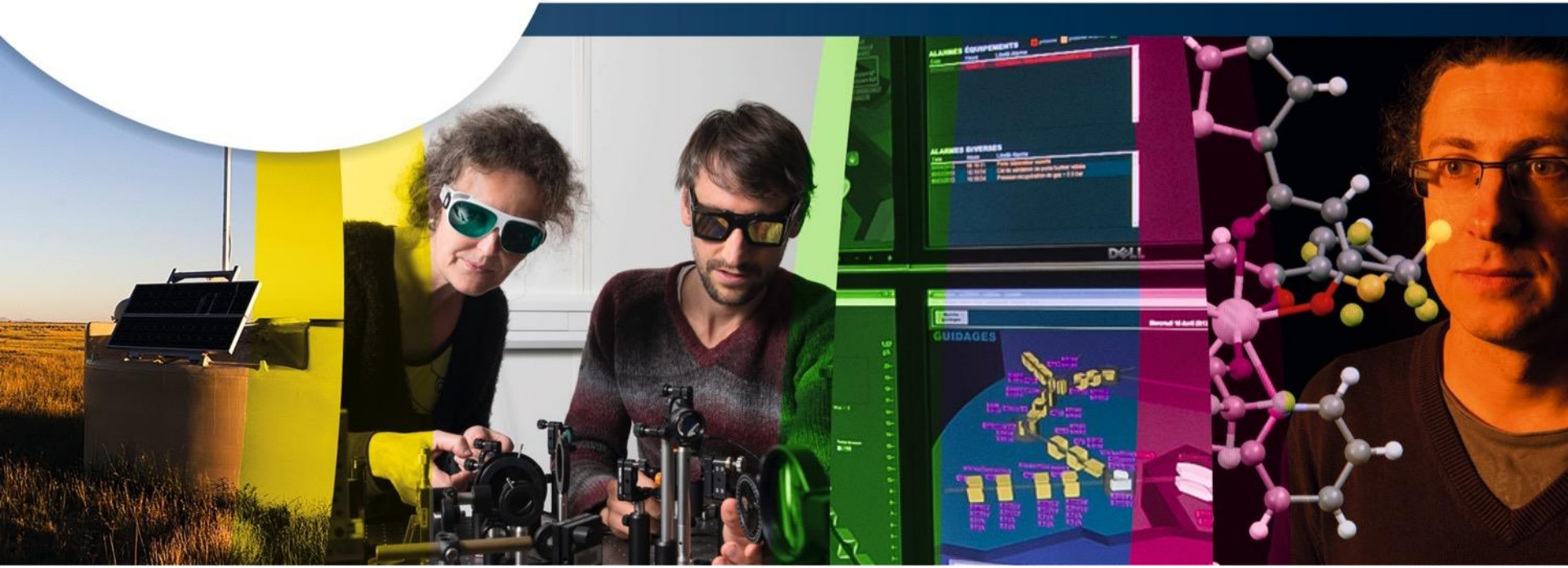
www.cnrs.fr

Risques



www.cnrs.fr

Sécurité de l'information

Sécurité de l'information

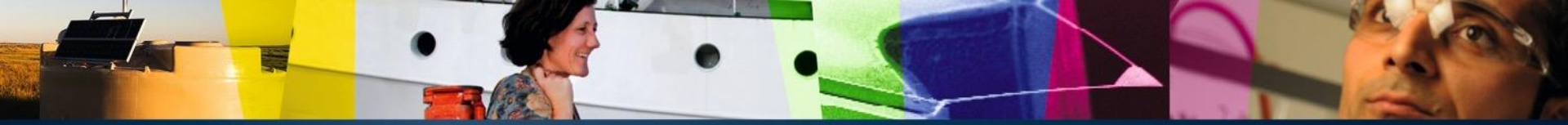
www.cnrs.fr

- La sécurité de l'information c'est la protection
  - Confidentialité
  - Intégrité
  - Disponibilité
- On y ajoute souvent d'autre propriétés
  - Authenticité
  - Imputabilité
  - Non-répudiation
  - Fiabilité

