Computer Emergency Response Team
Industrie Services Tertiaire

Evolution des menaces (15 ans du Cert-IST)

Philippe BOURGEOIS

Plan de la présentation

- Evolution des menaces (au cours des 20 dernières années)
  - Evolution des attaques
  - Evolution des moyens de protection
  - Profil type des attaquants et de leurs motivations
- La menace actuelle (vue au travers de l'actualité 2014)
  - L'exploitation du facteur humain
  - Les limites des défenses conventionnelles (le cas « Target »)
  - Heartbleed, Shellshock, etc…
  - Le piégeage du matériel (et du logiciel ?)
  - Externalisation des données : le Cloud et le BIOD

Computer Emergency Response Team
Industrie Services Tertiaire

Evolution des menaces

Evolution des attaques (1/6)

- 1994 : Internet s'impose (WWW) et change la nature de la menace
  - On apprend qu'il faut appliquer les patches de sécurité
- 2001 : CodeRed, Sasser, ..., Conficker (2008)
  - On apprend que les attaques peuvent bloquer une entreprise
- 2005 : Fuzzing -> 0-days -> Money
  - Les Cyber-criminels gagnent de l'argent avec Internet
- 2010 : Stuxnet / Snowden : a-t-on ouvert la boite de Pandore ?
  - Le Cyber devient une arme stratégique

Industrie Services Tertiaire

Evolution des attaques (2/6)

- 1994 : Internet s'impose (WWW) et change la nature de la menace
  - On apprend qu'il faut appliquer les patches de sécurité

- Les attaques existent depuis toujours ... mais Internet change la donne
  - Exposition du SI à des attaques externes
  - Partage d'informations sur les vulnérabilités

- Les vulnérabilités sont découvertes, partagées et exploitées
  - « Smash the stack for fun and profit » (AlephOne - Phrack magazine)
  - Mailing-lists Bugtraq et Full-disclosure, groupes de hackers (ex: 8LGM)
  - Kevin Mitnick : quand les attaques théoriques passent à la pratique

Industrie Services Tertiaire

Evolution des attaques (3/6)

- 2001 : CodeRed, Sasser, ..., Conficker (2008)
  - On apprend que les attaques peuvent bloquer une entreprise

- Des infections massives saturent les réseaux
  - CodeRed, Nimda (2001), Slammer (2003), Sasser (2004)
  - ces attaques sont a priori gratuites sans motivation apparente
  - Elles génèrent la phobie des vulnérabilités "wormables "

- Ce type de crise se produit encore
  - Conficker (2008)
  - HeartBleed, Shellshock (2014)

  L'objectif est désormais de prendre le contrôle, le plus vite possible, de machines vulnérables

Industrie Services Tertiaire

Evolution des attaques (4/6)

- 2005 : Fuzzing -> 0-days -> Money
  - Les Cyber-criminels gagnent de l'argent avec Internet

- Apparition des Fuzzers pour la recherche des failles
- Apparition du phénomène des 0-days et du marché noir des failles
- Arrivée de la cyber-criminalité avec des attaques visant principalement le grand public (phishing, vols de données bancaires et escroqueries).

- L'entreprise n'est pas directement visée : la menace est donc moins grande (accalmie sur le front des attaques).
- Les attaque deviennent « professionnelles » (plus structurées et rationalisées)

Industrie Services Tertiaire

Evolution des attaques (5/6)

- 2010 : Stuxnet / Snowden : a-t-on ouvert la boite de Pandore ?
  - Le Cyber devient une arme stratégique

- Les entreprises font face à un nouveau type d'attaques : les attaques par infiltration (APT)
- Ces attaques, qui visent traditionellement le secteur "Défense", se généralisent :
  - beaucoup plus fréquentes
  - sur des secteurs plus larges (commerce, R&D)
  - avec des moyens techniques et financiers nouveaux
- Ces attaques sont (assez) faciles et d'un risque limité

- Les états s'arment : Etats-Unis, Chine, Russie, France, Iran, etc....

