Services Généraux sur IP : nouveaux risques

01 Security Management – Paris

13 avril 2010

Pascal LOINTIER
Président du CLUSIF
Conseiller sécurité de l'information, CHARTIS

CLUSIF

Agenda de présentation

- ✓ **Périmètre d'étude**
- ✓ **Quelques faits, événements récents**
- ✓ **Migration technologique/commerciale, exposition croissante**
- ✓ **Eléments de solution**

Services Généraux (SG), périmètre d'étude

Il s'agit de l'ensemble des services nécessaires au fonctionnement normal d'une entreprise: achats de matériels, de fournitures, achat de terrains, construction de bâtiments, gestion des locaux techniques et des fluides: électricité, froid, chauffage, entretien des bâtiments. L'expression "Services Généraux" est généralement réservée à une activité interne de l'entreprise. Lorsque cette activité est externalisée, l'expression "Multi-service" est souvent employée. En anglais on appelle ce service "**Facility Management**" ou "**Facilities Management**". Il existe des entreprises spécialisées dans ce domaine.
(source Wikipedia)

2001 : virus CodeRed sur MFP

Un virus avec un moteur de scan IP très puissant pour détecter les cibles de contamination

- Saturation de la bande passante du réseau interne (et impossibilité de télécharger la mise à jour de l'antivirus ☺)
- Contamination des imprimantes sur le réseau (source Panorama 2001)

CLUSIF

MFP? Multi Function Printer

Printer ou *device (MFD)*, donc un équipement qui imprime, qui numérise, qui envoie un courrier, qui stocke tout cela sur un disque dur dans la machine…

- Système d'exploitation standardisé,, accès telnet, http… sans antivirus ni pare-feu
- Accessoirement, disque dur non chiffré (encodage propriétaire >< chiffrement), option d'écrasement non activée
- Les imprimantes restent souvent du ressort des SG à cause des commandes de papier. Le rattachement à la DSI ou l'implication du RSSI (Responsable Sécurité) semble pourtant légitime

2002 : DISA et caméras WiFi, les prémices

Mai 2002, un service de sécurité américain (DISA) admet avoir utilisé une infrastructure WIFi non sécurisée (802.11b) pour la transmission de vidéos de sécurité

- Exploitation par un tiers des images, DoS (déni de service) combiné à une intrusion, connaissance des angles de vidéosurveillance, etc. (source Panorama 2002)

2007 : CNN et groupe électrogène

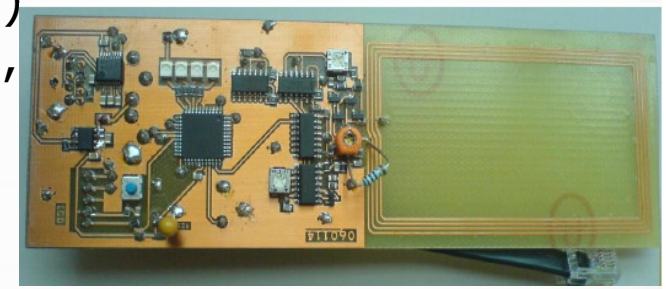
Septembre 2007 – Idaho (E-U): la chaîne CNN demande à des experts du DHS (*Department of Homeland Security*) de provoquer à distance la destruction d'u groupe électrogène. Cette action est rendu possible par l'injection de commandes numériques sur un équipement sans correctifs de sécurité (source Panorama 2007)

2008 : badges sur IP

Annonce faite par le CCC (Chaos Computer Club, Allemagne) le 1/1/2008 : Cassage de l'algorithme de chiffrement

Mifare : produit de la société NXP, destiné notamment à de l'authentification sans contact (technologie RFID)

- Système de transport public (Londres, Perth, Amsterdam…)



Cas du système hollandais : 2 types de tickets

- « Ultralight card », usage unique : simple mémoire + système sans contact, aucune protection
- « Classic card », pour abonnements : idem, mais protection cryptographique des échanges par un algorithme « secret » (CRYPTO1)

Mifare est utilisé pour des contrôles d'accès par badge en entreprise (source Panorama 2008)

