Bonnes pratiques pour les Utilisateurs

Sensibilisation aux menaces Internet & Formation aux bonnes pratiques pour les utilisateurs (BPU) de systèmes informatiques

Formation des Correspondants de Sécurité des Systèmes d'Information (CSSI)

Contexte de cette formation

- Large campagne de sensibilisation lancée sur tout le périmètre OSIRIS

- Formation « Internet sans crainte » : 1 jour ou 1,5 jours (avec TP) -> 2 à 3 sessions / an
- Groupe de travail national CNRS
- SMSI à l'université

- Formation « Internet sans crainte » (CERT-OSIRIS)  Sensibilisation interne (CSSI local)

- Lettre commune aux directeurs du président de l'université et de la déléguée régionale du CNRS

Contexte de cette formation

« Guide d'hygiène informatique » de l'ANSSI

I- Connaître précisément le système d'information et ses utilisateurs
II - Maîtriser le réseau
III - Mettre à niveau les logiciels -> BPU
IV- Authentification et mots de passe -> BPU
V- Sécuriser les équipements terminaux -> BPU
VI- Segmenter le réseau et contrôler l'annuaire
VII- Protéger le réseau interne de l'Internet
VIII- Surveiller les systèmes
IX- Sécuriser les postes des administrateurs
X- Contrôler l'accès aux locaux et sécurité physique
XI- Organiser la réaction en cas d'incident -> BPU
XII Faire auditer la sécurité
XIII Sensibiliser -> BPU

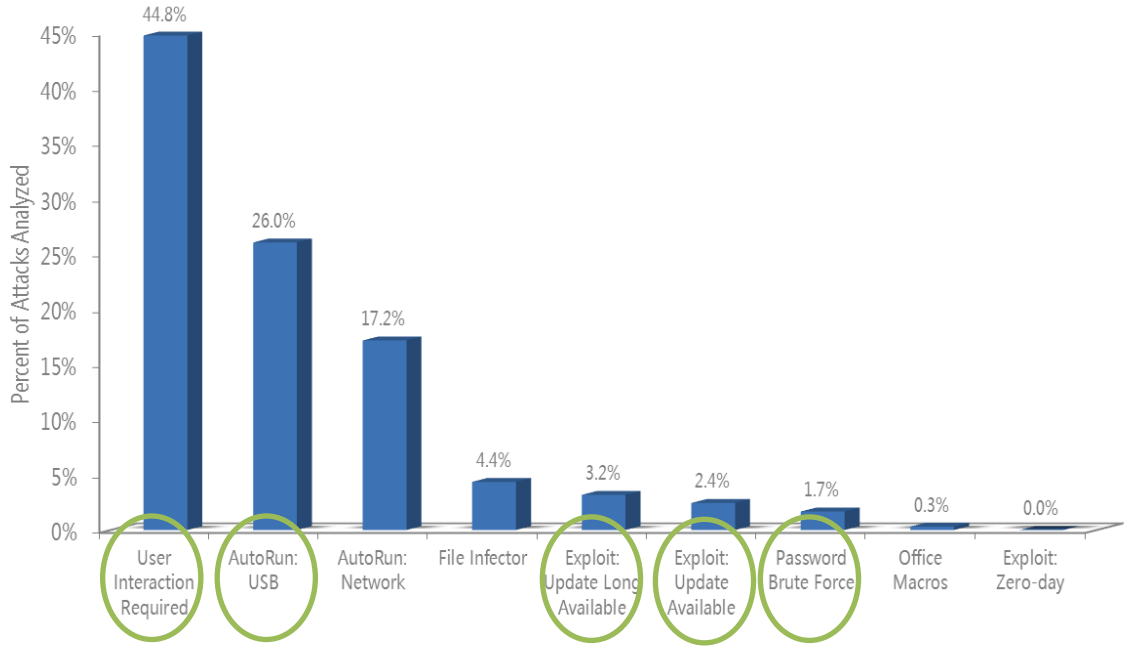
Les 10 règles des BPU **contribuent à la protection globale** des systèmes d'information.

http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf

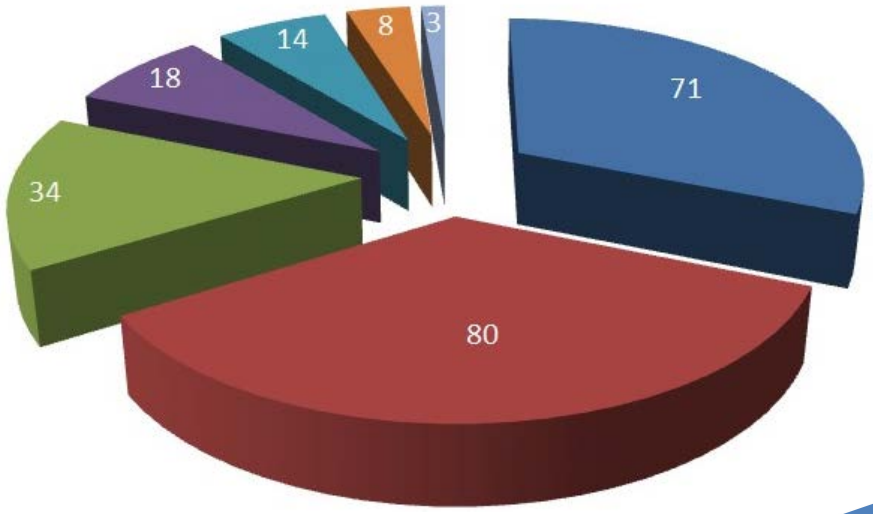
Objectifs de la démarche BPU

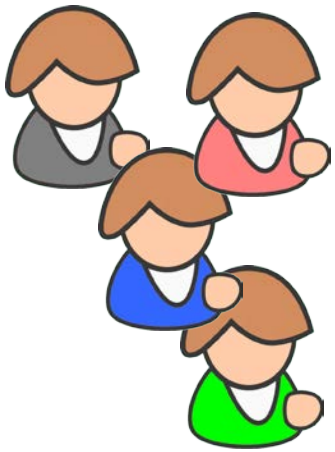
Améliorer de manière notable la protection de tous nos systèmes d'information

