Version 4df du : 29 avril 2010

Préconisations pour la protection des réseaux sans fil mis à la disposition des utilisateurs nomades

L'ensemble des sites RENATER est invité à mettre en œuvre les propositions explicitées ci-dessous.

Objectifs

La plupart des institutions, (établissements et organismes) mettent à disposition des personnes nomades un accès réseau, le plus souvent un accès sans fil (WiFi). Cette note, portant sur la sécurisation des accès sans fil, comporte un certain nombre de dispositions qui sont également applicables aux réseaux filaires.

Les préconisations explicitées ci-dessous ciblent deux objectifs :

- Pour l'institution « hôte »: préciser les moyens lui permettant de protéger les accès réseaux afin de minimiser le risque introduit par la présence d'utilisateurs externes et lui permettant de respecter les obligations légales liées à la fourniture du service ;
- Pour l'utilisateur nomade : lui recommander les pratiques lui garantissant tout à la fois une meilleure protection possible de ses flux et une conformité par rapport aux chartes d'usage en vigueur sur le site d'accueil.

Préconisations

La sécurité des points d'accès

Appliquer les préconisations explicités dans la partie 4.1 du document « Sécurité des réseaux sans fil (Wi-Fi) » : http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-002/

- Activer les fonctionnalités de chiffrement du lien radio pour éviter les écoutes
  - Ce qui est préconisé :
  - Activer le 802.11i mode « Enterprise » (WPA2 Entreprise) ; Ce mode doit intégrer le chiffrement fort AES (CCMP)
- Solution de repli (si la préconisation ci-dessus ne peut être appliquée):

- Activer WPA avec TKIP

Dans les deux cas, utiliser une « passphrase » robuste et suffisamment longue, et un SSID original ;

Authentification des accès

- Dans la communauté RENATER tous les accès doivent être authentifiés et nominatifs
- Solutions :
  - Ce qui est préconisé :
    - Authentification de type 802.1X avec protocole EAP-TTLS. Cette méthode d'authentification est notamment préconisée par le service « Eduroam ». Le mode « Enterprise » intègre le 802.1X pour l'authentification.
    - Authentification WPA « mode entreprise » de préférence, sinon, WPA PSK.
    - Pour les visiteurs et participants aux conférences, allocation de crédits temporaires nominatifs garantissant le lien entre la personne et le crédit affecté.
  - Par défaut mais non conseillé :
    - Passage par un portail captif pour l'authentification. ATTENTION dans ce cas le lien radio n'active aucune fonctionnalité de chiffrement. Il est important d'en informer les utilisateurs et de leur laisser la possibilité d'activer les moyens de protection mis à leur disposition par leur organisme de rattachement.

Infrastructure de transport IP

- Séparer les réseaux dits « invités » du réseau interne de l'établissement, par une politique de filtrage pertinente
- Mettre en place des mesures de filtrage similaires à ce que l'on trouve sur les réseaux filaires pour la protection des utilisateurs nomades
- Ouvrir au maximum, en sortie, la liste de ports préconisée dans le document « Politique de filtrage pour les réseaux invités », et par défaut interdire le reste. Il s'agit de permettre aux usagers nomades des accès permettant le télétravail dans de bonnes conditions tout en limitant les types d'entrées/sorties dans le réseau
  - la liste de ports ouverts en sortie doit notamment permettre aux nomades d'utiliser des protocoles sécurisés (POPS, IMAPS, HTTPS, VPN-SSL, VPN-IPSEC, SSH) pour joindre leur établissement de rattachement
- Journalisation

- Mettre en œuvre une politique appropriée de journalisation des connexions au réseau invité, centraliser les traces, assurer une analyse continue des traces.
- En ce qui concerne les connexions vers l'Internet, la loi impose une journalisation. Cette journalisation doit permettre en cas d'incident de retrouver la source. Il est préconisé de mettre en œuvre des outils de journalisation adaptés (Proxy-web par exemple).

- Mesures de contrôle complémentaires
  - Limitation du nombre de connexions par unité de temps
    - Surveiller son réseau (sondes IDS, Kismet,…);
  - Auditer son réseau
  - Exporter les journaux collectés vers une machine dédiée. Les contrôler régulièrement.

Préconisation aux établissements de rattachement des personnes nomades

Les établissements sont invités à informer leurs utilisateurs :

- à propos des risques liés aux réseaux sans fil et des solutions préconisées par la politique de sécurité de l'établissement ;
- de leur obligation de se conformer à la charte du site d'accueil, ou d'une charte globale type « Eduroam » ;
- des moyens mis à leur disposition pour protéger leurs flux réseau :
  - soit le chiffrement au niveau applicatif par utilisation des protocoles comme POPS, IMAPS, HTTPS, …
  - soit l'activation de tunnels type VPN-SSL, VPN-IPSEC ou SSH.

Les personnes nomades sont invitées à prendre connaissance de la note *« Partir en mission avec son téléphone mobile, son assistant personnel ou son ordinateur portable »* : http://www.ssi.gouv.fr/site_article170.html .

O o O o O