CLUSIF

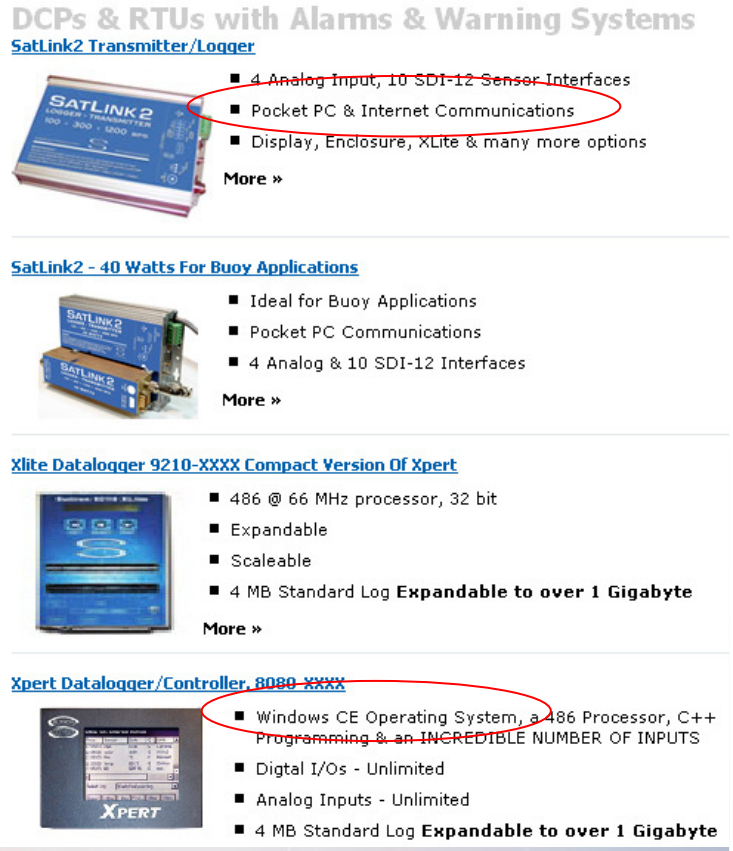
SCADA : malveillances internes (via le S.I.)

- 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)

2009 : la migration IP continue…

Après la téléphonie , le reste des infrastructures générales migre sur les réseaux IP :

- Systèmes SCADA (pilotage, processus industriel…)
- Migration complète (y compris le transport ou les équipements terminaux) ou partielle (supervision, commande, reporting…)
- Surveillance et accès (portes, badgeuses, caméras, détecteurs présence, détecteurs incendie, humidité…)
- Climatisation, chauffage, éléments de confort (volets)
- Energie (onduleurs, électrogènes…) (source Panorama 2009)



CLUSIF

2009 : serrures sur IP

Lyon, 29/08/2009 - La prison neuve de Corbas (Rhône) connait depuis une semaine des pannes du système d'ouverture automatisé des portes [...] Les serrures électriques commandées à distance par écran tactile ont cessé de fonctionner le week-end dernier, entre samedi 15h30 et dimanche soir, empêchant la circulation de prisonniers, gardiens et visiteurs à l'intérieur de la prison.

Roanne, 02/09/2009 - La prison de Roanne, inaugurée en janvier dans la Loire, a été paralysée par une panne informatique empêchant l'ouverture de toutes les serrures électroniques. Le système vidéo, les alarmes et les ouvertures de portes commandées à distance sont tombés en panne vers 15H00 et n'ont été réparés que vers minuit, après l'intervention de techniciens venus de Paris

2009 : SWATTING for Money

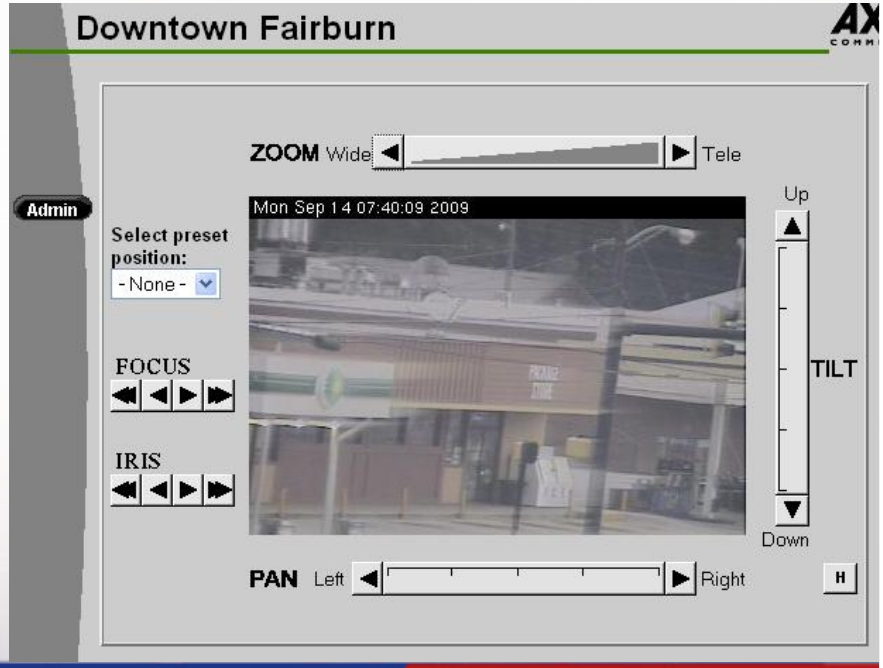
Hammond (Indiana, E-U), juillet 2009 : début du procès de jeunes hackers qui vendaient en ligne l'accès vidéo à une action SWAT en cours (partyvanpranks.com). Pour cela, ils ont commencé par prendre le contrôle à distance des caméras de surveillance

Google Search: camera linksys inurl:main.cgi

Another webcam, Linksys style.