Industrie Services Tertiaire

Evolution des attaques (6/5)

- 1994 : Internet s'impose (WW
  menace
- 2001 : CodeRed, Sasser, ..., Conficker (2008)
- 2005 : Fuzzing -> 0-days -> M
- 2010 : Stuxnet / Snowden : on a découvert la boîte de Pandore !

1995 : Bulletin de veille mensuel
1997 : Avis de sécurité publiés mensuellement

1999 : Création du Cert-IST / Avis au fil de l'eau
1999 : Création des ALERTES

2003 : Création des DG et Vuln-coord
2005 : Hub de crise, Veille 7/7

2008 : Veille média
2010 : Veille scada

Industrie Services Tertiaire

Evolution des moyens de protection

- 1994 - La technique : les Firewall
- 2002 - La conformité : SOX, PCI-DSS, … RGS, PSSIE (2014)
- 2004 - La loi : LCEN (resp. des hébergeurs / conservation des log / détention d'outils offensifs) , … LPM (2013)
- 2012 - La supervision de sécurité

Industrie Services Tertiaire

Profil type des attaquants et leurs motivations

- Les amateurs
  - Défacement de sites web avec des revendications fantaisistes ou puériles,
  - Ver expérimental, ou virus amateur lancé sur Internet sans objectif précis,
  - Arnaques artisanales (du type « Nigerian scam ») visant à convaincre des victimes d'envoyer de l'argent à un escroc.
- Les hacktivistes
  - Attaques pour des revendications politiques. Visent des proies faciles (low hanging fruits)
  - Apparus en 2010 (Anonymous), pic en 2011, en recul depuis.
- Les cyber-criminels
  - Attaques crapuleuses de grandes ampleurs : Spam, Botnet, Vol de données bancaire, faux anti-virus, Ransomware
  - Apparus en 2003, dominant depuis 2005. Très organisé (exploit-kits, infrastructure, etc.)
- Les cyber-espions
  - Devenus visible en 2010 (Stuxnet, APT)
  - Visent les états et les entreprises (espionnage, sabotage)

Industrie Services Tertiaire

Computer Emergency Response Team
Industrie Services Tertiaire

La menace actuelle (vue au travers de l'actualité 2014)

L'exploitation du facteur humain

- Un attaquant a au moins 2 moyens pour s'introduire dans l'entreprise
  - Utiliser une vulnérabilité sur un système exposé
  - Ou utiliser la complicité (involontaire) d'un utilisateur autorisé
- L'attaque du facteur humain est souvent la plus facile
  - Envoi d'un email pour convaincre d'exécuter une pièce jointe ou visiter un site piégé
  - Appeler sa victime pour convaincre de réaliser un virement frauduleux ou pour obtenir un mot de passe.
- Il n'y a pas de sécurité possible sans prendre en compte le facteur humain
  - Informer régulièrement des nouvelles techniques d'ingénierie sociale (une nouvelle attaque ne devrait marcher qu'une fois)
  - Limiter les privilèges (segmenter)
  - Détecter les attaques réussies le tôt vite possible (l'utilisateur peut y aider)

Industrie Services Tertiaire

Les limites des défenses conventionnelles Le cas « Target »

- Attaque de la chaine de magasins « Target » aux USA
  - Vol d'un accès de maintenance pour la climatisation
  - Installation d'un infrastructure interne par le pirate
  - Piégeage du système de paiement des caisses enregistreuses (RAM scraper)
- Limites des défenses en place
  - Certification PCI-DSS
  - Outils de détection (antivirus Symantec, IDS FireEye)
  - Les alarmes n'ont pas été (correctement) traitées
- En 2014 les systèmes de paiement des points de vente US ont été la cible d'attaques en série
  - UPS Stores, SuperValu, Home Depot, Goodwill Stores, Jimmy John sandwich restaurants, PF Chang, etc…

Industrie Services Tertiaire

Heartbleed, Shellshock, etc… (1/2)

