Computer Emergency Response Team
Industrie Services Tertiaire

Evolution des failles et attaques
Bilan de l'année 2012

www.cert-ist.com

Industrie Services Tertiaire

Mars 2013

Philippe Bourgeois

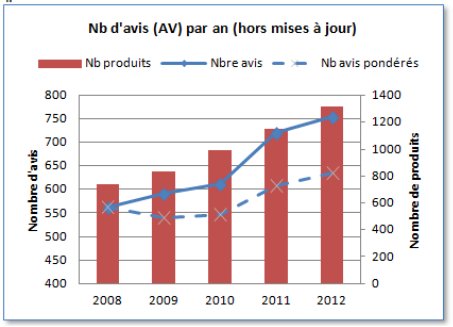
Plan de la présentation

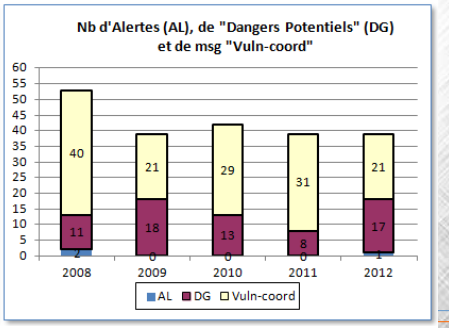
- 1) Veille sur les vulnérabilités et les menaces
- 2) Evénements majeurs de 2012
  - SCADA : la menace s'amplifie
  - APT : une évolution majeure de la menace pour l'entreprise
  - 0-day : un risque plus grand qu'estimé jusqu'à présent
- 3) Sujets d'actualité
  - Cloud, BIG data, smartphones, BYOD, etc…

1: Veille sur les vulnérabilités et les menaces

Avis, Dangers Potentiels et Alertes émis en 2012

- 755 Avis de sécurité (AV) émis en 2012
  - Le nombre de vulnérabilités (AV) découvertes par an ne faiblit pas
  - Un système non mis à jour se dégrade donc au fur et à mesure du temps
- 1 Alerte (Java) et 17 Dangers Potentiels (DG)
  - Le danger provient souvent du fait que des vulnérabilités récentes sont intégrées aux outils d'attaques
  - Cette intégration est de plus en plus rapide : Vulnérabilité ⇨ Metasploit ⇨ Blackhole





Les Alertes et DG émis par le Cert-IST en 2012

- Enormement : Java
- Beaucoup : Internet Explorer & Windows (mais Mac OS-X n'est pas sans défauts)
- Un peu : Android, Flash (pas de DG Adobe Reader en 2012)
- Autres
  - Quelques failles graves peu médiatisées : Oracle, Samba, Networker, ClearQuest
  - 1er DG sur un produit SCADA (Schneider-Electric)
  - Vol de code source (PCAnywhere), vulnérabilités Sophos

Industrie Services Tertiaire

Computer Emergency Response Team
Industrie Services Tertiaire

2: Evénements majeurs de 2012 (pour les menaces visant les Entreprises)

1) SCADA : la menace progresse

- SCADA = Supervisory Control And Data Acquisition
  - Ce terme est employé au sens large pour désigner l'informatique industrielle
- L'année 2010 a été l'année de la découverte de STUXNET
  - Ver probablement conçu pour détruire les centrifugeuses iraniennes d'enrichissement nucléaire.
  - Depuis, les chercheurs de failles s'intéresse au SCADA (ex: Luigi Auriemma – revuln.com , Gleg.net : « Agora SCADA+ exploit pack »)
- Actualité 2012 :
  - Pas d'incident majeur, mais plusieurs attaques visant le domaine de l'énergie :
    - Shamoon contre Aramco, Intrusion chez Telvent (Schneider) visant le produit OASys
  - Un niveau de sécurité parfois inquiétant
    - 500 000 équipements industriels accessibles depuis Internet ? (moteur de recherche Shodan)
    - Une nouvelle classe de failles ? : les « forever-day » (aka « insecure by design)
  - Les professionnels du SCADA se mettent à publier des failles
    - Projet « Base camp » de Digital-Bond
    - Les vulnérabilités identifiées sont plus critiques
- La sécurisation des systèmes SCADA est une préoccupation majeure

2) Attaques par infiltration (APT)

- Sujet préoccupant depuis 2 ans
  - Les attaques se multiplient et touchent un plus grand nombre d'organismes (changement d'échelle)
  - Beaucoup d'organismes sont vulnérables
  - Phénomène révélateur d'une montée de la sécurité offensive
  - Effet boule de neige ?
- Qui sont les attaquants ?
  - Des états ? (pour des objectifs stratégiques)
  - Des individus isolés ? (agissant pour des commanditaires)
  - Bientôt des cyber-groupes indépendants ? (agissant pour eux-mêmes dans l'objectif de revendre leurs prises)
- Ce risque doit être pris en compte par les entreprises

Paysage actuel de la menace

- Attaques par des amateurs
  - Defacement de sites web
  - Attaques par des Anonymous
- Attaques par des professionnels
  - Cyber-criminels visant le grand public (depuis 2005)
    - Spam
    - Botnets
    - Vol de données bancaires
    - Escroquerie visant le particulier (faux antivirus, ransomware « virus de la Police »)
  - Cyber-espions : Attaques par infiltration (APT)
    - cyber-espionnage ou sabotage
- Les attaques par infiltration sont un risque nouveau pour les entreprises.

