Computer Emergency Response Team
Industrie Services Tertiaire

Le Cert-IST
Déjà 10 ans !

Forum 2009

Pierre Klein
Président du Cert-IST

Sommaire

- Genèse du Cert-IST
- Le Cert-IST en quelques chiffres
- Ses évolutions
- Le Cert-IST face aux nouvelles frontières de l'Entreprise

Genèse du Cert-IST

L'Histoire du Cert-IST

- Phase pilote au CNES depuis 1997

- Création du Cert-IST en 1999 par le consortium

  - Objectif : Mutualisation des ressources et des connaissances

- Le Cert–IST devient une association Loi 1901 le 26 avril 2003

  - Objectif : Assurer pour ses membres (adhérents et partenaires) des services de prévention des risques, d'assistance aux traitement d'incidents.

Le Cert-IST au-delà des frontières

Partenaire National

- Collaboration permanente avec les 2 autres Certs Français
  - CertA, Cert-Renater
- Liens privilégiés avec les autorités nationales
  - OCLCTIC, SGDN
- Liens privilégiés avec les éditeurs de sécurité
  - McAfee, Microsoft, …

Partenaire Européen

- Le Cert-IST a été le coordinateur du projet européen EISPP
  - Travail collaboratif avec le Cert-Siemens, Cert Barcelone, CLUSIT, Callineb Suède
  - Définition d'un format commun d'avis
  - Etude des services Cert pour les PME/PMI
- Membre de la TF-CSIRT (Réseau européen des Certs et CSIRT)
  - Accrédité « TI level 2 »

Le Cert-IST au-delà des frontières

Partenaire International

- Membre du FIRST (Réseau mondial des Certs) depuis 1999
  - Echanges fréquents avec les autres Certs
  - Canal d'information privilégié

- Membre en tant que Cert du « Security Cooperation Program » de Microsoft

- Echanges privilégiés avec le Cert-TCC (Tunisie)

- Support quotidien :
  - Contre l'hébergement d'activités malveillantes sur des « machines » impactant nos adhérents (ex. Phishing, etc)
  - Collaboration avec le projet ShadowServer dans le cadre de l'identification de machines compromises en France

Le Cert-IST en quelques chiffres

Cert IST
Industrie Services Tertiaire

Nos productions en quelques chiffres

- En termes de veille technologique
  - 1999 : 280 produits suivis

  …
  - 2003 : 525 produits suivis

  …
  - Aujourd'hui : 770 produits suivis et 6600 versions

- En termes d'avis produits
  - 1999 : 294 avis

  …
  - 2003 : 392 avis

  …
  - 2008 : 563 avis

  Depuis 1999 : plus de 4600 avis produits et plus 7500 vulnérabilités traitées

- En termes de « Gestion des menaces »
  - Depuis 1999 : 45 Alertes
  - Depuis 2003 : 68 DG dont 15 avec un niveau de risque très élevé
  - Depuis 2005 : 66 hubs de crise

- Et c'est aussi :
  - 140 « Bulletins mensuels » depuis 1999 (en anglais depuis 2005)
  - 484 articles

Computer Emergency Response Team
Industrie Services Tertiaire

Les évolutions du Cert-IST

Evolutions des services depuis 1999

- Evolutions de 1999 à nos jours
  - Veille technologique
    - Avis de sécurité, Alertes de sécurité et Base de vulnérabilités
  - Assistance téléphonique
  - Sites web (public/privé)
  - Gestion de crise (hub)
  - Workflow (XML)
  - Veille média
  - Échanges avec les autres organismes
    - Certs français, FIRST, TF-CSIRT
  - Investigations / Interventions sur incident
  - Coordination d'incidents (FR, INT)
  - Etudes de sécurité / Articles de sécurité / Support
  - Transfert de compétences
  - *Formations*

1999 :

Création du Cert-IST

Reconnaissance FIRST

2000 : www.Cert-ist.com

2003 : Association Loi de 1901

2005 :

Site web

Gestion de Crises

« HUB »

2007-2008 :

Veille média

Industrie Services Tertiaire

Axes majeurs

- Maturité du service de veille technologique
  - Productions adaptées aux besoins des entreprises
    - Qualification des vulnérabilités (niveau de risque, solutions)
    - Analyse des menaces (Alertes, hub de crise)
    - Envois simultanés de toutes les publications en français et en anglais
  - Processus maîtrisé et professionnel
    - Arbre de décision, métrique
    - Enrichissement permanent de la base de connaissance
    - Coopération avec les Certs français en cas d'alerte
- Effort de mutualisation
  - Mutualisation des connaissances
  - Espace d'échanges entre membres (forum)
- Participation aux conférences internationales
  - Du FIRST, de la TF-CSIRT

Computer Emergency Response Team
Industrie Services Tertiaire

Le Cert-IST face aux nouvelles frontières de l'Entreprise

Evolutions des frontières par les vulnérabilités

- Des malwares de plus en plus virulents, répandus, mais surtout hautement avancés techniquement
  - Conficker/Downadup
- Les systèmes industriels plus vulnérables
  - SCADA
- Des vulnérabilités d'implémentation
  - Faille DNS, TCP-Dos
- SAP Pentest framework (SAPYTO)

Evolutions des frontières par les technologies

Les besoins de l'Entreprise déplacent les frontières traditionnelles.

- Convergence des technologies
  - voix, conférence, télé-administration, vidéo, etc.
- Le nomadisme
  - Portable, VPN, télétravail, travail collaboratif, externalisation de l'activité
- L'émergence des réseaux sociaux
  - Facebook, Yammer, Twitter, LinkedIn, etc.
- Le Cloud-Computing ou le Software-as-a-Service (SaaS)

En termes de Sécurité,

les Entreprises sont-elles réellement préparées à

l'évolution de leurs frontières ?

Les maîtrisent-elles réellement ?

Comment un Cert peut les aider ?

Fin de la présentation