: nouveau système de rasoir
- en février et mars 1997, a montré documents secrets aux compétiteurs
  - Warner Lambert
  - Bic
  - American Safety Razor
- arrêté en octobre 1997
- janvier 1998: plaidé coupable aux charges fédérales de vol de secrets professionnels
- 2 ans et 3 mois en prison

Joy Mining Machinery vs United Mining Cable (1997)

- John Fulton
  - ex-employé de Joy Mining Machinery
  - a fondé cie. compétitrice United Mining Cable
- Fulton a offert de l'argent à un employé de JMM pour le plan d'une unité spécialisé
  - l'employé a collaboré avec JMM et le FBI pour enregistrer les conversations
- en avril 1998 Fulton plaide coupable de vol de secrets professionnels

Les déchets de Microsoft (2000)

- Microsoft s'est plaint que plusieurs organismes avait volé des documents des poubelles de la compagnie
  - Association for Competitive Technology
  - Independent Institute of Oakland, CA
  - Citizens for a Sound Economy
  - Oracle Corporation
- Lawrence Ellison de la cie. Oracle a offert d'envoyer les déchets de sa compagnie à Microsoft. . . .

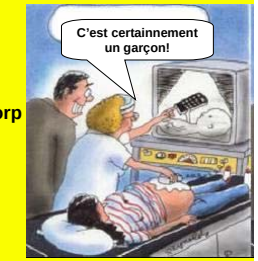
Echelon (2000)

- Parlement européen s'intéresse à *Echelon*
  - forme comité temporaire
  - analyse du réseau d'espionnage électronique
- plusieurs nations responsable du réseau Echelon
  - É-U, Australie, Canada, G-B, NZ
- Interception des communications électroniques
  - Téléphone
  - Télécopie
  - Courriel
- Question d'espionnage industriel contre les firmes européennes

Barksdale (2001)

- assistante administrative congédiée
- en partant, vole des documents secrets d'un valeur de 1,5$M
- avec une carte de crédit de la compagnie elle s'achête 100.000$ de bijoux
  - et 2 téléviseurs
  - et 2 chaises et un sofa
  - et un micro-onde
  - et une croisière en bateau
  - et des montres
  - et 3 caméras
  - et des sacs à main
  - et un tapis
  - ....

Acuson vs Bell Imaging (2000)



- Junsheng Wang
  - travaillait pour Bell Imaging
  - compagnie chinoise (communiste)
- épouse travaillait pour Acuson Corp
  - ingénieur
  - a emmené documents secrets chez eux
  - plans d'un nouvel appareil ultrason
- Wang est allé en chine
  - a donné les copies à son employeur
  - trouvé coupable de contravention de 18 USC §132(a)(2) (vol des secrets industriels)

Lucent vs Datang Telecom (2001)

Lucent Technologies
Bell Labs Innovations

- citoyens chinois
  - Hai Lin, Kai Xu & Yong-Qing Cheng
  - employés respectés de Lucent
- ont volé le code source de PathStar Access Server
  - immense valeur compétitive
  - envoyé à Datang TelecomTechnology
    - ✓Beijing
    - ✓propriétaires majoritaires: gouvernement communiste de la Chine
    - ✓voulaient créer le « Cisco de la Chine »
- en 2002, accusés d'espionnage contre Telenetworks, NetPlane Systems, Hughes Software Systems & Ziatech

Ericsson vs Russie (2003)

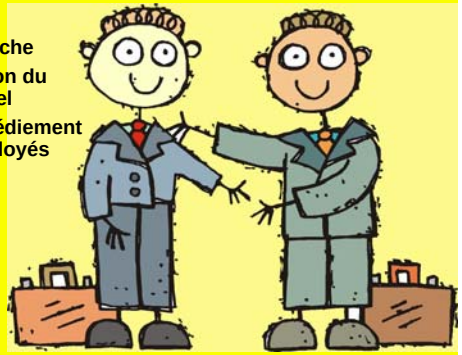
- Ericsson
  - grande compagnie suédoise
  - communications sans fil
- accuse 3 employés d'espionnage industriel
  - Afshin Bavand
  - Mansour Rokkgireh
  - Alireza Rafiei Bejarkenari
- collaboration avec compagnie de télécommunications russe

Troyen en Israël (2005)

- compagnies d'investigation privée ont utilisé un logiciel maléfique (Troyen)
  - porté par CD-ROM (présentation d'affaire)
  - accès illégitime (« back door »)
  - enregistre touches de clavier (« keystroke logging »)
- douzaines de compagnies atteintes
  - aucune compagnie ciblée n'a suspecté Troyens
  - découvert parce que un criminel a matériel volé sur l'Internet

Les fonctions cruciales

- L'embauche
- La gestion du personnel
- Le congédiement des employés



L'embauche d'un employé potentiel

- porter attention à l'histoire de travail
  - Limitations légales des questions
  - éviter l'embauche négligent
- faire interviewer les candidats par leurs futurs collègues
  - la meilleur façon d'identifier des fraudes et des fabulateurs
- mettre en vigueur des accords d'emploi
  - contrat légal
  - adhérence aux politiques de la compagnie
  - définir les raisons potentiels de congédiement s'il y a lieu
- protéger la propriété intellectuelle avec les accords de non révélation des secrets commerciaux

