



France

*Setting the Standard for Automation™*

## Sensibiliser de manière efficace les collaborateurs

au bénéfice de l'entreprise et du leur

En partenariat avec



Patrice Bock, ISA-France

**Cyber-attaques : comment faire face ? - Paris – 26 et 27 juin 2013**

### Le sujet et l'intervenant



- Sensibilisation à la cyber sécurité dans l'industrie
- Objectifs d'une sensibilisation
- REX de plusieurs années et de dizaines de sessions

Patrice Bock, [patrice.bock@isa-france.org](mailto:patrice.bock@isa-france.org)

ISA France, CLUSIR, Euriware

Blog : <http://securid.novaclis.com> (cybersécurité industrielle principalement)

Sensibilisation des collaborateurs

## 1999 : Bellingham, USA



- Source : National Transportation Safety Board (USA)



Sensibilisation des collaborateurs

## Pourquoi sensibiliser ?



- Parce que toutes les normes l'exigent...
- Situations dans lesquelles la sensibilisation est utile
- Bénéfices

## Des architectures peu sécurisées, exemple 1 Le ver Slammer chez un constructeur automobile

Date : Jan 2003  
Localisation : Multiple  
Industrie : Automobile  
Type d'incident : Logiciel malveillant  
Impact: Perte de Production



Source: *The Repository of Industrial Security Incidents* ([www.securityincidents.org](http://www.securityincidents.org))

## La sensibilisation, c'est facile



- Dans l'industrie, on ne protège pas que « l'information »
- Culture sûreté et sécurité existante
- Merci google

## Des architectures peu sécurisées, exemple 2: 11 automates sur Ethernet tombent en panne

Date : May 2003  
Localisation : Georgia, USA  
Industrie : Métallurgie  
Type d'incident : Panne API/SCADA  
Impact : Perte de production



*Source: The Repository of Industrial Security Incidents (www.securityincidents.org)*

## Modalités d'une sensibilisation



- 1 à 3h
- Interactivité à encourager
- Intervenant interne à l'entreprise (devient le référent)

## Démonstration d'une cyber-attaque



- 2007 : Idaho National Labs



Sensibilisation des collaborateurs

## Contenu type d'une sensibilisation



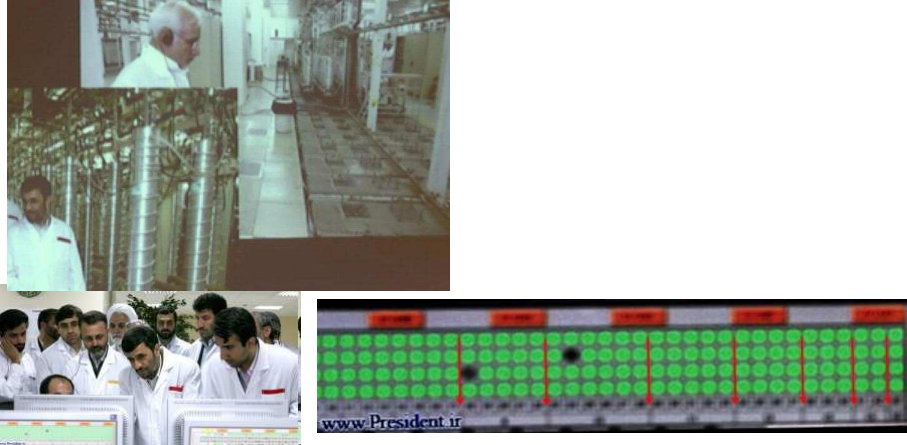
- Mettre un doigt dans la technique
- Culture générale de la sécurité
- Narratif des événements des dernières années
- Conséquences pour nous

Sensibilisation des collaborateurs

## Stuxnet : la préparation



- Source : blog de Ralph Langer

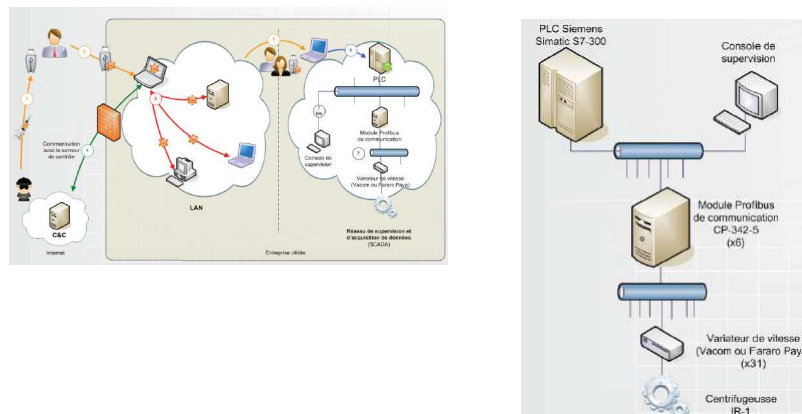


Sensibilisation des collaborateurs

## Stuxnet : l'exécution



- Source : XMCO (<http://www.xmco.fr/actu-secu/XMCO-ActuSecu-27-STUXNET.pdf>)

