Enjeux de sécurité des infrastructures SCADA

17/04/2008

En partenariat avec :

BlackBerry – CA – McAfee – Orange Business Services – Orsyp –TelecityGroup

Le CLUSIF : agir pour la sécurité de l'information

Association sans but lucratif (création au début des années 80)

> 600 membres (pour 50% fournisseurs et prestataires de produits et/ou services, pour 50% RSSI, DSI, FSSI, managers…)

Partage de l'information

- Echanges homologues-experts, savoir-faire collectif, fonds documentaire

Valoriser son positionnement

- Retours d'expérience, visibilité créée, Annuaire des Membres Offreurs

Anticiper les tendances

- Le « réseau », faire connaître ses attentes auprès des offreurs

Promouvoir la sécurité

Adhérer…

La dynamique des groupes de travail

Des livrables en libre accès

Des traductions en anglais

Des prises de position publiques ou des réponses à consultation

Des espaces d'échanges permanents :MEHARI, Menaces, RSSI

Les groupes actifs en 2008

- Botnet
- Conception d'un centre informatique sécurisé
- Criminalistique
- Documentation de MEHARI™
- Enquête sur les politiques de sécurité et la sinistralité informatique en France
- Fiches de sécurité pour la micro-informatique
- Gestion des incidents
- Infogérance
- Intégration de MEHARI™
- Label Formation CLUSIF
- Métriques 7799
- Malveillance téléphonique
- MEHARI 2007
- Panorama de la cybercriminalité

Agenda de session

Introduction : définitions, incidents

- ✓ **M. Pascal Lointier**, Président du CLUSIF, Conseiller en Sécurité de l'Information (AIG Europe)

Adaptation des pratiques de sécurité des SI aux infrastructures critiques

- ✓ **M. Yannick Fourastier**, Ingénieur de Recherche (EADS France)

RTE France : Enjeux de sécurité des infrastructures SCADA pour le transport de l'électricité

- ✓ **M. Philippe Bedu**, Département Urbanisation et Solutions Informatiques (RTE France)
- ✓ **Frédéric Lenoir** , Architecture Sécurité Téléconduite

Eau de Paris : éléments techniques et organisationnels de sécurisation du système d'alimentation en eau de Paris

- ✓ **M. Jacques Coutelan**, Chef du service Informatique et Télécommunications
- ✓ **M. Frank Montiel**, Adjoint du chef du service Informatique et télécommunications

Les images sont D.R.

SCADA ?

Ce n'est pas une danse brésilienne ☺

Supervisory Control And Data Acquisition (commande et acquisition de données de surveillance)

- ✓ Télégestion à grande échelle réparti au niveau des mesures et des commandes
- ✓ Transmission et distribution de fluides et services essentiels : eau, gaz, électricité, produits chimiques ou signalisation, etc.

Mais aussi, dans une acceptation plus large, l'informatique industrielle et son réseau local, quelque soit la taille de l'entreprise (cf. PME)

Des enjeux

Au niveau macro économique, gestion de la criticité

- ✓ Secteur d'Activité d'Importance Vitale (SAIV, 06/2006)
- ✓ Directive Nationale de Sécurité
- ✓ Nouvelle sensibilisation (E-U) après les événements 2001

Au niveau entreprise, des impacts sur l'activité et le besoin d'assurances

- Perte de chiffre d'affaires et/ou pénalités/amendes
- Risque d'environnement et de pollution
- Responsabilité civile vis-à-vis de tiers
- Image et notoriété
- Dommages corporels…

Accidents (hors S.I.)...

Texas City Explosion 3/23/05

- Gauge-in-error assumed correct
- Accurate-gauge assumed wrong.
- 15 dead, 170 injured, economic losses in excess of $1.5 billion

(Chemical Safety Board)

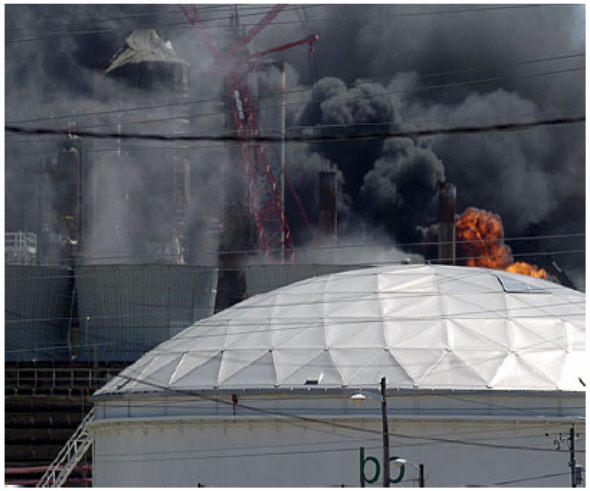


Photo by Dwight C. Andrews

Homeland Security

5th Annual Boise ISSA InfoSec, April 25, 2007

Bellingham (USA), 1999 : 3morts. Très récemment, le système informatique a été mis en cause également

Accidents et malveillances (via le S.I.)

