Computer Emergency Response Team
Industrie Services Tertiaire

Cert-IST et les nouvelles frontières de l'entreprise

Forum 2009

Philippe Bourgeois

Plan de la présentation

- Les activités du Cert-IST pour l'entreprise maître de son SI
- L'évolution des frontières et l'impacts pour l'entreprise
- La prise en compte des nouvelles frontières

Computer Emergency Response Team
Industrie Services Tertiaire

Les activités du Cert-IST pour l'entreprise maître de son SI

Les domaines de responsabilité

- Le niveau de sécurité du SI dépend de :
  - L'architecture initialement définie
  - Le maintien dans le temps du niveau de protection

- Le Cert-IST a la responsabilité de :
  - Veiller pour identifier les nouvelles vulnérabilités impactant les composants techniques du SI
  - Alerter en cas de menace grave nécessitant des actions spécifiques de protection

- L'entreprise a la responsabilité d'appliquer les mesures adéquates de protection sur les éléments de son SI.

Les activités du Cert-IST

- Le suivi des vulnérabilités
  - Le Cert-IST émet des avis de sécurité pour informer sa communauté des vulnérabilités dès qu'un moyen fiable de protection existe (correctif ou palliatif).
  - Les avis de sécurité permettent aux responsables de plates-formes de maintenir leurs parcs machines au niveau maximum de protection.
  - Le Cert-IST émet par an de l'ordre de 600 avis de sécurité (+ 1000 mises à jours)

- Le suivi des menaces
  - Le Cert-IST émet des Alertes (AL) ou des Danger Potentiel (DG) lorsqu'il y a un risque important que des attaques se produisent (ex: une vulnérabilité est « wormable »).
  - Les Alertes et Dangers indiquent aux responsables sécurité les situations d'alertes où des actions spécifiques de protection doivent être entreprises (par exemple la mise en place d'un filtrage en périphérie de l'entreprise).
  - Le Cert-IST émet par an de l'ordre de 10 DG et 2 AL.

Evolution du modèle de gestion des vulnérabilités

- Modèle centré au départ sur les moyens du SI de l'entreprise
  - Protection des systèmes de l'entreprise (maintien à jour en terme de sécurité)
  - Application de mesures de protection périphériques en cas de menace

- L'évolution des frontières impacte ce modèle
  - Externalisation des moyens
  - Transfert de responsabilité

Computer Emergency Response Team
Industrie Services Tertiaire

L'évolution des frontières et les impacts pour l'entreprise

CERTIST
Industrie Services Tertiaire

Les anciennes "nouvelles frontières"

- Le SI a connu récemment des évolutions significatives
  - Nomadisme (télétravail)
  - Convergence IP (VoIP, ToIP)

- Ces évolutions technologiques ne modifient pas le périmètre des responsabilités de l'entreprise
  - L'entreprise conserve le contrôle complet des moyens mis en œuvre.
  - Elle a, pour ces moyens, la responsabilité de
    - La protection
    - La mise en conformité
    - Du contrôle d'accès
    - …

Les nouvelles frontières examinées aujourd'hui

- Les réseaux industriels (SCADA)

- Les solutions externalisées choisies (Cloud – SaaS)

- La perméabilité des frontières existantes
  (détournement de l'accès web autorisé)

  - Les outils que mes fournisseurs et clients m’imposent (WebEx, GotoMyPC, etc..)

  - La génération spontanée des "services web" (Web 2.0, facebook, etc…)

Computer Emergency Response Team
Industrie Services Tertiaire

La prise en compte des nouvelles frontières

Les réseaux industriels (SCADA)

- Implications sécurité
  - Les réseaux industriels ne sont pas isolés (interconnexions réseaux, clés USB)
  - Des incidents arrivent de temps en temps accidentellement (infections virales)
  - La possibilité d'attaques volontaires est une préoccupation majeure depuis Sept. 2001
- Les particularités du monde SCADA
  - Forte culture sûreté de fonctionnement (safety)
  - Monde très séparé du monde de la sécurité informatique "IT"
  - Des solutions "boites noires", peu ou pas de communication des fournisseurs sur la sécurité
  - Difficultés d'appliquer des correctifs de sécurité sur les chaines opérationnelle

- L'expérience des CERT doit servir de modèle pour la gestion des vulnérabilités
  - Apporter le savoir faire du monde "IT" pour la veille et l'alerte
- L'entreprise doit adopter une démarche structurée pour gérer la sécurité
  - Identifier les SCADA sensibles (Analyse de risque)
  - Définir des processus de réponse appropriés
    - Isolation des ressources critiques en cas de menace
    - Patch management

Les solutions externalisées choisies (Cloud – SaaS)

- Qu'est ce que le SaaS et le Cloud ?
  - Une délégation d'une partie des moyens du SI à un tier, externe à l'entreprise
  - L'entreprise n'a plus la responsabilité de la plate-forme technique

- Les Implications sécurité
  - Quel est le niveau de sécurité de mon fournisseur ?
  - Quel est son processus de maintien de ce niveau de sécurité
    - Processus de veille sur les menaces ? / Processus de patch-management ?
  - Quelle collaboration en cas d'incident de sécurité ?

- L’apport d’un CERT
  - Le CERT du fournisseur : pour le maintien du niveau de sécurité de ses infrastructures
  - Le CERT de l'entreprise : pour être au courant des situations à risque (Alertes)
  - Collaboration inter-CERT au travers de réseaux de confiance (ex: FIRST)
- Les implications pour l'entreprise
  - Analyser les risques et les traduire en engagements contractuels
  - Suppression de contraintes techniques / au profit de problèmes juridiques (dans un contexte souvent transfrontalier)

Les outils que mes fournisseurs et clients m'imposent (WebEx, GotoMyPC, etc..)

- Spécificités
  - Outils à génération spontanée. Exemple :
    - Un utilisateur est invité à une WebConférence
    - Un fournisseur propose une maintenance à distance via Internet
  - Ces outils savent passer outre les firewalls (tunneling HTTP-HTTPS). Il n'existe pas de solution de blocage universelle (mais des "trucs" permettent de bloquer au cas par cas)
  - C'est l'explosion des fonctionnalités (aka « convergence »)
    - L'outil de web-conférence sait faire de la prise de contrôle à distance
    - L'outil de télé-administration sait faire de la télé-conférence
- L'apport d'un CERT
  - Mutualisation entre adhérents : échange de retour d'expérience (nouveaux outils, méthode de blocage).
- Recommandations pour l'entreprise
  - Définir clairement la politique sécurité de l'entreprise
  - Structurer les besoins :
    - Identifier les besoins / Identifier les risques
    - Emettre des recommandations

La génération spontanée des services web (Web 2.0, facebook, etc…)

- Implications sécurité de FaceBook
  - La fuite de données
  - Les attaques des utilisateurs via une vulnérabilité ou par ingénierie sociale

- La situation est comparable à un SaaS … mais sans cadre contractuel entre le fournisseur et l'entreprise.

- L’apport d’un CERT (en cas de vulnérabilités)
  - Emission d'alerte en cas de menace critique

Q & R ?

Fin de la présentation