CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

SCADA :
Qui ? Quoi ? Comment ?

6 juin 2009

Journée CERT-IST

Pascal Lointier
Président du CLUSIF
Conseiller sécurité de l'information, AIG Europe

CLUSIF

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 7 NUMBER 8

FEBRUARY 2009
SCADA

Featured in this month's issue of *The CIP Report* are Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems monitor and control the processes of many of our Nation's infrastructures. The security and safety of transportation, water, communications, and many other vital parts of our everyday lives all rely on SCADA systems. In this issue we look at some of the different SCADA systems and their applications.

Melbourne, mai 2009 :

SECURING SCADA SYSTEMS '09

Managing Change, Security & Configuration of SCADA Systems

MIT (#Boston), 2007

Pourquoi ?

Nouvelles opportunités de malveillance en environnement industriel

- 2007, ouverture et standardisation des systèmes
  - TCP/IP, éthernet
  - Windows CE (embedded, v.6, www.microsoft.com/windowsembedded/en-us/news/events/teched.mspx)
  - Télémaintenance
- Diffusion des savoirs
  - Sabotage par salarié
  - Cyber-terrorisme (un jour, peut-être)
  - Violences politiques (dont éco-terrorisme)
  - ...

Quoi ? 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

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

Homeland Security

5th Annual Boise ISSA InfoSec, April 25, 2007

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 pour le Ph) des eaux de ville, dizaines de victimes, blessures légères (Michigan)

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 (Lodz), déraillement de 4 wagons par un adolescent

Où ?

Bien sûr, les infrastructures macroéconomiques

- Transports
- Acheminements des fluides

Mais, en fait, la PME à production assistée par ordinateur

- Tout secteur d'activité
- Toute taille

Comment ?

Différentes composantes

- Organisation
- Moyens
- Transfert du coût du préjudice
- Responsabilités (Environnement, Responsabilité Civile…)
- Partage d'information
  - Entre métiers
  - Acteurs 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

Eléments d'organisation (suggestions)

Répartition des taches

- La responsabilité fonctionnelle (administration) reste aux métiers (« prod », « process »)
- La responsabilité technique est, *a minima*, partagée avec le département SSI
  - A l'instar de la téléphonie (quoique souvent basculée vers la DSI) ou le contrôle d'accès (*badging*)

Priorité aux architectures en migration, éléments de surveillance

- Mise en réseau TCP/IP
- Evolution des équipements (OS et interfaces)
- Télémaintenance (modem, Internet)

Assurances et risks management

Possibilité de litige

- Volonté d'assurance (acte de malveillance immatériel)
- Montant garantis (PE après fraude sous dimensionnée)

Fusion des assurances Dommages (*Property*) et Fraude (*Crime*)

- Financement des frais de remise en état
- Remboursement des préjudices (PE (Pertes d'Exploitation), FSE (Frais Supplémentaires d'exploitation))

Quelques principes de l'assurance

- Aléa
- Pas d'enrichissement => valorisation d'impact. Confer

Paramètres d'assurance

- Fait générateur, éléments assurés,, capitaux garantis, franchises, exclusions… pour une modique prime à payer

Partage d'information… faible

Information offreurs orientée sûreté de fonctionnement (fiabilité, maintenabilité, disponibilité)

Une DNS (Directive Nationale de Sécurité ;-)) à diffusion limitée en 2006

- Focalisation IFN, SAIV, OIV-PIV…

Littérature et colloques essentiellement anglo-saxons

Création d'un Groupe de Travail CLUSIF ? ☺

Conclusion : quand ?

Dès que possible…

- Ex. projet de mise en sécurité planifiée sur 5 ans par un groupe français de dimension internationale

A priori, pas de scénario « big bang » mais déploiement des nouveaux équipements en intégrant une sécurité logique (et sa dynamique de SSI)