Disponibilité

www.cnrs.fr

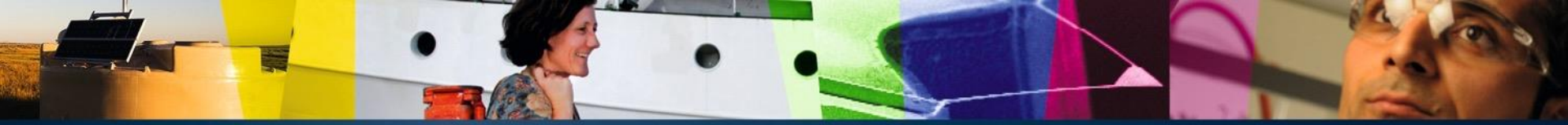
- Définition ISO 27000:2016
  - *propriété d'être accessible et utilisable à la demande par une entité autorisée*
- C'est l'exigence généralement mise en avant par les utilisateurs, les responsables des services (MOA)
- Exemples de non disponibilité sur un service web
  - Incendie salle machine, panne de serveur
  - Erreur d'exploitation
  - Déni de service
- Mesures de sécurité
  - Redondance



Intégrité

www.cnrs.fr

- Définition ISO 27000:2016
  - *propriété d'exactitude et de complétude*
- Trop souvent ignorée
- Le fondement de la confiance
- La non vérification de l'intégrité permet toutes sortes d'attaques
  - TLS
  - HTTP sans état, le serveur envoie une valeur dans un champ caché et l'attend dans la prochaine requête du client → modification par le client (prix d'un produit)
- Mesures de sécurité
  - Cryptographie



Confidentialité

www.cnrs.fr

- Définition ISO 27000:2016
  - *propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus non autorisés*
- Exemple de non confidentialité sur un site web
  - Fuite du contenu de la base de données à la suite
    - Injection SQL
    - Usurpation d'identité (vol de mot de passe)
    - Vol de session à l'aide d'un XSS
- Mesures de sécurité
  - Contrôle d'accès des personnes ayant le besoin d'en connaître
  - Chiffrement
  - Attention particulière à la gestion de l'authentification

Auditabilité

www.cnrs.fr

- Audibilité, terme générique qui regroupe différentes propriétés
  - *Authenticité : propriété selon laquelle une entité est ce qu'elle revendique être*
  - *Imputabilité : capacité à pouvoir attribuer une action à quelqu'un*
  - *Non-répudiation : capacité à prouver l'occurrence d'un événement ou d'une action donnée et des entités qui en sont à l'origine*
  - *Fiabilité : propriété relative à un comportement et des résultats prévus et cohérents*
- Domaine de la preuve
- Nécessité pour un site web
  - Détection d'incidents, analyse *post mortem*
- Mesures de sécurité
  - Journalisation
  - Authentification
  - Cryptographie : intégrité des journaux, authentification

www.cnrs.fr

Evénements redoutés

Menaces

www.cnrs.fr

- Menace, sens courant
  - Expression du projet de nuire à autrui
  - Éventualité d'un événement fâcheux
- Menace, sécurité de l'information
  - Cause potentielle d'un incident indésirable, qui peut nuire à un système ou à un organisme
- Source de la menace
  - Source non humaine
    - Inondation
  - Source humaine agissant de manière accidentelle
    - Erreur d'exploitation (rm –fr *)
  - Source humaine agissant de manière délibérée
    - Pirate

Impacts et conséquences

- 2 termes plus ou moins synonymes
  - Impact : immédiat
  - Conséquence : plus ou moins long terme
- Impact (EBIOS)
  - Fonctionnement
    - Missions
    - Capacités de décision
  - Humain
    - Sécurité des personnes
    - Lien social interne
  - Image
  - Financier
  - Patrimoine intellectuel
  - Juridique, non-conformité
  - Environnement

Impacts et conséquences

www.cnrs.fr

- Pour la recherche scientifique les conséquences sont souvent à long terme
  - Vol de données, impossibilité de déposer un brevet
  - C'est les paysage économique qui va changer quelques années plus tard
  - Les usines vont disparaître pour s'installer ailleurs
- Pensez à vos enfants !

www.cnrs.fr

Gestion des risques

Gestions des risques

www.cnrs.fr

- Faire face aux évènements redouté
- Appréciation des risques
  - Déterminer les impacts
  - Estimer la vraisemblance de leur survenue
- Traiter les risques

