Computer Emergency Response Team
Industrie Services Tertiaire

Evolution des failles et des incidents

Forum 2010

Philippe BOURGEOIS
Cert-IST

Sommaire

- Evolution des failles et attaques
  - L'année 2009 vue par le Cert-IST
  - Les attaques visant le poste de travail
  - Le niveau de sophistication des attaques
  - Des attaquants et des défenseurs de plus en plus déterminés
- Attaques externes vs incidents internes
  - Le risque « interne » ne doit pas être sous-estimé
  - Evolution du risque interne

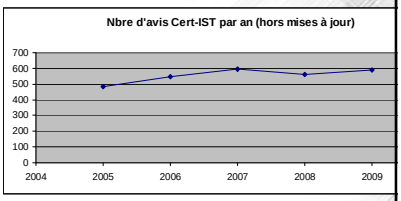
Computer Emergency Response Team
Industrie Services Tertiaire

Evolution des failles et attaques

CERT-IST
Industrie Services Tertiaire

1) L'année 2009 vue par le Cert-IST

- 592 Avis de sécurité (+1590 mises à jour)
  - Le nombre de vulnérabilités découvertes chaque année reste élevé (presque 2 par jour)

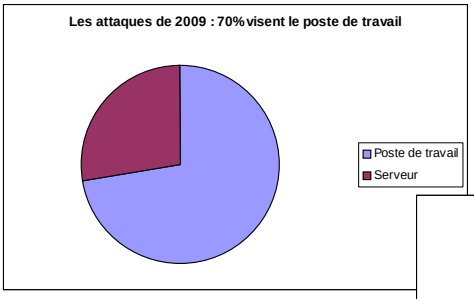


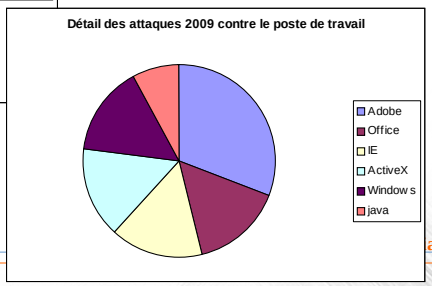
- Les situations à risque augmentent
  - 18 Dangers Potentiels
    - Prés de 2 fois plus de situations à risque ont été identifiées (par rapport aux années précédentes)
  - Pas d'Alerte en 2009
    - les attaques sont restées d'ampleurs limitées (aucune "alerte générale" n'a été lancée)
    - Conficker (2008) est resté très présent (au moins jusqu'en avril 2009)

  Nota : Il y a avait eu 2 alertes en 2008 (Conficker et DNS)

1) L'année 2009 : les situations à risque

- 70 % des situations à risques sont dues à des attaques visant le postes de travail
- Elles utilisent des vulnérabilités dans les logiciels clients (Acrobat Reader, etc…)





Industrie Services Tertiaire

2) Les attaques visant le poste de travail

- Ces menaces sont présentes depuis plusieurs années (cf. Forum 2008)
  - Ces attaques visent le plus souvent des logiciels applicatifs (lecteur PDF, logiciels Office, navigateurs web)
  - Les outils d'attaque sont sophistiqués (e.g. Eleonore, FastFlux, etc…) et les attaques discrètes (Drive-by download)
  - De nombreux sites web relaient involontairement les attaques (ils sont compromis)

  Naviguer sur Internet avec un ordinateur non à jour est devenu TRES dangereux.

- Deux scénarios d'infection
  - Attaque massive : un grand nombre de sites infectés attaquent l'internaute lors de la visite de sites anodins.
  - Attaque ciblée : e-mails piégés envoyés à quelques collaborateurs dans l'entreprise

  En 2008 : Plusieurs vagues d'attaques massives (au premier semestre)
  En 2009 : peu d'attaques massives, mais beaucoup d'attaques ciblées

Industrie Services Tertiaire

2) Les attaques visant le poste de travail (suite)

