Cybersécurité

Etat des lieux et constats
4 Juillet 2016

CLUBEBIOS

Quelques chiffres

CLUBEBIOS

- 83% of all attacks were not highly difficult
- 73% of data breaches came from external sources
- 285 million records analyzed were compromised in the past year. That's more than one per adult in the U.S..
- 58% of all incidents analysed for the 2012 report were tied to hacktivist groups

Quelques chiffres, le retour

CLUBEBIOS

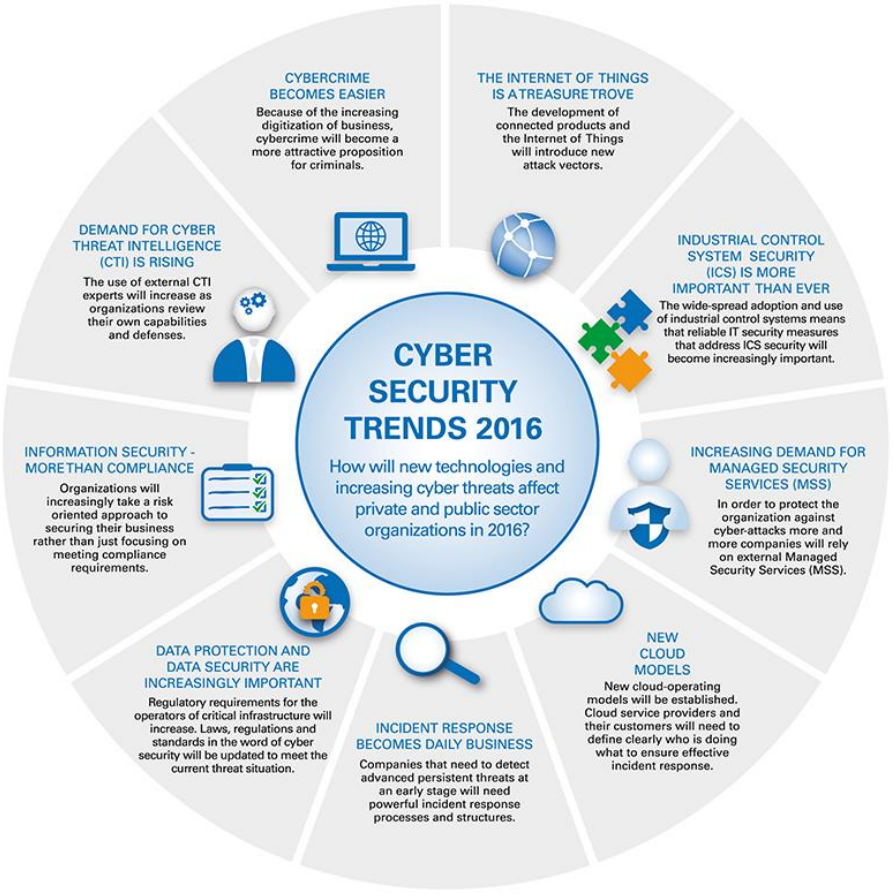
- Most cyberattacks are committed by Spies, Criminals, Activists
  - De STUXNET au malware bancaire !
- 84% of initial compromises took hours or less
- 80% of incidents had a financial motive
- 63% of 2,260 confirmed breaches leveraged weak, default or stolen passwords

92% of security incidents were described by just nine patterns

CLUBEBIOS

- Cyber-espionage
- Miscellaneous errors
- POS intrusions
- Payment card skimmers
- Web App attacks
- Denial of Service (497 Gb/s few days ago)
- Physical theft and loss
- Crimeware
- Insider and privilege misuse