La gestion

- identifier les circonstances favorisant l'abus
- l'accès n'est pas un privilège ou u droit
- méfiez-vous de l'employé indispensable
- respecter les vacances
- être vigilant aux changements du comportement
- départager des responsabilités
- interdiction des enquêtes non autorisées

Identifier les circonstances favorisant l'abus

- penser comme un criminel
  - chercher à contourner des règles
  - élaborer des scénarios d'infraction
- développer des contre-mesures
  - procédures de vérification systématique
  - méfiez-vous de l'accès aux ressources critiques par une seule personne
- établir des réponses aux offres de corruption des employés

L'accès est ni privilège ni droit

- l'accès n'équivaut pas au prestige
  - les directeurs n'ont pas besoin d'accéder aux lieux physiques des grands ordinateurs et des réseaux
  - ne pas distribuer les clefs maîtres sans justification
- personne ne doit partager son mot de passe ou son jeton sécuritaire
- l'accès *limité* peut être accordé temporairement dans les circonstances particulières (ex., aux assistants)
  - raison spécifique à documenter
  - temps limité
  - journalisation adéquate «audit trails»

Méfiez-vous de l'employé indispensable

TOUTE LES COMPÉTENCES ET LES INFORMATIONS CRITIQUES DOIVENT ÊTRE PARTAGÉES

- dépendre d'une seule personne pour les fonctions critiques invite le désastre
- difficulté extrême de congédier cette personne
- une fois congédiée cette personne est à grand risque de faire du mal
- si vous n'avez pas transféré leurs fonctions avant le départ le chaos peut en survenir

Forcez les vacances

- les vacances sont bénéfiques – non seulement pour les employés
  - les vacances offrent l'occasion d'assurer l'intégrité des opérations
  - les opérations ne devraient pas souffrir à cause de l'absence d'un employé
- Exemple:
  - un employé est parti en vacances sur une île tropicale sans possibilité de communication
  - les opérations étaient en catastrophe toute la semaine
  - manque de connaissances des autres employés
  - manque de documentation adéquate pour soutenir les opérations

Répondez aux changements du comportement

- tout changement exceptionnel dans l'humeur ou le comportement devrait stimuler l'attention des gérants
  - heureux → triste
  - maussade → amical
  - délassé → nerveux
  - pauvre → riche
- Cas:
  - Lamborghini
  - administrateur détesté soudainement souriant

Départager des responsabilités

- ne pas accorder *l'autorisation* et *l'exécution* d'une fonction critique à la même personne
- exemples
  - ✓comptabilité: émettre le chèque et signer le chèque
  - ✓opérations: annoncer un nouveau poste et le lancer
  - ✓programmation: exiger un changement et le mettre en cours
  - ✓sécurité: rajouter un utilisateur et autoriser l'ajout
- la séparation des fonctions oblige la collaboration des employés – plus difficile pour le criminel

Pas d'enquêtes de sécurité sans autorisation

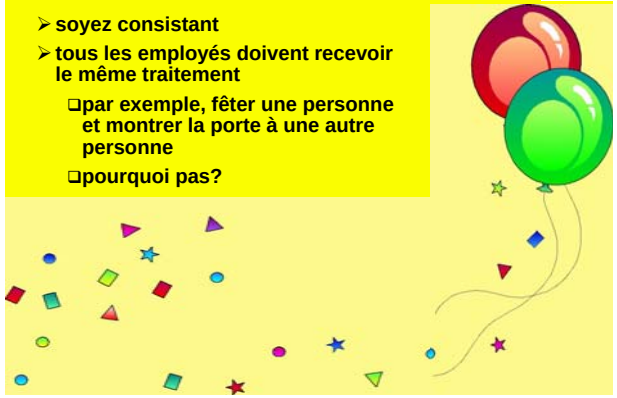
- interdiction explicite des évaluations de sécurité non autorisées
- personne n'a permission d'installer un logiciel (de sécurité ou autre) sans autorisation
- les enquêtes de sécurité exigent l'autorisation écrite des responsables
- aviser les employés de ne pas coopérer aux « nouvelles procédures de sécurité » ou à la « vérification de la sécurité » sans s'assurer que ces procédures soient mandatées

Congédiement (1)

- démission ou congédiement:
  - ✓lequel est plus dangereux?
- bloquer l'accès
  - ✓pendant l'interview final
  - ✓procédure en place pour l'élimination des privilèges
  - ✓récupération de la propriété de la compagnie
- équipement, jetons, insignes, documents, formulaires, listes des clients, ….

Congédiement (2)

- soyez consistant
- tous les employés doivent recevoir le même traitement
  - par exemple, fêter une personne et montrer la porte à une autre personne
  - pourquoi pas?



DISCUSSION