****

* inurl:"ViewerFrame?Mode=
* intitle:Axis 2400 video server
* intitle:"Live View / - AXIS" | inurl:view/view.shtml^
* inurl:ViewerFrame?Mode=
* inurl:ViewerFrame?Mode=Refresh
* inurl:axis-cgi/jpg
* …



CLUSIF

2009 : caméra pas sur IP ;-)

Septembre – Vincennes : vers 6h ce jeudi matin, un Egyptien et un Marocain retenus au centre de rétention de Vincennes (Paris 12e) se sont évadés en escaladant une clôture, selon Le Parisien.

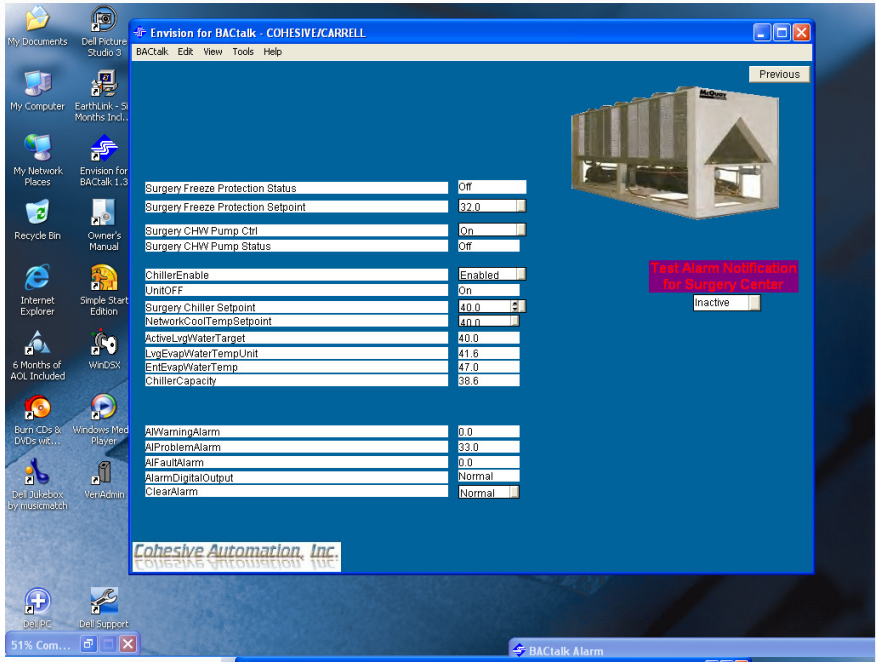
Pour s'échapper, les deux hommes ont arraché le grillage d'une fenêtre et modifié le champ d'observation d'une caméra, en secouant le poteau où elle était accrochée.

2009 : hacking de la ventilation dans un hôpital

FACTS IN SUPPORT OF AFFIDAVIT

6. On 6/24/2009, The Dallas Division of the FBI was contacted by Special Agent Charles Provine of the FBI in the Jackson Division of the FBI regarding a computer intrusion of a Heating Ventilation and Air Condition (HVAC) computer system at a Dallas, TX hospital, the Carrell Clinic located at 9301 North Central Expressway, Dallas, Texas. This was believed to present a risk to health and safety as the Hospital was a facility that kept patients around the clock who could be adversely affected by the cooling if it were turned off during Texas summer weather conditions and the hospital also maintained drugs which could be adversely affected by the lack of proper cooling if the intruder were to disturb the HVAC system. SA Provine stated that he was in contact with Lieutenant (LT) Lannie Hilbolt, Texas Attorney General's office and CW-1, a network

Page 4 of 18



Absence de ventilation = évacuation

2010, La flotte (auto) est sous contrôle !

Austin, Texas (E-U) : plus de 100 véhicules ont été immobilisés ou leurs klaxons incontrôlables après qu'un individu se soit introduit dans le système web gérant l'immobilisation de véhicules (Webtech Plus) en cas de défaut de paiement

Eléments de solution

Tout le monde est concerné : existence de services généraux, production/logistique industrielle assistée par ordinateur

Corollaire, 5 S.I. dans une entreprise (en fonction de l'activité)

- ✓ Management (gestion, comptabilité, etc.)
- ✓ Externalisé/infogéré
- ✓ Production/régulation/logistique (cf. SCADA)
- ✓ VoIP
- ✓ Services Généraux (sans oublier le cyber-mapping)

Les responsables de la sécurité physique n'ont pas tous une sensibilité/savoir faire quant à la sécurité logique

