COMPTE RENDU DE LA REUNION DU 18/10/2011

Présents:

Jean-Philippe Payet
Isabelle Ginet-Kauders
Olfa Dhouib
Jean-Pierre Guiné
Alain Gérard
Sébastien Lamour
Bernard Besson
Eric David
Pascal Lointier
Claude Aschenbrenner
David Commarmond:
Séverine Dissard
Louise Mercier

L'essentiel de la séance a été consacrée à la présentation de Pascal Lointier, du Clusif.

Présentation Pascal Lointier - président CLUSIF / Responsable sécurité compagnie d'assurance

Clusif:
Le CLUSIF est le Club de la Sécurité de l'Information Français
C'est une Association sans but lucratif, créé dans les années 80 et qui regroupe + 600 membres (fournisseurs, prestataires, entreprises utilisatrices …)
Il met à disposition des groupes de travail, des espaces dédiés, un panorama de la cybercriminalité, des conférences

Agenda et présentations de cas concret de vulnérabilités:

1. Stuxnet: les mystères d'une cyber-attaque industrielle
2. Services Généraux
3. Crime sur mobile

1. **Stuxnet**:

C'est un exemple d'une "advanced persistente threat" (attaque lente & persistente, qui se propage sur +1 an)
Il correspondait à une attaque sur les centrifugeuses.
L'objectif réel n'est toujours pas officiellement identifié. De nombreuses théories du complot ont vu le jour.
Publiquement, il s'agit de la première fois qu'un système de production (l'informatique industrielle) est visé.

2. Les services généraux:

Exemple de CodeRed – moteur de recherches de toutes les adresses IP extrêmement rapide -> saturation de la bande passante mais aussi découverte de nouvelles machines telles que les imprimantes (les Multi Function Printer). Pas de chiffrement (souvent que du codage propriétaire) de ces machines, qui sont souvent gérées par les Services Généraux (qui n'ont pas nécessairement la sensibilité à la sécurité informatique et laissent des failles)

Exemple d'équipements attaqués:
- videos et alarmes par wifi
- groupe électrogènes
- cartes de contrôle d'accès (dont accès à des zones sécurisées)
- SCADA
- système de ventilation d'un hopital

Importance prise par le déploiement d'OS type Windows CE, Pocket PC avec des supports à distance -> augmente les risques.

3. Le crime est de plus en plus mobile

Tous les téléphones sont attaquables. Historique depuis 1980.
Les types d'attaques: bluetooth, MMS, cable, carte SD,
On considère que l'App Store contient près de 20% de programmes malveillants