- Les failles “célèbres” de 2014 :
  - GotoFail (Apple SSL - 02/2014), HeartBleed(OpenSSL - 04/2014),
  - Shellshock (bash - 09/2014), Poodle (SSLv3 10/2014)
- Les tendances 2014 en termes de failles :
  - Des failles très médiatisées
  - Deux ont donné lieu à des attaques massives : HeartBleed, ShellShock
  - Beaucoup de failles crypto, et souvent sur des logiciels open-source
- Les failles crypto :
  - La crypto est un élément clé de protection des données (Cloud, Byod, etc…)
  - Elle a été mise à rude épreuve en 2014 : Failles, Arrêt de TrueCrypt

Industrie Services Tertiaire

Heartbleed, Shellshock, etc… (2/2)

Les attaques massives de 2014 :

- Shellshock
  - Faille facile à exploiter (sur un "vieux" composant - CGI scripts)
  - scan de reconnaissance dès l'annonce de la vulnérabilité
  - attaques industrialisées 48h plus tard
- HeartBleed
  - Faille atypique (Lecture de la RAM à distance)
  - une semaine a été nécessaire pour mettre au point des attaques
  - mais quelques attaques très ciblées ont aussi été détectées dès le lendemain de l'annonce de la faille (selon la société Mandiant)
- Les problèmes mis en évidence par ces attaques
  - Médiatisation
  - identification des systèmes impactés
  - gestion des composants obsolètes

Industrie Services Tertiaire

Le piégeage du matériel (et du logiciel ?)

- Un phénomène nouveau ?
  - Existe depuis toujours dans la panoplie « James Bond »
  - Mais devient plus commun, plus accessible
  - Annonce une banalisation de la pratique ?
- Exemples
  - Bilan Cert-IST pour 2013 : « Les attaques matérielles deviennent une menace réelle. »
    - Publications académiques : backdoor disque dur (Eurecom), vulnérabilité IPMI, BadBIOS
    - Révélation d'outils opérationnels (depuis 2008) : catalogue ANT de la NSA
  - Vu en 2014
    - Fonction « Computrace » ajoutée dans le BIOS
    - Peut-on faire confiance au générateur aléatoire inclus dans INTEL ?
    - « ZombieZero » : des lecteurs de code barre piégés pour espionner les expéditions de colis
- Comment réagir ?
  - Qualification des équipements achetés / Surveillance des flux réseaux
  - Ces techniques sont bien connues des projet sensibles, mais une mise en œuvre plus large parait difficile.

Industrie Services Tertiaire

Externalisation des données : Le Cloud et le BIOD

- Le Cloud s'impose comme une solution de référence
  - "Cloud computing is becoming the backbone of the EU's digital society" (ENISA 2013 - Incident Reporting for Cloud Computing)
- Encore peu d'incidents connus
  - Vol de compte / Interruption de service
  - "There is clearly a need for more efforts to increase the accountability [12, 13] of cloud service providers." (CSA 2013 - Cloud Computing Vulnerability Incidents : A Statistical Overview)
- La solution de Cloud adoptée doit être en accord avec la sensibilité des données.

Industrie Services Tertiaire

Computer Emergency Response Team
Industrie Services Tertiaire

Conclusions

Conclusions

- Une situation complexe
  - L'informatique est une ressource clé, dans l'entreprise et dans la vie privée
  - L'évolution technologique :
    - disperse l'information à protéger (Cloud, BIOD)
    - cherche à rendre facile l'accès à cette information
- Le risque d'intrusion a augmenté de façon importante au cours des 5 dernières années
  - de nouveaux attaquants visant spécifiquement les entreprises (cyber-espionnage, cyber-sabotage) ont été identifiés
  - des attaques plus fréquentes et plus perfectionnées
  - le "cyber" est devenu un enjeu stratégique pour les états
- La médiatisation importante de ces nouveaux risques est une opportunité pour
  - évaluer son exposition à ce type d'attaques
  - renforcer ses défenses
  - développer sa capacité de détection et de réaction aux intrusions

Industrie Services Tertiaire

Computer Emergency Response Team
Industrie Services Tertiaire

Questions

CERTIST
Industrie Services Tertiaire