Traitement des risques

- 4 options de traitement des risques
  - Réduction du risque
    - Mise en place de mesures de sécurité pour réduire le risque
  - Maintien du risque
    - On accepte le risque tel quel
  - Refus du risque
    - On renonce au projet
  - Transfert du risque
    - Assurance
- C'est le rôle d'un responsable que de savoir prendre des risques
  - Arbitrage en fonction des coûts
  - Sans prise de risques aucun espoir de gain
  - Il doit être éclairé

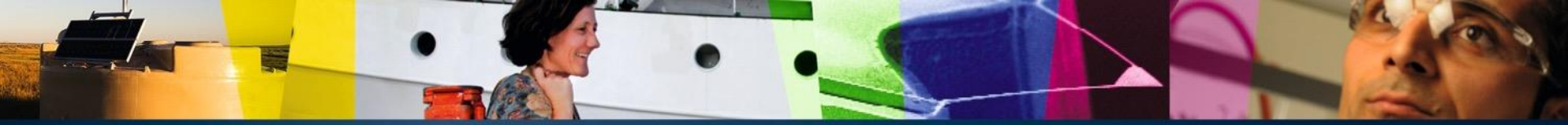
www.cnrs.fr

Cela n’arrive pas qu’aux autres

Dénis de service - victime

www.cnrs.fr

- Atteinte à la disponibilité
  - Saturation du serveur, du réseau par de nombreuses requêtes
- Assez fréquents
  - Pas toujours détectés ou remontés : manque de supervision
  - Serveurs contenant les notes des élèves
  - Serveurs DNS
- Attaques parfois très violentes
  - OVH 1,1Tbits/s
  - DynDNS est tombé → grand opérateurs inaccessibles
- Attaques extrêmement faciles
  - Requêtes légitimes
  - *DDoS as a service,* les premières minutes sont gratuites
  - Mirai
- Parades
  - Dimensionnement : charge acceptée, bande passante
  - *BGP → Sinkhole* ***de l'adresse IP***
  - Reroutage vers un équipement de nettoyage (coûteux)



Dénis de service – attaquant à notre insu

www.cnrs.fr

- Serveurs (NTP, DNS, SNMP, SSDP, etc.) mal configurés servant de relais
  - UDP avec adresse source usurpée et amplification (réponse beaucoup plus grosse que la requête)
- Intrusion d'une machine avec installation d'outil d'attaques
  - Il suffit à l'attaquant de réussir à déposer sur un serveur web un fichier PHP pour s'en servir comme relais pour des attaques
- On l'apprend généralement à la suite d'une plainte d'un site de e-commerce, d'une banque
- Impacts
  - Légaux
  - Image
  - Financiers
- Sécuriser ses systèmes : toute faille est susceptible d'être exploitée

Défigurations de sites

- Atteinte à **l'**intégrité + souvent à la disponibilité
  - Ajout ou/et modification de pages
  - L'accès au site web est souvent rendu impossible
- #OpFrance
  - Suite Charlie Hebdo
  - Nombreux sites défigurés
  - **Exploitation de failles dans les CMS ou les outils développés localement**
  - Utilisations par des attaquants de faible niveau de recettes et outils glanés sur Internet
  - Impacts
    - Image
    - Coût traitement des incidents et réinstallation des sites
- Parades
  - Qualité et sécurité du code
  - Mises à jour

Fuite d'informations

www.cnrs.fr

- Atteinte à la confidentialité
- Canard enchaîné
  - Publication sur Internet de données issue d'une base
  - Article dans le Canard enchaîné
  - Découverte sur un site développé localement d'une injection SQL par un outil automatique
  - Impacts
    - Image
    - Légaux : données à caractère personnel
  - Parades
    - Qualité et sécurité du développement
    - Limitation des données stockées, chiffrement
- Yahoo! et autres
  - Tout mot de passe connu est mort

Ethereum et DAO

www.cnrs.fr

- Ethereum
  - Blockchain
  - Smart contracts : code is law
- DAO
  - Fond d'investissement participatif et mutualisé
- Découverte et exploitation d'une vulnérabilité dans le code
  - Détournement de fonds
  - Impossible de corriger, le code est figé dans la block chain
- Les programmeurs ne sont pas infaillibles
  - Langages plus sûrs mais aussi plus contraignants
  - Preuve du code
- Quelle responsabilité pour le développeur ?

