Administration de la sécurité 3.0

Nicolas RUFF
EADS Innovation Works
nicolas.ruff(à)eads.net

Sécurité 1.0 : rien

- BYOD (*Bring Your Own Disquette* :)
- Administration et contrôles manuels
- Peu de risques
  - Peu de connectivité
  - Peu d'attaquants externes
- Peu de compétences
- Peu d'outils
- Peu de ~~buzz~~ volonté politique

Sécurité 2.0 : formalisation

- Analyses de risques
- Politiques de sécurité
- Automatisation des processus
  - Correctifs, scans de vulnérabilités, …
- Tableaux de bord
- Audits avant mise en production
- Audits récurrents
- Structuration du marché et l'offre

Sécurité 2.0 : résultats

- Echec !
  - Les dérives constatées
    - *Compliance*
    - *Cover Your Ass Security*
  - Processus techniques : faux
    - Mesures biaisées
      - "100% des virus connus …."
    - Outils bogués ou mal configurés
    - Informatique invisible
  - La sécurité devient un *Lemon Market*
    - L'ANSSI espère réguler …
    - … mais va-t-elle faire apparaître des compétences ?

Sécurité 3.0 : idées

- La protection a atteint son maximum
  - La sensibilisation des utilisateurs a ses limites
  - Failles "0day" (ou pas)
  - Système non sécurisables
  - Les mots de passe resteront mauvais
  - Inventaire des usages réels
  - Droits d'accès aux systèmes vs. infogérance
- … il faut passer à la détection

Sécurité 3.0 : idées

- Les outils …
  - … ont une durée de vie limitée
    - Les attaquants ont les mêmes
  - … sont eux-mêmes un danger
    - Bugs, backdoors, …
  - … nécessitent d'être testés / configurés
  - … ne remplacent pas la décision humaine

Sécurité 3.0 : idées

- Oubliez …
  - … le "mode projet"
    - Une application est comme un enfant: vous en êtes responsable toute votre vie
  - … la politique
    - Les attaquants n'ont aucune problème de "périmètre"
    - *Red Team*
  - … les problèmes d'argent
    - Dans la plupart des entreprises, il faudrait multiplier par 10 le budget sécurité pour être sérieux

Sécurité 3.0 : idées

- Attention à l'intégration / l'infogérance
  - Les [gros|vieux] logiciels sont souvent mauvais
  - Les prestataires sont souvent mauvais

Sécurité 3.0 : idées

- Questions ouvertes
  - Le Cloud et/ou l'externalisation vont-elles sauver le monde ?
  - "L'informatique est-elle une chose trop sérieuse pour être confiée à des clients finaux ?"