



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

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

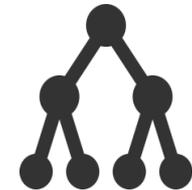
POSITIONNEMENT DE L'ANSSI



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 **chaîne logistique**
- **Augmentation** des surfaces d'attaques
Les mobiles/tablettes
Usages pro/perso : moins de frontières
Le cloud plus ou moins maîtrisé
- 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



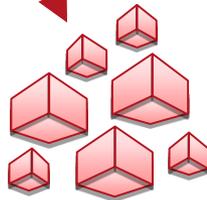
Publications de rapports
sur techniques et outils



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**
- **Systemes 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**

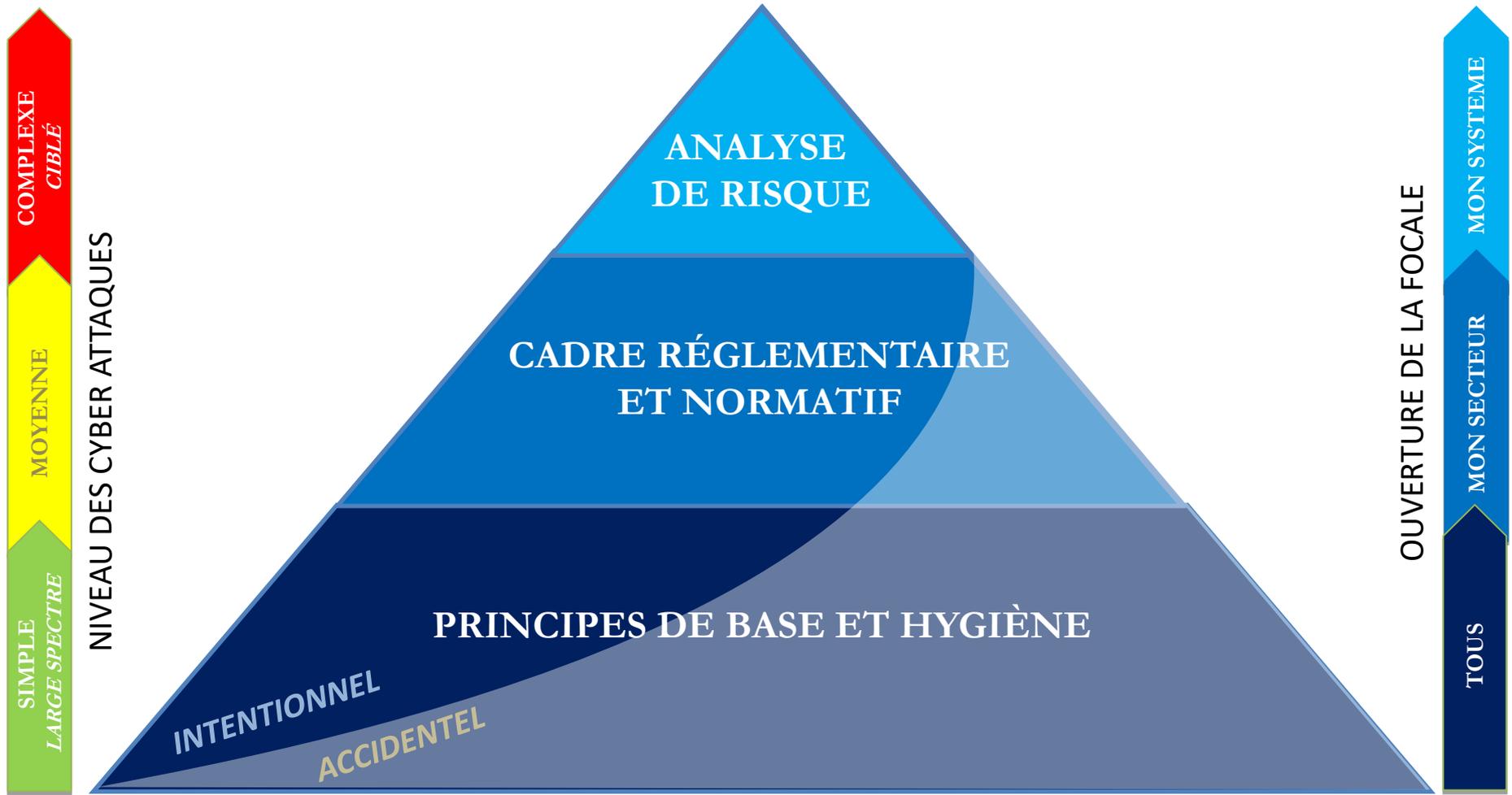
- Absence de mise à jour des systèmes d'exploitation, des applications
- Absence de mécanisme de signature des firmwares (diffusion d'une maj piégée)
- Absence de politique de gestion des médias amovibles