- Fournir au plus grand nombre les connaissances et les outils pour mieux se protéger
- Prise de conscience du rôle central et des responsabilités de l'utilisateur final
- Améliorer la perception des risques et des enjeux



Année 2012 : 232 incidents traités par le CERT OSIRIS

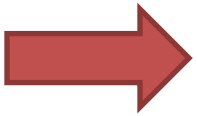




- Compromission poste de travail
- Atteinte aux droits d'auteurs
- Autres
- Compromission de compte
- Compromission serveur
- Vol / perte / destruction de matériel
- Vol / perte / diffusion de données sensibles

Plan d'actions & Ressources

Etape 1
Formation de formateurs
1 session longue + 4 sessions courtes



Etape 2
Sensibilisation des utilisateurs finaux
Organisation locale par le CSSI

Ressources

Kit de formation avec
- *2 diaporamas principaux*
- *4 diaporamas « goodies »*
- *dépliants « Les 10 règles d'or »*
- *base documentaire*

Les diaporamas sont **modifiables** :
- adaptation à votre environnement
- rajout d'éléments de sensibilisation spécifiques à votre structure

Sur demande : Accompagnement par le CERT-OSIRIS lors des sessions locales

Sommaire de cette formation

1ère partie :	présentation du kit	1h30
2ème partie :	mise en œuvre chez vous	1h

1ère partie : présentation du kit

Module 1
Panorama des menaces SSI

goodies : Les botnets

Module 2
Les règles élémentaires de protection

goodies : Gestion des risques

goodies : Défense en profondeur

goodies : Antivirus, que valent-ils ?

Dépliant joli

Textes règlementaires
Documents officiels
Revue d'actualité
Liens utiles

Module 1
Panorama des menaces SSI

Pourquoi ce module ?

- Introduction à l'usage des « bonnes pratiques »
- Connaitre *le contexte actuel des menaces sur internet*
- Comprendre *les attaques, les motivations*
- Percevoir *le risque*

Outils

- 1 diaporama (15 à 20 mn ?)
- Documents complémentaires : Revue d'actualités internationales 2012-2013

Résumé

1. *« **Tous** les internautes sont **exposés en permanence** à des menaces »*
2. *« Les attaques les plus sophistiquées (APT) sont **indétectables** »*
3. *« Usage des **bonnes pratiques** pour contrer les attaques/menaces courantes »*

Module 2
Les règles élémentaires de protection

☐ Pourquoi ce module ?

- Savoir comment se protéger
- Comprendre *le rôle de l'utilisateur final*
- Connaitre *les mesures de protection collectives et individuelles*
- Savoir *mettre en œuvre les bonnes pratiques*

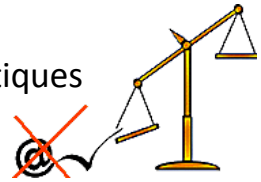
☐ Outils

- 1 diaporama personnalisé (40 à 45 minutes ?)
- Une liste de logiciels et de services à utiliser :
  - ✓ dans un cadre professionnel
  - ✓ dans un cadre privé

Module 2
Les règles élémentaires de protection

Obligations légales

Règle 1 - Respect des chartes informatiques



La protection technique du poste de travail

Règle 2 - Sauvegarde systématique et quotidienne des données

Règle 3 - Utilisation des outils de protection et mises à jour régulières

Règle 4 - Limitation des droits « administrateurs »

Un comportement avisé de l'utilisateur

Règle 5 - Protection de son poste de travail contre les accès illégitimes et le vol (chiffrement)

Règle 6 - Mots de passe robustes et personnels

Règle 7 - Attitude prudente vis-à-vis des supports de données amovibles (clés USB, etc.)

Règle 8 - Utilisation prudente d'Internet (navigation, téléchargements, services gratuits)

Règle 9 - Attitude prudente vis à vis des messages reçus

Règle 10 - Ordinateur infecté : les bons réflexes

Grille de lecture des diaporamas

Pour chacune des règles :
1- on énonce la règle avec des termes simples, compréhensibles de tous
2- on indique nos conseils de mise en œuvre
3- on donne une liste de logiciel, de pratiques

- ☒ Enoncé de la règle
- ☒ Les bonnes pratiques
- ☒ Les outils

- Dans tous les cas, on privilégie une solution interne ou un service local (s'ils existent !)
- Puis les solutions collectives proposées par l'université, le CNRS, Renater ou toute autre tutelle

Grille de lecture des diaporamas

- Passerelles pro-privé : plusieurs logiciels et bonnes pratiques sont utilisables sur tout équipement


Usage professionnel


Usage privé

- Indication des OS compatibles pour chaque outil


2ème partie : mise en œuvre chez vous

Préparation

- Mobiliser, motiver, convaincre (rôle des responsables, contexte SI local, incidents vécus…)
- Choisir la durée (par module, 1h, ½ journée…)
- Types de sessions (plénière, par équipe, par service, nouveaux arrivants…)
- Type d'accompagnement (mutualisation, CERT, lonesome)
- Adapter les supports au contexte local

Réalisation

- Sessions de sensibilisation / formation locales : à vous de jouer ☺
- Diffusion des dépliants

Suivi

- Récurrence
- Retour d'expérience (évolution des supports, des types de sessions, …)
- Mise à disposition des supports (site web CERT, intranet)