Scénarios catastrophe

www.cnrs.fr

- Blocage total d'un pays
  - C'est possible
    - Des mafias, des services étatiques possèdent le savoir faire et les moyens
    - Des éléments ont déjà été testés
      - Coupure électrique en Ukraine
      - Mise hors service de DynDNS
        - Il suffit d'un modèle de caméra vulnérable
      - Dénis de service pour bloquer les opérations financières
        - Le CNRS y a déjà participé à son insu
      - Stuxnet
    - 0 days
  - Pour le moment les attaques sont restées étrangement en deçà de ce qui est possible
    - Nombre d'experts pensent que jusqu'à maintenant on n'a eu que des bisounours
  - Inquiétante convergence d'éléments
    - Panorama de la cybersécurité en 2016 (Clusif)

Scénarios catastrophe

www.cnrs.fr

- Préoccupation des autorités
  - LPM, OIV
  - Directive européenne NIS (Network an Information Security)
  - Attention particulière au processus électoral
- Tous concernés, tous responsables
  - La non-sécurité d'un système peut être utilisée pour participer à une attaque d 'envergure
  - Intégrer la sécurité dans les développements

Une très bonne excuse pour les développeurs

- Qui a conçu des langages aussi tordus ?
  - Mind your language (ANSSI), présentation HES2015 (à partir de 37mn)

```
$h1=md5("QNKCDZO");
$h2=md5("240610708");
$h3=md5("A169818202");
$h4=md5("aaaaaaaaaaaumdozb");
$h5=sha1("badthingsrealmlavznik");
if ($h1==$h2) print("Collision\n");
if ($h2==$h3) print("Collision\n");
if ($h3==$h4) print("Collision\n");
if ($h4==$h5) print("Collision\n");
```

➔ 4 fois collisions : tout lors de == est converti à float(0)

www.cnrs.fr

Dans la peau des attaquants

Typologie des attaquants

www.cnrs.fr

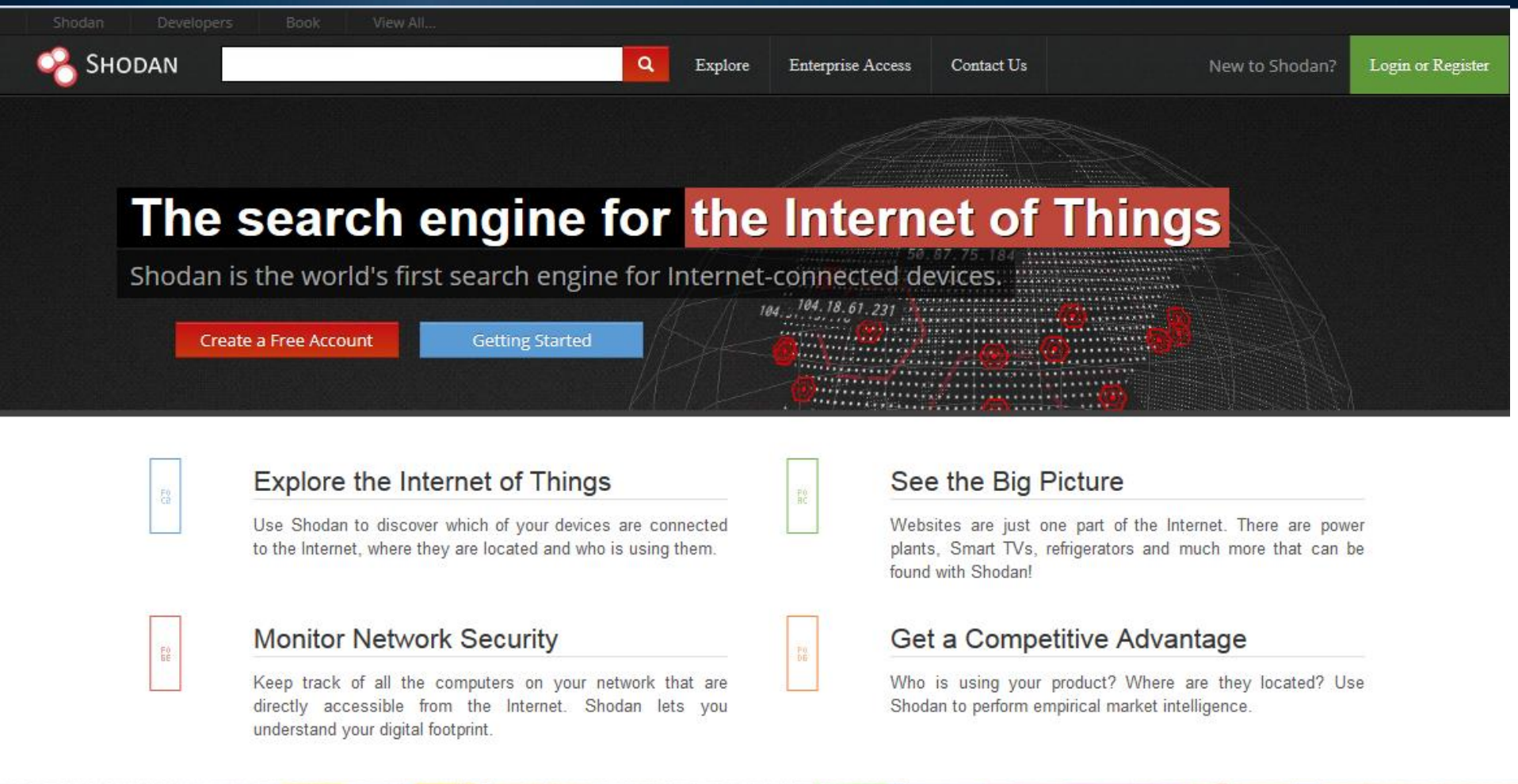
- Capacités différentes
  - Script kiddie
  - Mafias
  - Services étatiques
- Des motivations différentes
  - Ego
  - Cupidité
  - Cause à défendre
  - Soif de pouvoir, désir de domination