- 2003 : ver Slammer et site nucléaire (Ohio)
- 2003 : ver Nachi et réseau DAB (billeterie) Diebold
- 2003 : virus SoBig et signalisation ferroviaire (Floride)
- 2005 : ver Zotob, arrêt de 13 usines d'assemblage de véhicules (E-U)
- 2007 : erreur de commande et contamination accidentelle (hydroxide de sodium) des eaux de ville, dizaines de victimes, blessures légères (Michigan)

Accidents et malveillances (via le S.I.)

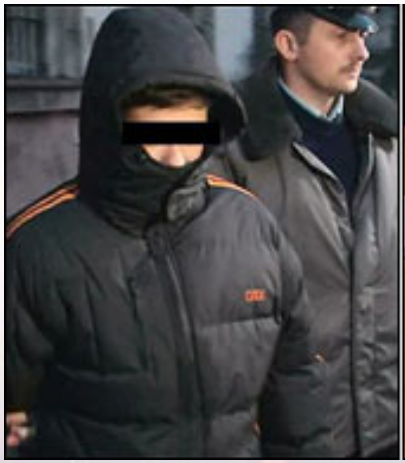
- 2007 : bombe logique d'un employé sur un système de contrôle d'irrigation des eaux de barrage (Californie)
- 2007 : prise de contrôle et perturbation des feux de signalisation (Californie)
- 2007 (et 2000 en Australie) : sabotage logique par un administrateur réseau du système d'approvisionnement en eau (Californie)
- 2007 destruction expérimentale d'un générateur électrique (Idaho pour CNN)
- 2008 : prise de contrôle et déraillement de 4 wagons, plusieurs blessés (Pologne)

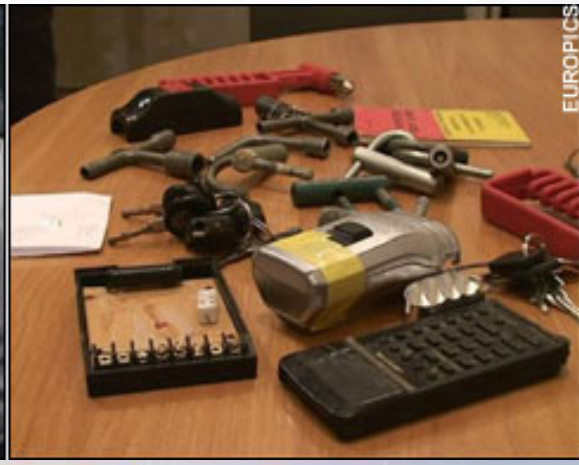
Malveillances (via le S.I.)

« Exercice » de destruction d'une turbine à partir d'une faille de sécurité, depuis corrigée