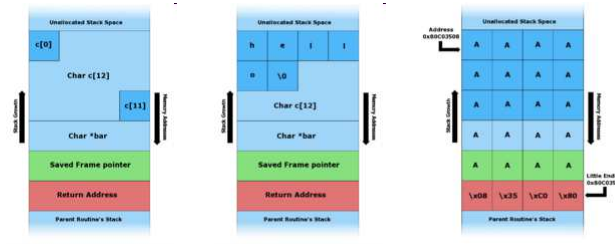


Sensibilisation des collaborateurs

## Buffer overflow



- Source: wikipedia



Sensibilisation des collaborateurs

## Les chausse-trapes



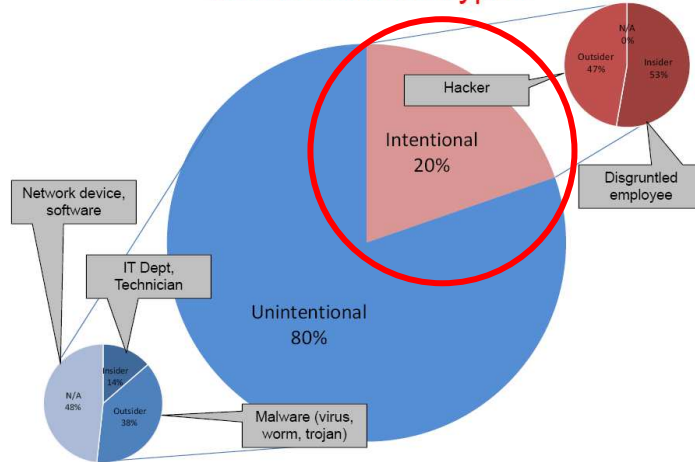
- Erreur de casting de l'intervenant
- Exemples non appropriés / hors contexte
- Absence de solutions pratiques
- Masse non critique de personnes sensibilisées

Sensibilisation des collaborateurs

## Peu de cyber-incidents malveillants



### Actual Incident Types



© 2011 Security Incidents Organization

Sensibilisation des collaborateurs


## Risi

The Repository of Industrial Security Incidents  
[www.securityincidents.org](http://www.securityincidents.org)

### Un hacker met à l'arrêt d'une usine pharmaceutique

Date : Février 2011  
Localisation : Smyrna, Georgia, USA  
Industrie : Pharmaceutique  
Type d'incident : Accès non autorisé  
Impact : Perte de production



 SHIONOGI & CO., LTD.



## Après la sensibilisation...



- ( lancement de projet de sécurisation )
- Entretien de la dynamique
- Utilisation commerciale
- Bilan et suivi dans le temps

Sensibilisation des collaborateurs

## Questions ?



- Les supports seront disponibles - avec les exemples et les liens internet

Sensibilisation des collaborateurs

## Les systèmes industriels visibles sur internet

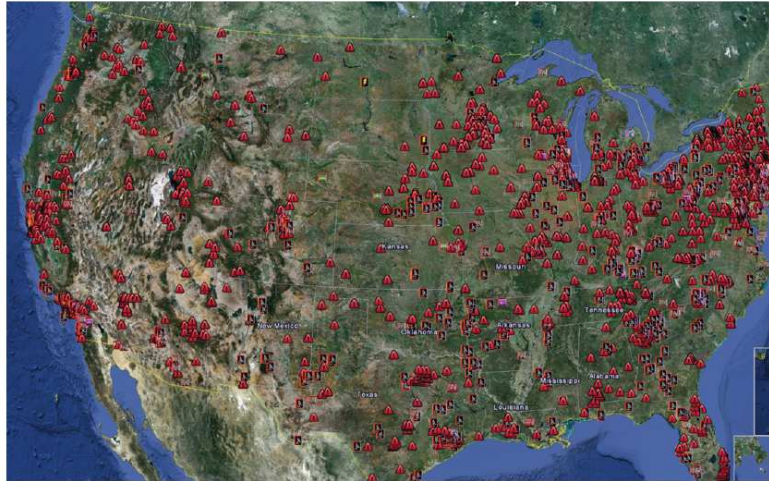


Figure 3. Approximately 7,200 Internet facing control system devices in the US.

Source : ICS-CERT\_Monthly\_Monitor\_Oct-Dec2012

Sensibilisation des collaborateurs