Visibilité sur les axes d'amélioration retenus aujourd'hui



http://go.openskycorp.com/cyber-security-trends-2016

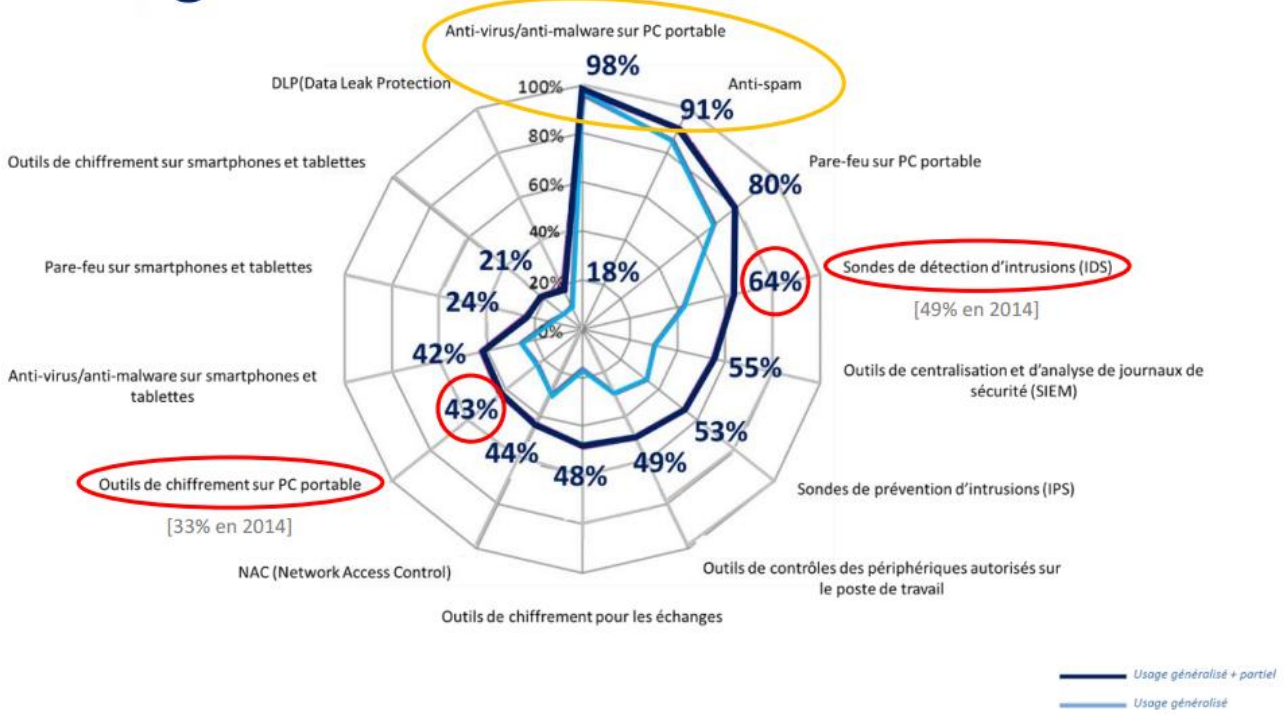
TÜVRheinland®
Precisely Right.

OPENSKY
A TÜV Rheinland Company

Retour sur Clusif

CLUSIF
MIPS 2016

Technologies de sécurité utilisées…



Le cadre

- Un monde chaotique et geopolitiquement instable
- Des évolutions poussées par les marchés et des rythmes de renouvellement courts
- SDLC d'un cycle en V rassurant à une démarche Agile, efficace et réactive
- Du BYOD au tout connecté - IoT (Smartphone, balance, cardio, voiture, maison, …) – Dire non au concept devient complexe ...

Les constats

- On remarque une approche de la **gestion des risques SSI** toujours très orientée sur les **technologies** et non sur les usages.

- De fait, il est dès lors difficile de négocier avec les métiers qu'ils sont censés fiabiliser du fait de **l'incompréhension des métiers** à comprendre les enjeux de ces sujets (Pas pour tous mais pour la plupart)

- Le client veut toujours plus, plus vite

- On transforme plus qu'on ne construit

- On fait évoluer plus qu'on ne résoud

Les pistes d'améliorations

- Un partage des enjeux – ENSEMBLE
  IT/Métiers/Régulateurs

- Une ouverture vers l'autre qui ne s'enferme pas sur une expertise spécifique (technique, juridique, métiers supports, métiers) MAIS sur une construction partagée des points de vue

- Des solutions pensées pour le monde de demain – Tokenization, réduction de la durée de vie des données, environnement de confiance commun, chiffrement, …

Développer des réflexes

- On parle des problèmes détectés avec les métiers
- On partage ses solutions car elles peuvent être interprétées différemment par d'autres dans des sphères différentes
- On construit des équipes pluridisciplinaires
- On verouille sa station et on ne laisse pas trainer ses affaires ☺