

# Cybercriminalité, mythes et réalités

Conclusion

Olivier DEBROSSE - SECALYS

- Mythes et réalités s'engendrent l'un l'autre
- Les mythes décrédibilisent la réalité
  - Déstabilisation du système
  - Accroissement du risque
- Tordre le cou aux mythes et aux rumeurs

# Comment tuer les mythes ?

- Bon sens
  - Le plus simple est souvent le plus efficace
  - Le plus plausible est souvent vrai
- Rester pragmatique (cf intervention de V.Hinderer)
- Travailler sur l'humain (cf intervention de B.sueur)

# L'humain

- Elever le niveau de conscience face au risque
  - Vigilance
  - Lucidité
- Contre exemples
  - Un DG connu qui passe par son i-phone pour s'affranchir des contraintes du VPN
  - Etude SECALYS en cybercafé

# 3 AXES D'EFFORT

# 1 - Former les spécialistes dans les entreprises

- L'expertise s'entretient
- Des informaticiens ne devraient pas être surpris en apprenant qu'il existe des clés usb aspirantes
  - L'habitude tue la conscience
  - Attention à la culture du sachant
  - Ménager du temps de formation malgré les contraintes de production, c'est investir sur la sécurité de l'entreprise
  - Repenser la gestion des RH

## 2 - Amener les experts à plus de réserve ...

... ou mieux définir la notion d'expert

- Une opinion, aussi éclairée soit elle, n'est pas un avis d'expert
- La parole d'un expert a du poids et doit être employée avec mesure et réflexion
  - Faire preuve de circonspection
  - Être vigilant à ne pas sortir de son champ d'expertise
  - Accepter l'idée qu'il n'y a rien de déshonorant à dire « je ne sais pas »
- L'expert a une lourde responsabilité dont il doit rester conscient

# 3 - Poursuivre l'implantation d'une culture de sécurité dans les organisations

- Qu'on n'entende plus ces phrases à forte capacité létale :
  - Ça ne peut pas nous arriver
  - Nous sommes très bien protégés
  - Chez nous c'est différent
  - Etc...
- Que l'estimation du risque ne soit plus émotionnelle ou appuyée sur les seules opinions
- Que la sécurité soit confiée à des spécialistes ou à tout le moins que les acteurs de la sécurité soient formés à ses pratiques et à ses modes de pensée
- Que les acteurs sachent prendre du recul vis-à-vis des informations qui leur parviennent
  - La gestion de l'information est un puissant outil de sécurité
- Que les acteurs sachent changer de point de vue et s'inscrire dans une démarche globale

# Application à la cellule de crise cf intervention de H. Berry

- Attention à la sur expertise
  - Les oppositions d’avis augmentent la difficulté des choix et les temps de réaction de la cellule
- Attention à l’effet « focus »
  - La concentration sur le disfonctionnement et l’urgence à rétablir le service peut occulter des éléments de fonds

# Clés de la réduction du risque en général et de la gestion de crise en particulier

- Savoir multiplier les points de vue
- Accepter le relativisme des perceptions
- Elargir le champ de conscience face aux considérations de sécurité
- Adopter une démarche systémique