Agence Nationale de la Sécurité des Systèmes d'Information - ANSSI

Patrice Bigeard – Délégué Ile de France
patrice.bigeard@ssi.gouv.fr

POSITIONNEMENT DE L'ANSSI

Premier Ministre

SGDSN
Secrétariat Général de la Défense et de la Sécurité Nationale

Coordination interministérielle en matière de défense et de sécurité nationale

ANSSI
Agence Nationale de Sécurité des Systèmes d'Information

Autorité nationale en matière de sécurité et de défense des systèmes d'information

Créée le 7 juillet 2009 par le décret n°2009-934, l'ANSSI est un **service à compétence nationale.**

TENDANCES

- Le **nombre global d'attaques** informatiques **augmente**

- **La sophistication des codes malveillants augmente**

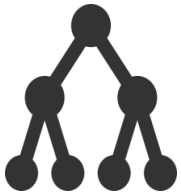
- Développement des attaques par la **chaine logistique**

- **Augmentation** des surfaces d'attaques

  Les mobiles/tablettes

  Usages pro/perso : moins de frontières

  Le cloud plus ou moins maitrisé



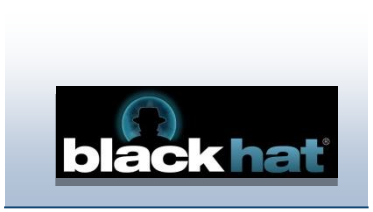
- L' **Internet des Objets** complique les choses (botnets)

Se préparer à des attaques plus nombreuses et d'impact croissant.

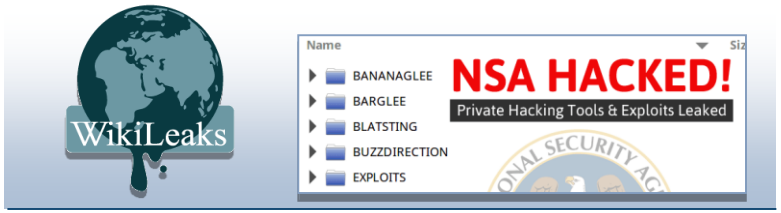
Et donc anticiper.

PROLIFÉRATION DE CODES D'ATTAQUE

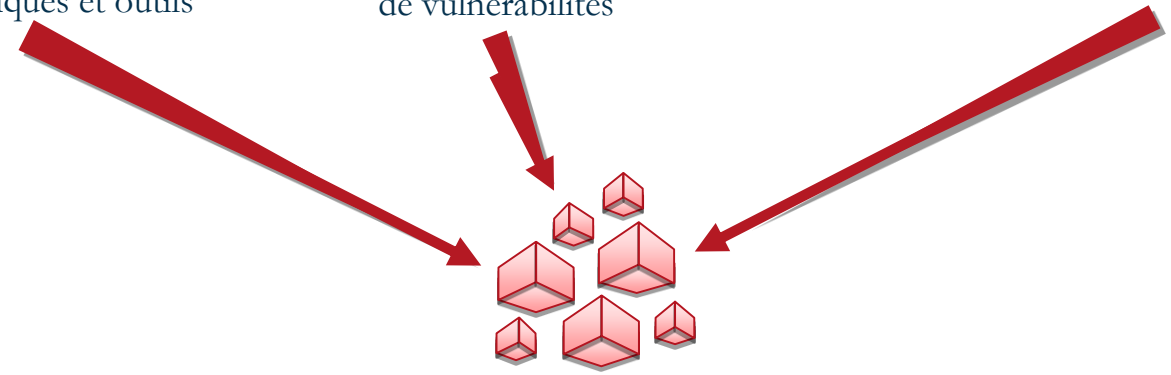
Publications de rapports sur techniques et outils



Découvertes et publications de vulnérabilités



Divulgations de codes très sophistiqués



Somme de codes et techniques réutilisables

Aujourd'hui, les attaquants vont plus vite à réaliser de nouveaux codes d'exploitation que les défenseurs à mettre à jour leur système d'information

LE CYBERCRIME TRÈS RENTABLE

POURQUOI LES ATTAQUES RÉUSSISSENT-ELLES TROP SOUVENT ?

- **Sensibilisation et maturité insuffisante des utilisateurs**
- **Systèmes et applications pas à jour dont sites Web**
- **Politique de gestion des mots de passe insuffisante**
- **Pas de séparation des usages (utilisateur/administrateur) et des réseaux**
- Laxisme dans la gestion des droits d'accès
- Absence de surveillance des SI
- Cloisonnement insuffisant des systèmes (propagation latérale)
- Absence de restrictions (périphériques…)
- Nomadisme / télétravail incontrôlés
- **Implication faible ou inexistante du Codir dans la stratégie SSI**

VULNERABILITES FREQUEMMENT RENCONTREES DANS L'INDUSTRIE

- **Architecture et cartographie du SI**
  - Pas d'inventaire précis du parc de SI industriel, méconnaissance des générations technologiques qui cohabitent
  - Pas d'analyse de risques