http://www.cnn.com/2007/US/09/26/power.at.risk/index.html

Pologne, déraillement de 4 wagons par un adolescent

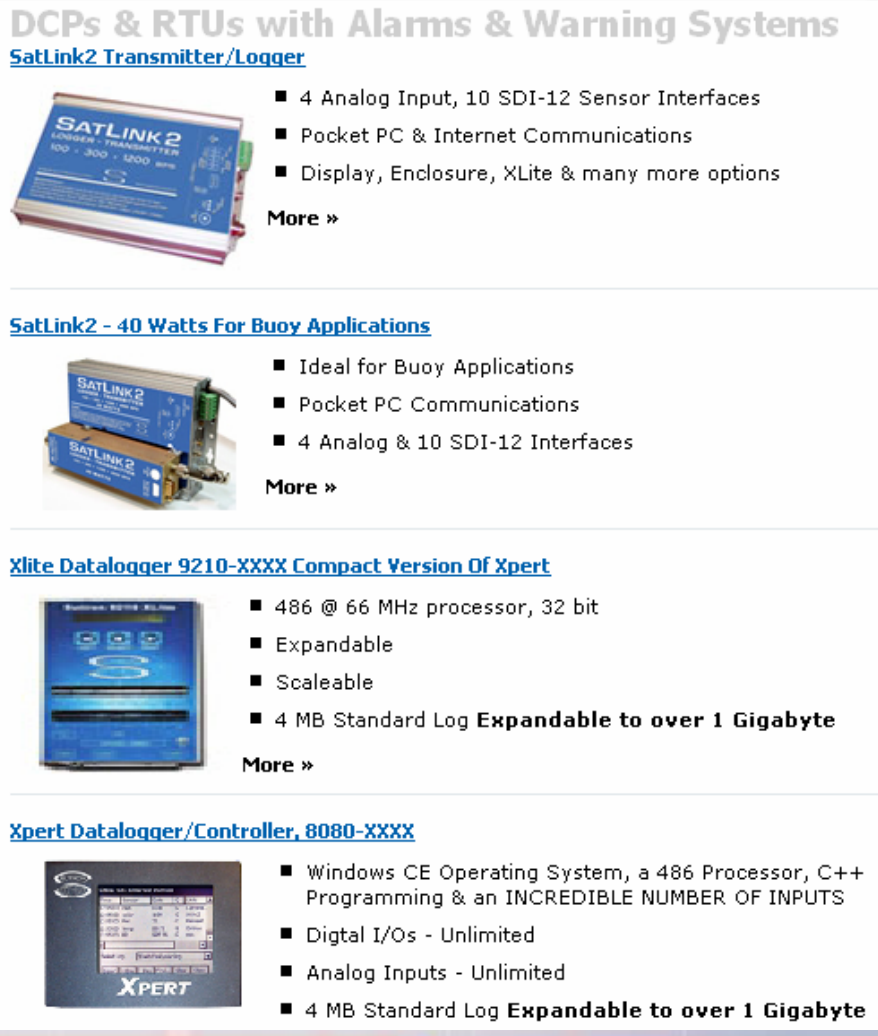




2007 : une actualité spécifique

L'offre commerciale des équipements qui utilisent désormais des technologies publiques

- ✓ TCP-IP, ethernet
- ✓ Systèmes d'exploitations Windows (CE), etc.
- ✓ Télémaintenance pour accès par les spécialistes des équipements (interconnexion Internet)



2007 : une actualité spécifique

Volumétrie importante de livrables, documentations sur la sécurité SCADA

- ✓ Idaho National Laboratory
- ✓ NIST (SP800-82)
- ✓ SANS
- ✓ TSWG
- ✓ US-CERT…

SCADA (in)Security

- HITB SecConf 2007 (Malaisie)
- 24C3 (CCC, Berlin)
- Black-Hat DC (2008)

Un contexte spécifique, une nécessaire adaptation de la SSI

(source : INL Critical Infrastructure Protection Center, 2007)

SECURITY TOPIC	INFORMATION TECHNOLOGY	CONTROL SYSTEMS
Anti-virus & Mobile Code Counterfeasures	Common & widely used	Uncommon and difficult to deploy
Support Technology Lifetime	3-5 Years	Up to 20 years
Outsourcing	Common & widely Used	Rarely Used
Application of Patches	Regular/Scheduled	Slow (Vendor specific)
Change Management	Regular/Scheduled	Legacy based – unsuitable for modern security
Time Critical Content	Delays are generally accepted	Critical due to safety
Availability	Delays are generally accepted	24x7x365 (continuous)
Security Awareness	Good in both private and public sector	Generally poor regarding cyber security
Security Testing/Audit	Scheduled and mandated	Occasional testing for outages
Physical Security	Secure	Very good but often remote and unmanned

Premières conclusions…

Potentiellement tout secteur d'activité et toute taille d'entreprises

- Une exposition similaire, peut-être supérieure, pour une PME ayant une informatique industrielle sans toutefois une conscience du risque ou des enjeux
- Des événements accidentels mais aussi des malveillances (personnel interne, hackers). Crime organisé, (cyber)-terrorisme ?

Créer/renforcer l'échange d'information entre le RSSI et le Responsable de la Production

Webographie

http://www.theregister.co.uk/2007/05/21/alabama_nuclear_plant_shutdown/
http://www.informationweek.com/story/showArticle.jhtml?articleID=13100807
http://www.theregister.co.uk/2007/11/30/canal_system_hack/

http://www.networkworld.com/news/2007/112907-insider-charged-with-hacking-california.html

http://www.cnn.com/2007/US/09/26/power.at.risk/index.html
http://www.theregister.co.uk/2003/11/25/nachi_worm_infected_diebold_atms/
http://www.securityfocus.com/news/11351
http://www.forbes.com/2007/08/22/scada-hackers-infrastructure-tech-security-cx_ag_0822hack.html

http://blog.wired.com/27bstroke6/2008/04/industrial-cont.html
http://www.eetimes.com/showArticle.jhtml?articleID=205918880
http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2008/01/11/wschool111.xml

http://www.industrialdefender.com/
http://www.us-cert.gov/control_systems/
http://byressecurity.com/