Computer Emergency Response Team
Industrie Service Tertiaire

Simulation d'une montée de crise

Industrie Services Tertiaire

Juin 2008

Agenda

- Simuler une montée de crise à travers un scénario réaliste
- Expliquer la réaction de chaque acteur
  - Entreprise (Alcatel-Lucent)
  - Constructeur (Microsoft)
  - CERT (Cert-IST)
- Participants
  - Alcatel-Lucent
    - Hervé Chappe
    - Jalel Mzali
  - Microsoft - PSS Security in EMEA
    - Jean Gautier
    - Jérôme Leseinne
  - Cert-IST
    - Philippe Bourgeois

Industrie Service Tertiaire

Vue globale du scénario

- Une vulnérabilité est découverte dans Abobe Flash
- Des postes de l'entreprise se font infecter
  - Un prermier poste se fait infecter en visitant un site web Internet ("drive-by download")
  - L'infection se propage sur un site web intranet (injection SQL) et infecte ensuite les utilisateurs de l'intranet
  - Les postes infectés joignent un "botnet" et reçoivent l'ordre d'envoyer du SPAM
- La crise éclate
  - La SPAM provoque par effet de bord un **déni de service sur le DNS**
  - La perte du DNS bloque de nombreux utilisateurs
- Le traitement de la crise
  - Réaction à chaud
  - Identification de la "root cause" et désinfection du parc

Industrie Service Tertiaire

Simulation d'une montée de crise

- Une vulnérabilité est découverte dans Abobe Flash

- Cas nominal : un correctif est disponible
  - Réaction des participants ?
  - Complexité induite par le fait que la vulnérable touche un composant "tiers" ?
  - En cas d'accélération de la menace que se passe-t-il ?
- Cas d'une attaque 0-day

Industrie Service Tertiaire

Simulation d'une montée de crise

- Des postes de l'entreprise se font infecter
  - Un premier poste se fait infecter en visitant un site web Internet ("drive-by download")
  - L'infection se propage sur un site web intranet (injection SQL) et infecte ensuite les utilisateurs de l'intranet
  - Les postes infectés joignent un "botnet" et reçoivent l'ordre d'envoyer du SPAM
- Cette phase a de fortes "chances" de passer inaperçue …
  - Quels sont les moyens de protections (et quelle est leur efficacité) ?
  - Comment anticiper ou éviter la crise ?

Industrie Service Tertiaire

Simulation d'une montée de crise

- La crise éclate
  - La SPAM provoque par effet de bord un **déni de service sur le DNS**
  - La perte du DNS bloque de nombreux utilisateurs
- Quelle est la réaction de l'entreprise face à un incident ?
  - Comment évaluer la portée de l'incident ?
  - Collaboration entre les équipes SSI et les équipes opérationnelles ?

Industrie Service Tertiaire

Simulation d'une montée de crise

- Le traitement de la crise
  - Réaction à chaud
  - Identification de la "root cause" et désinfection du parc

- Comment l'entreprise gère-t-elle la crise ?
  - Qui sont les acteurs et quels sont leurs rôles ?
  - Quelles sont les priorités ?
  - Qui pilote la crise ?

Industrie Service Tertiaire

Conclusion