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



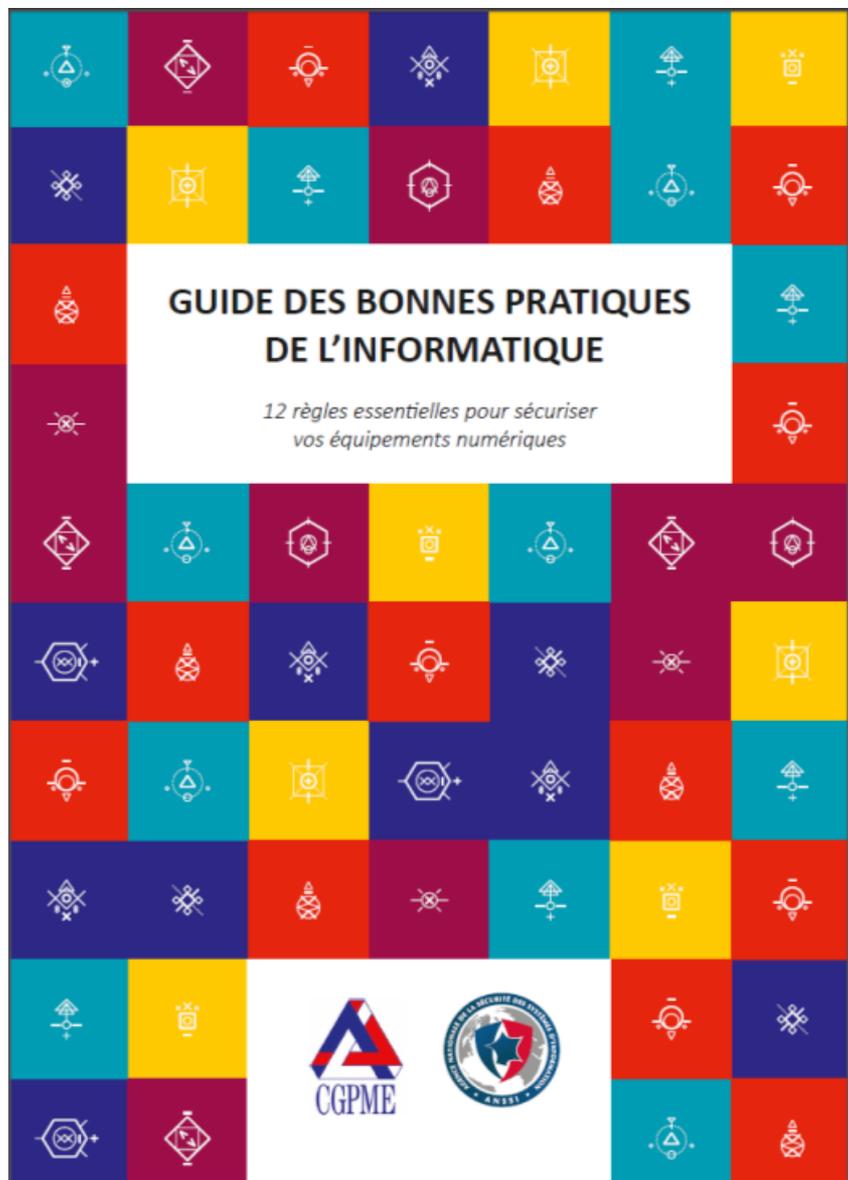


TABLE DES MATIERES

Pourquoi sécuriser son informatique ? (7)

- 1 / Choisir avec soin ses mots de passe (8)
- 2 / Mettre à jour régulièrement vos logiciels (10)
- 3 / Bien connaître ses utilisateurs et ses prestataires (12)
- 4 / Effectuer des sauvegardes régulières (14)
- 5 / Sécuriser l'accès Wi-Fi de votre entreprise (16)
- 6 / Être aussi prudent avec son ordiphone (smartphone) ou sa tablette qu'avec son ordinateur (20)
- 7 / Protéger ses données lors de ses déplacements (22)
- 8 / Être prudent lors de l'utilisation de sa messagerie (26)
- 9 / Télécharger ses programmes sur les sites officiels des éditeurs (28)
- 10 / Être vigilant lors d'un paiement sur Internet (30)
- 11 / Séparer les usages personnels des usages professionnels (32)
- 12 / Prendre soin de ses informations personnelles, professionnelles et de son identité numérique (34)

En résumé (36)

Pour aller plus loin (36)

En cas d'incident (37)

Glossaire (38)

POUR ALLER PLUS LOIN

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

The screenshot displays the user interface of the SecNumAcadémie MOOC. At the top, there is a navigation bar with links for 'ACCUEIL', 'FORUMS', 'MON PROFIL', and 'F.A.Q.', along with a power icon and the 'SecNumAcadémie ANSSI' logo. Below this is a 'MODULES' section with four cards, each representing a course module. Each card includes a title, a progress indicator, and a time spent indicator.

- 1. PANORAMA DE LA SSI**: Progression (info icon), Temps passé (clock icon)
- 2. SÉCURITÉ DE L'AUTHENTIFICATION**: Progression (info icon), Temps passé (clock icon)
- 3. SÉCURITÉ SUR INTERNET**: Progression (info icon), Temps passé (clock icon)
- 4. SÉCURITÉ DU POSTE DE TRAVAIL ET NOMADISME**: Progression (info icon), Temps passé (clock icon)

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](http://www.ssi.gouv.fr/administration/guide/guide-d-hygiene-informatique)

INFORMER - SENSIBILISER

