



Evaluation Financière d'un incident de sécurité

15 octobre 2009

Introduction

Pascal Lointier
Chartis



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...



Une dynamique d'échanges et de production

Une collaboration à l'international

- ⊕ 5 associations consœurs

Une collaboration en région

- ⊕ 8 CLUSIR

Une production, résultat des conférences et de l'activité des Groupes de Travail et de l'Espace RSSI

- ⊕ Des **livrables en libre accès** Des traductions en anglais (entre autres)
- ⊕ Des prises de position publiques ou des réponses à consultation

La dynamique des groupes de travail

Nouveaux documents en ligne

- Sécurité des Applications Web
- Synthèse « Chiffrement des données locales des moyens nomades »
- Bots et Botnets
- Synthèse « Fraude interne, malveillance interne : détection et gestion »
- Métriques (série 27000)

Documents en relecture

- Malveillance Téléphonique
- PCI-DSS
- Infogérance

Nouveaux Groupes de Travail

- MIPS 2010
- DoS (*Denial of Service*)
- Sécurité des Applications Web – WAF
- ...MFP (en cours de soumission)

Intérêt initial d'une évaluation

Contribution possible au RoSI

Justification/incitation aux budgets d'investissements

Transfert du risque

- ⊕ Financement du plan de crise
- ⊕ Remboursement des frais de remise en état
- ⊕ Remboursement du chiffres d'affaires non réalisé (et autres dommages indirects)

Préjudices, vu dans la Presse

3/09/2009 (date presse) : **Arrêt du réseau données et voix du London Ealing Council**

- ⊕ Mis en examen : Conficker-D
- ⊕ Mode opératoire : clef USB (on ne change pas une méthode qui marche ☺, cf. suite de la conférence...)
- ⊕ Traitements arrêtés/perturbés pendant une semaine
- ⊕ Préjudices indirects > 500 000 GBP (> 1M considérant l'amélioration de la sécurité)
 - 👉 1 883 amendes non collectées (90 000 GBP)
 - 👉 Pénalités de retard sur livres empruntés (25 000 GBP)
 - 👉 Traitement supplémentaire des fonds de soutien (14 000) GBP
 - 👉 Collecte des loyers...

Sources : Guardian, The Register

La sécurité n'est pas une fin en soi...

Finalité : maintenir ou faciliter la remise en état de l'outil de production (contexte entreprise)

- ⊕ Pour être plus exhaustif, prévenir les dommages corporels et environnementaux
- ⊕ Pour être cynique, les non-respects dans ces deux derniers cas se traduisent par des sanctions, des amendes...

4 postures de gestion du risque

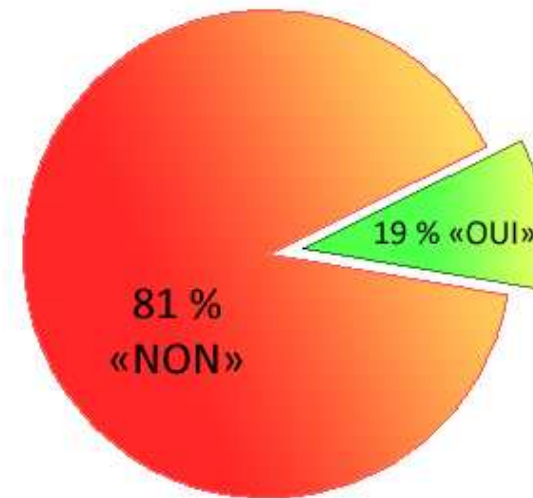
- ⊕ Acceptation tel que
- ⊕ Réduction
- ⊕ Transfert
- ⊕ Evitement (arrêt du processus exposant)

Constat MIPS



« Procédez-vous à une évaluation de l'impact financier des incidents de sécurité ? »

- ⊕ Non → 72%
- ⊕ Parfois → 9%
- ⊕ Souvent → 6%
- ⊕ Systématiquement → 13%



Avec plusieurs dizaines de RSSI membres du CLUSIF, on partait confiant pour obtenir un témoignage... 😊

Agenda de session

Introduction

*M. Pascal LOINTIER - Conseiller Sécurité de l'Information - **Chartis**
Président - **CLUSIF***

SRE-SMP, éléments de valorisation

*M. Luc VIGNANCOUR – Directeur – **Marsh MC***

Expertise de sinistres – analyse de cas

*M. Jean-François MOULIN – **MOULIN International Loss Adjusters Consulting***

Contribution d'une méthode d'analyse ou d'une norme

*M. Pierre DEWEZ – **Devoteam Belgique***



Agenda de session

Table ronde

Animateur : M. Fred MESSIKA, Président de SEKOIA et Responsable de l'organisation des conférences du CLUSIF

Mme Hélène COURTECUISSÉ - **Lisis Conseil**

Mme Elisabeth RIZET – **France Telecom**

M. René SAINT-GERMAIN – **Veridion**

M. Luc VIGNANCOUR – **Marsh MC**

M. Jean-François MOULIN – **MOULIN International Loss Adjusters Consulting**

M. Pierre DEWEZ – **Devoteam Belgique**

Cocktail !

Pour prendre date, 12 novembre : **Vulnérabilités des systèmes téléphoniques (TDM et VoIP)**