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

Goodies
Défense en profondeur

Septembre 2013

Sommaire

Défense en profondeur : les principes

- Les biens à protéger sont entourés de plusieurs lignes de défense :
  - segmentation et protection des réseaux (pare-feu, surveillance, ...etc.).
  - protection du poste (anti-virus, pare-feu, authentification, ...etc.).
  - *comportement de l'utilisateur (les bonnes pratiques).*

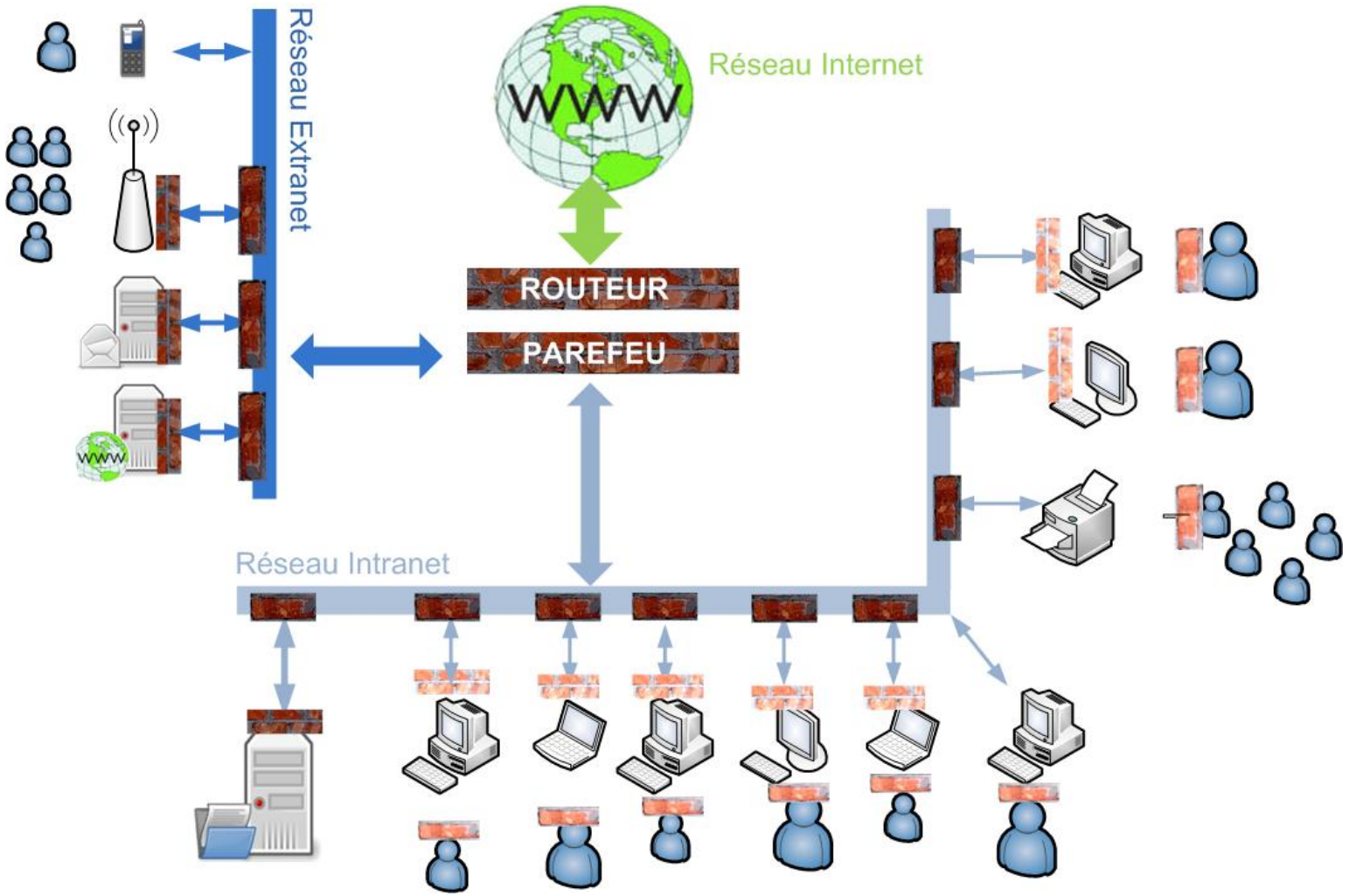
- Chaque ligne de défense a un rôle à jouer (affaiblir l'attaque, la gêner, la retarder, la neutraliser, l'empêcher).

- Chaque ligne de défense participe à la défense globale :
  - Le comportement « responsable » de l'utilisateur est indispensable au maintien de la sécurité de l'ensemble.

ANSSI : La défense en profondeur appliquée aux systèmes d'information (2004)

http://circulaire.legifrance.gouv.fr/pdf/2009/04/cir_2014.pdf

Les différents niveaux de protection



Défense en profondeur : les recommandations de l'ANSSI

Ces recommandations sont toutes mises en œuvre dans le cadre global de la politique de sécurité des systèmes d'information (PSSI) de l'unité.

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

Plusieurs recommandations sont déclinées dans les Bonnes Pratiques de l'Utilisateur (BPU). http://www.securite-informatique.gouv.fr/gp_rubrique34.html