- ☞ Document du NYPD (2009) sur le contre-terrorisme dans les bâtiments publics sans aucune mention de cette évolution d'environnement :la seule référence à un élément informatique recommande l'installation d'une caméra sur un capteur d'ouverture pour la levée de doute

CLUSIF

Eléments de solution

La redondance n'est plus…

- Hypothèse (obsolete ?) de sûreté de fonctionnement
  - ☞MTBF (*Mean Time Between Failure*)
  - ☞Faible probabilité de défaillance quasi-simultané de deux équipements identiques
- Aujourd'hui, une couche logicielle, un « point de passage » électronique-informatique, sur tout type d'équipement

Partage nécessaire d'informations et de taches entre

- RSSI ou équivalent
  - ☞Responsabilité fonctionnelle, évaluation du niveau de sécurité, politique de mise à niveau
- SG, responsable opérationnel (exploitation)

Points de vigilance

- ✓Systèmes d'exploitation et langages standards
- ✓Correctifs
- ✓Infrastructure (Ethernet, WiFi)
- ✓Point de supervision (poste de travail)
- ✓Accès distants (modem, Internet)
- ✓Dialogues M2M
- ✓…

Services Généraux sous IP – Nouvelles expositions

Club de la Sécurité des Systèmes d'Information du Languedoc-Roussillon
954, avenue Jean Mermoz
34000 MONTPELLIER
Contact : Christian FERRAND
Site web : www.clusirlr.info

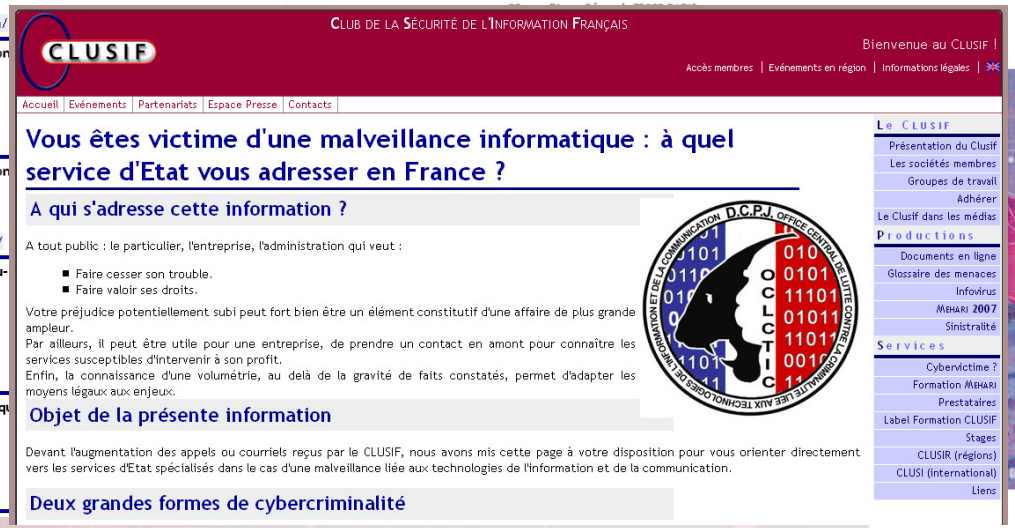
Club de la Sécurité des Systèmes d'Information de la Région Midi Pyrénées
S/C INSA
Département de Génie Electrique et Informatique
135, Avenue de Rangueil
31077 TOULOUSE CEDEX 04
Contact : Laurent PELUD
Site web : www.clusir-mp.asso.fr

Club de la Sécurité des Systèmes d'Information de la Région Est
16, rue de Pont-à-Mousson
57000 METZ
Contact : Thierry RAMARD
Site web : www.clusir-est.fr

Club de la Sécurité des Systèmes d'Information de la Région Provence-Alpes-Côte-d'Azur
500, rue de Paradis
13008 MARSEILLE
Contact : Claude LELOUSTRE
Site web : http://www.clusif.fr/clusir-paca/

Club de la Sécurité des Systèmes d'Information
SITIV
Passage de l'Avenir
69200 VENISSIEUX
Contact : Yannick BOUCHET
Site web : www.clusir-rha.fr

Club de la Sécurité des Systèmes d'Information
1862, avenue Général De Gaulle
59910 BONDUES
Contact : Gérard MOLINES
Site web : http://www.clusif.fr/clusir-npp/

Club de la Sécurité de l'Information de Poitou-
Technopole Venise Verte
Rue Euclide
BP 8421
79024 NIORT cedex 9
Contact : Sébastien Gioria
Site web : http://www.clusir-poi.fr/

Club de la Sécurité de l'Information Région Aqu
s/c Philippe Marty (Vice-Président)
51 rue Manon Cormier
33000 Bordeaux
Contact : Marc Ferrigno