CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

CLUSIF

CNAMTS

Sensibilisation de la MOE Informatique

Sécurité sociale
L'Assurance Maladie
Caisse Nationale

Le comité RSSI

Comité RSSI

- Un RSSI est lié à un domaine géographique d'activité MOE National
- Il y a donc un RSSI dans chaque CTI et un RSSI par Pôle de Fabrication
- Couvre tous les métiers informatiques de son domaine
- Peut être, en plus, MSSI si pas de MSSI couvrant son territoire

Sensibilisation : pour quoi faire ?

Sensibiliser et Former

FORMATION
Action de donner à quelqu'un, à un groupe, les connaissances nécessaires à l'exercice d'une activité

SENSIBILISER
Rendre quelqu'un, un groupe sensible, réceptif à quelque chose pour lequel il ne manifestait pas d'intérêt

La sensibilisation est donc un acte différent de la seule transmission des bonnes pratiques.
Quitte à abuser des simplifications, nous pouvons dire que nos sensibilisations ont comme objectif de rendre les agents réceptifs à « l'existence du mal » et adhérer à l'idée de le « combattre… »

En définitive : l'inclure dans notre « système de protection »

SWOT « tentative » des informaticiens (informatique interne)

S :	W :
- Facilités compréhension sujets techniques - Connaissance d'une partie du vocabulaire - Professionnalisme - Habitudes de communication (team) - Goût de vérité (science)	- Vision « techniciste » - Vocabulaire non unifié - Avoir leur propre idée - Communication informel - Croit avoir la vérité
T :	**O :**
- Accord avec les règles… pour les autres - Sentiment de « supériorité » - Sentiments de frustration si privilèges limités - Contradiction « sécurité » versus « opérationnel »	- Intelligence - Goût du « travail bien fait » - Sécurité est à la mode : Valorisant - Compréhension des « exceptions »

Focus Sensibilisation

Schéma d'une sensibilisation: Objets

- Le mal (malveillance, mais aussi négligence, méconnaissance mais aussi erreurs)
- Le champ de la sensibilisation (domaine du « mal » à traiter, les composants seront délimités par le champ)

  Exemples de champs : protection du poste, intrusion réseaux, malveillance téléphonique, fuite d'information, protection des information en CTI, etc. Plusieurs sujets peuvent être groupés
- Les vulnérabilités (failles ou faiblesses permettant au « mal » d'agir)
- Les bonnes pratiques (référentiels, POGS, normes et standards)
- Le « non prévisible » (mal ne pouvant pas être prévu à l'avance)
- Le RSSI du domaine (et de la DS)
- Les participants (tous agents présents, RSSI compris)
- La bonne réaction : **c'est l'objectif de la sensibilisation (comme en allergologie)**

Et alors…

Focus Sensibilisation

Schéma d'une sensibilisation : Déroulement

Le « mal » dans le champs choisi EXISTE :

- Exemples externes (presse, clubs, etc.)
- Exemples internes (« anonymisés ») OPS, AM ou locaux

Les vulnérabilités fréquemment exploitées

Les bonnes pratiques applicables

- Référentiels et POGS AM (si existent)
- Référentiels et POGS DS
- Autres (externes ou simples)

Le « non prévisible »

- La méfiance nécessaire
- L'aide du RSSI

Echange entre participants

Conclusion : **le « mal » existe, appliquons les bonnes pratiques et soyons vigilants. Et concrètement…**

Les sujets et déroulement
des sensibilisations ces 2 dernières années

Sensibilisation 2014 et 2015 : Sujets

Champs :
2014 : Les attaques informatique et l'exploitation de failles informatiques
2015 : Les incidents sécurité et leur gestion (préparé avec le SOC)

L'idée est que chaque RSSI fasse cette sensibilisation dans son CTI ou Pôle, avec ma présence si (vraiment) nécessaire voir le remplacement par un collègue d'un autre organisme ou moi-même si nécessaire

Peut être participation d'autres collègues de la Direction Sécurité

Pour aller plus loin : ces sensibilisations ne vont pas assez loin pour les développeurs : « Sensiboformation » en couplant sensibilisation et formation sur les bonnes pratiques

Quelques exemples « vécus »

Sensibilisation MOE Nationale

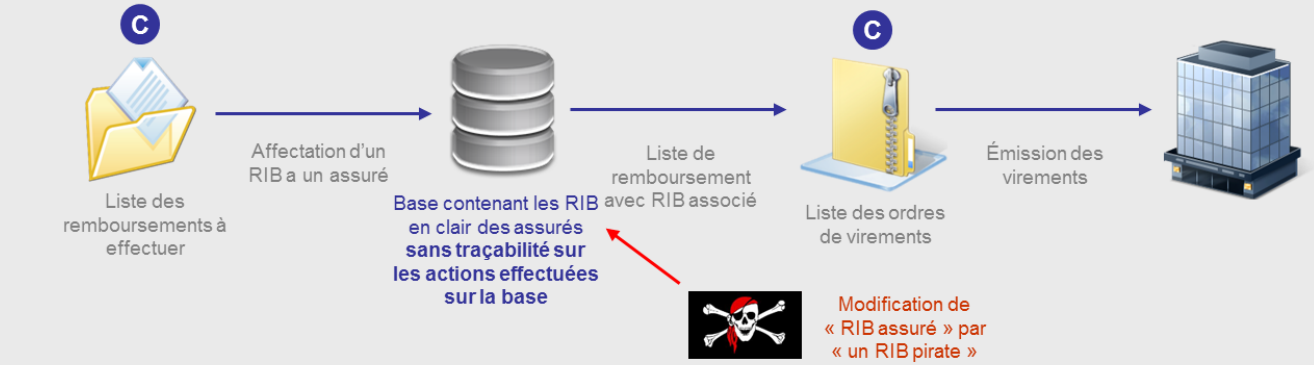
Quelques exemples de transparents pour générer le dialogue avec la salle

2012 : Fuite d'information
adhérer à la traçabilité (l'allié des innocents)

1 Contexte

Un contrôle est réalisé au sein d'une mutuelle sur une de ces applications de gestion de trésorerie
➔ Il a permis de détecter des incohérences dans la base de gestion et notamment des remboursements effectués vers un compte « non assuré »

2 Technique



C ➔ Les contrôles métiers (traçabilité sur les actions) étaient systématiquement effectués

Le discrédit a été porté par la totalité des administrateurs systèmes puisque la traçabilité sur les actions sur la base de RIB n'a pas permis de les innocenter
➔ Perte de confiance de la part des collaborateurs envers les administrateurs systèmes

Sensibilisation 2009 :
Les règles de sécurité