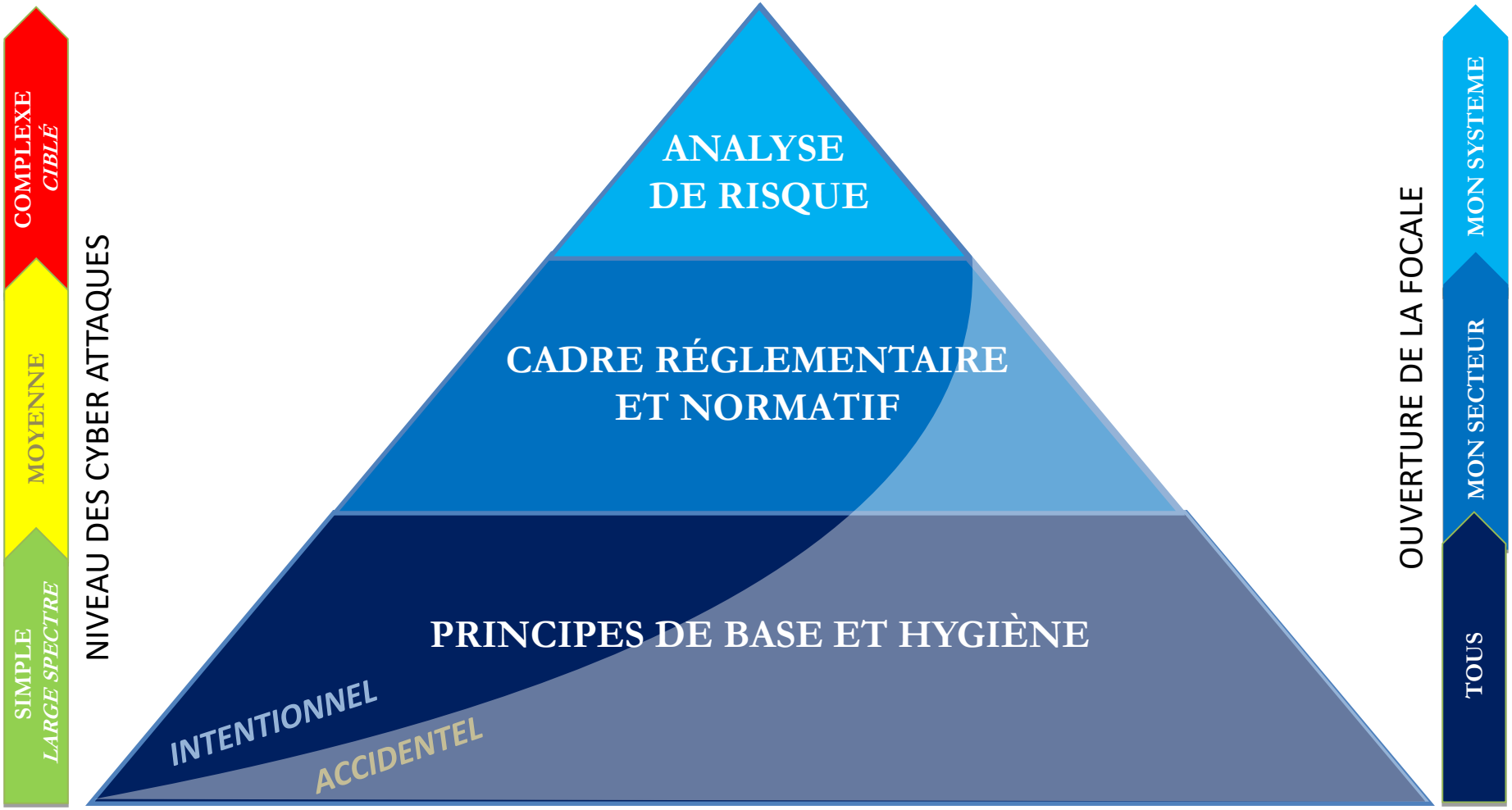
- **Mesures techniques préventives**
  - Faiblesse de gestion des accès (mdp par défaut, comptes génériques, comptes non fermés)
  - Outils de prise en main à distance non sécurisés

- **Maintenir la sécurité dans la durée**
  - Absence de mise à jour des systèmes d'exploitation, des applications
  - Absence de mécanisme de signature des firmwares (diffusion d'une maj piégée)
  - Absence de politique de gestion des médias amovibles

BONNES PRATIQUES DE SSI DES SYSTÈMES INDUSTRIELS

1. Contrôle d'accès physique
2. Cloisonnement des réseaux
3. Gestion des médias amovibles
4. Gestion des comptes (accès logique, authentification)
5. Durcissement des configurations
6. Gestion des journaux d'événements et alarmes
7. Gestion des configurations
8. Sauvegardes/restaurations
9. Documentation
10. Protection antivirale
11. Mise à jour des correctifs (planification)
12. Protection des automates
13. Stations d'ingénierie, postes de développement

VALEUR AJOUTÉE DE L'ANALYSE DE RISQUE



VISAS DE SÉCURITÉ ANSSI

TABLE DES MATIERES

POUR ALLER PLUS LOIN

Le MOOC de l'ANSSI : https://secnumacademie.gouv.fr

Les guides de l'ANSSI :

www.ssi.gouv.fr/entreprise/bonnes-pratiques/systemes-industriels/
www.ssi.gouv.fr/guide/organiser-un-exercice-de-gestion-de-crise-cyber/
www.ssi.gouv.fr/administration/guide/guide-d'hygiene-informatique

INFORMER - SENSIBILISER