Cycle de vie d'une vulnérabilité

- Scénario type
  - Le pirate achète ou découvre une vulnérabilité
  - Il l'utilise dans des attaques ciblées : 1er vague d'attaques.
  - L'attaque est découverte et la vulnérabilité devient publique
  - Elle est reprise par d'autres pour des attaques massives (en plus des attaques ciblées) : 2eme vague d'attaques
- Risque induit pour l'entreprise
  - Il est difficile de se protéger contre les attaques ciblées (vulnérabilité « 0-day »)
    - Gestion méthodique des informations sensibles de l'entreprise
    - Défense en profondeur
    - Développer la capacité de détection (l'utilisateur est un maillon clé)
  - Il est plus facile de se protéger contre la 2eme vague d'attaques (mais Conficker a montré que le niveau de maîtrise est ici très hétérogène)
    - Veille sur les menaces et attaques
    - Mise en place de mesures de protection périmétriques en cas de menace
    - Déploiement de correctifs

Industrie Services Tertiaire

3) Le niveau de sophistication des attaques

- Les codes d'attaques sont sophistiqués
  - Ils peuvent utiliser des vulnérabilités encore inconnues
  - Il intègrent des fonctionnalités avancées
    - Dissimulation du malware (via un « rootkit »)
    - Communication P2P (ex StormWorm) ou multi-canaux, mécanismes de rendez-vous sophistiqués (Conficker)
    - Fonctions cryptographiques (ex Conficker)
- Les infrastructures déployées par les attaquants sont sophistiquées
  - Une organisation structurée (R&D, Développement en projet, gestion des déploiement)
  - Des infrastructures de déploiement sophistiquées (Exemple) (Zoom)
- Les moyens de défense restent limités
  - Les antivirus ne sont pas une protection suffisante (cf. Forum 2006)
  - Il n'y a pas de protection technique infaillible face à un attaquant motivé :
    - La solution ne peut pas être que technique
    - Le risque doit être identifié et analysé

Industrie Services Tertiaire

4) Des attaquants et les défenseurs de plus en plus déterminés

- Les attaquants sont des professionnels
  - La partie la plus visible : Spam, Phishing, Botnet (cyber-fraud)
    - Vol d'identifiants, Fraude CB, escroqueries (ex. faux antivirus)
  - Les attaques ciblées sont également une réalité (cyber-espionnage / cyber-attaque)
    - L'opération Aurora (visant Google) en est un exemple
- Les défenseurs se structurent et sont déterminés
  - Opérations de démantèlement internationales
    - Actions coordonnées de groupes privés (Chercheurs) et de forces gouvernementales
  - Création d'Agences gouvernementales
  - Augmentation de la maturité des constructeurs dans la gestion des vulnérabilités
    - Gestion sur les failles complexes, coordination multi-constructeur, publications programmées
- Globalement le paysage se « durcit » et se professionnalise
  - L'entreprise doit également continuer à améliorer ses processus et sa capacité à maitriser le risque d'attaque.

Industrie Services Tertiaire

Computer Emergency Response Team
Industrie Services Tertiaire

Attaques externes vs Incidents internes

Industrie Services Tertiaire

Attaques externes vs Incidents internes

Le risque « interne » ne doit pas être sous-estimé

- Malveillance interne (Vol de données, Sabotage, Fraude)
  - L'impact d'une attaque interne peut être majeur
    - L'attaquant connait le système et ses faiblesses
  - Les mesures de protection sont connues, mais parfois difficile à mettre en œuvre (parce qu'elles demandent beaucoup de rigueur)
    - Politique de sécurité, moindre privilège, séparation des tâches, Information des utilisateurs, etc
    - Nota: L'US-CERT travaille à développer des processus de maitrise de ces risques (MERIT)
- Utilisation inappropriée du S.I. de l'entreprise
  - Utilisation du S.I. pour des activités personnelles répréhensibles
    - Téléchargement illégal, Activité diffamatoire, etc… mené depuis l'entreprise.

    => Risque d'engagement de la responsabilité de l'entreprise envers un tiers lésé
  - comportement à risque
    - clés USB, réseaux sociaux, installation de logiciels à risque

    ⇒ Risque d'affaiblissement de la sécurité de l'entreprise

Industrie Services Tertiaire

Evolution du risque interne ?

- Peu de données sont disponibles
  - Quid de la règle des 80/20 ?
- Malveillance interne
  - Les attaques internes peuvent (aussi) être sophistiquées
    - connaissance des défenses, les outils d'attaque sont disponibles
  - Le traitement des incidents est souvent plus complexe
    - Altération très fréquentes des indices
    - Gestion humaine très délicate
- Usages inappropriés
  - L'explosion de l'usage des TIC fait penser que ce risque augmente aussi.

Industrie Services Tertiaire