Attaques par infiltration (APT)

- Comment contrer ces attaques ?
  - Renforcer les fondamentaux :
    - sensibiliser les utilisateurs,
    - renforcer les mots de passes, limiter les comptes administrateurs,
    - protéger les données sensibles sur des serveurs sécurisés,
    - appliquer les correctifs de sécurité et mettre en place une collecte et une gestion des logs.
    - Ex : 20 Critical Security Controls for Effective Cyber Defense (USA)
    - Ex : Guide de l'hygiène informatique (France – ANSSI)
  - Mettre en place une surveillance active au sein de l'entreprise, au travers d'une structure responsable de la supervision de la sécurité.
  - Définir une procédure de réaction en cas d'incident définissant le comportement à adopter et les personnes à impliquer. Traiter les attaques par une équipe spécialisée

3) Augmentation du risque 0-day

- 0-day : Vulnérabilité gardée secrète jusqu'au jour où elle est utilisée dans une attaque réelle
- Depuis 2005 on sait que le risque 0-days existe
- On se rend compte aujourd'hui que le risque est plus grand qu'estimé jusque là
  - Quatre 0-days utilisés en 2010 dans une seule attaque (Stuxnet)
  - L'étude Elderwood (Symantec - 2012) montre que certains groupes (sponsorisés par des états ?) possèdent de nombreux 0-days
  - L'étude « Before we knew it » (Symantec - 2012) estime qu'un 0-day reste en moyenne non découvert pendant 300 jours

3) Augmentation du risque 0-day

- Il faut intégrer le risque 0-day à la gestion de la menace
  - Détecter au plus tôt que cet événement s'est produit,
  - Limiter la conséquence pour le S.I. de la compromission d'un poste de travail ou d'un serveur,
  - Définir une procédure d'isolation, d'analyse d'impact et de remise en service des éléments compromis.

3 : Sujets d'actualité

Actualité 2012 [1/4]

- Cloud : les risques sont désormais bien identifiés
  - 2010 : Attention danger ! : les experts préviennent des dangers potentiels
  - 2011 : Le détail des difficultés : les experts détaillent les difficultés sur les volets contractuels, juridiques et techniques
  - 2012 : Prêts pour la mise en pratique : les RSSI connaissent désormais bien les difficultés et les chantiers à couvrir dans un projet Cloud. L'effort à déployer est bien sûr proportionnel au niveau de sécurité à assurer.
- BIG-Data : Sujet à la mode, ou réel problème pour les entreprises ?
  - Big data = small security ?
  - Big data = Big Brother ?

Actualité 2012 [2/4]

- Smartphones : Pas d'évolution significative de la menace
  - Android est la plate-forme préférée des malwares mobiles
  - Montée en flèche du nombre de malwares détectés par les éditeurs antivirus
  - La majorité des attaques consistent à cloner des applications à succès et à leurs ajouter une fonction cachée qui génère automatiquement des appels vers des numéros surtaxés
  - Les techniques d'attaques reproduisent les techniques connues du mode IT : (drive-by download, botnet, Ransomware).
  - Pas de cas d'attaque sophistiquée répertorié
- Réseaux sociaux : R.A.S.
- Hacktivisme : Des revendications fantaisistes montrent certaines limites des mouvements de type Anonymous

Actualité 2012 [3/4]

- BYOD : le sujet le plus commenté en 2012
  - Phénomène émergeant avec des risques réels
  - Prolongement du Cloud ? (en termes de risque)
  - Pas d'incident connu ou le BYOD aurait été un vecteur d'attaque (mais c'est théoriquement possible)
- Cyber-espionnage et APT
- La montée des états
  - Mise en place ou le renforcement de structures dédiées à la cyber sécurité (ANSSI = 2009)
  - Officialisation de la possibilité de cyber-guerres (USA 2011 = Plan « Cyber 3.0 ») (OTAN 2012 = Manuel de Tallinn)
  - Médiatisation d'incidents supposés d'origines étatiques : Chine, USA, Israel, Iran ?

Actualité 2012 [4/4]

- Cybercrime : 2012 a vu la montée en flèche des ransomwares avec le malware « Reveton » (malware de la Police)
- Vol de données personnelles (logins, mots de passe, numéros de cartes bleues, etc.)
  - Le phénomène s'amplifie d'années en année. Exemples :
    - Zappos : 24 millions de coordonnées clients volées en janvier 2012
    - LinkedIn : 6,5 millions de comptes volés en juin 2012
    - Apple : 12 millions de données relatives à des terminaux iPad, iPod et Iphone volés en septembre 2012
    - Etc.

Computer Emergency Response Team
Industrie Services Tertiaire

Conclusions

Conclusions

- **L'entreprise doit composer avec une situation complexe**
  - Un risque accru d'attaque
    - Risque d'APT, risque SCADA, risque d'Hacktivisme
  - Une demande utilisateur pour plus d'ouverture (Cloud, BYOD, etc…)
  - Il faut connaitre les risques pour arbitrer
    - Le Cert-IST donne une vision argumenté de la menace
    - Et rappelle que le modèle de sécurité éprouvé est celui de la sécurité en profondeur

- **La veille sur les vulnérabilités et menaces est une composante indispensable de la SSI**
  - Importance de la gestion des vulnérabilités dans l'entreprise
    - 4000 vulnérabilités par an, 800 avis de sécurité Cert-IST
  - Il ne s'agit pas simplement de déployer des correctifs
    - Mise en place de mesures de protections spécifique en cas de menace
    - Considérer que la compromission d'un poste ou un serveur est un événement possible

Industrie Services Tertiaire

www.cert-ist.com