Google Dorks

www.cnrs.fr

- Utiliser Google pour rechercher des sites vulnérables
- site:cnrs.fr inurl:spip.php → CMS SPIP, trop large

Shodan


Shodan
Developers
Book
View All...
SHODAN
Explore
Enterprise Access
Contact Us
New to Shodan?
Login or Register
The search engine for the Internet of Things
Shodan is the world's first search engine for Internet-connected devices.
Create a Free Account
Getting Started
Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.
See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!
Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.
Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

157.136.38.177 camera-axis2.icsn.cnrs-gif.fr

City	**La Terrasse**
Country	**France**
Organization	**Centre National de la Recherche Scientifique**
ISP	**Centre National de la Recherche Scientifique**
Last Update	**2017-01-16T03:03:42.200437**
Hostnames	**camera-axis2.icsn.cnrs-gif.fr**
ASN	**AS2200**

Ports

2058

Services

2058
udp
upnp

```
HTTP/1.1 200 OK
CACHE-CONTROL: max-age=1800
DATE: Mon, 16 Jan 2017 04:03:39 GMT
EXT:
LOCATION: http://157.136.38.177:49155/rootdesc1.xml
SERVER: Linux/2.6.16, UPnP/1.0, Intel SDK for UPnP devices /1.2
ST: upnp:rootdevice
USN: uuid:Upnp-BasicDevice-1_0-00408C7A8808::upnp:rootdevice
```

Outils d'analyse de vulnérabilités

www.cnrs.fr

- Gratuits disponibles sur Internet
  - Pour les attaquants de peu d'envergure
- Attaque ciblée
  - Beaucoup plus subtil et discret
- Il vaut mieux faire procéder à ses propres tests d'intrusion que d'en attendre un « gratuit »

www.cnrs.fr

Comment se protéger ?

Quelques principes à appliquer

www.cnrs.fr

- En informatique il ne faut jamais ignorer les méchants
  - Impunité des criminels
  - Il y a de l'argent à gagner avec de faibles risques pour les criminels
  - L'attaque est facile, la défense ardue
- Corriger les failles connues
  - Appliquer sans délai les correctifs de sécurité : système, CMS, frameworks, bibliothèques, etc.
  - Suivre les avis de sécurité
    - CERT : CERT-FR, CERT Renater
    - Différents fournisseurs des produits utilisés
  - La première mesure à mettre en œuvre

Quelques principes à appliquer

www.cnrs.fr

- Prendre en compte la sécurité dans les développements
  - Approche par le risque
  - Se former aux bonnes pratiques et les appliquer

www.cnrs.fr

Questions ?