Bordeaux, le 23/10/2017

Affaire suivie par :
Patrick Bénazet
RSSI Académie de Bordeaux
rssi@ac-bordeaux.fr

RECOMMANDATION DE SECURITE

Utilisation des réseaux sans fil 'WiFi' (normes IEEE 802.11)

Référence	SG-SSI-2017-REC-01
Date dernière version Date 4ème version Date 3ième version Date 2nd version Date 1ère version	23/12/2017 02/10/2014 23/11/2012 12/03/2009 24/03/2006
Destinataires cibles	Rectorat : DSI, DANE, DAFPIC DSDEN : CDTI EPLE : chef d'établissement, correspondant sécurité
Destinataires pour information	DSR Pôles de compétences : sécurité (Aix-en-Provence), réseaux (Clermont-Ferrand)
Source	ANSSI « PSSIE - Politique de Sécurité des Systèmes d'Information de l'Etat » 17 juillet 2014 Note technique ANSSI « Recommandations de sécurité relatives aux réseaux WiFi » 30 mars 2013 Guide ANSSI « l'hygiène informatique en entreprise » octobre 2012 Courrier du 11/05/2006 de M ANTOINE directeur DPMA Courrier RSSI du 25/01/05 aux chefs d'établissements Avis CERTA-2002-REC-002
Pièces jointes	SG-SSI-2017-FICHE-02 Formulaire de déclaration d'un réseau WiFi
Niveau de confidentialité	C1 : usage interne MEN

SOMMAIRE

INTRODUCTION et REFERENCES

Les recommandations issues de l'ANSSI [1] et publiées dans différents documents

- la PSSIE du 17 juillet 2014, objectif 15 « sécurité des réseaux sans-fil » [2]
- la note technique de l'ANSSI du 30 mars 2013 « Recommandations de sécurité relatives aux réseaux WiFi »[3]
- le guide de l'**ANSSI « l'hygiène informatique en entreprise »[4]** , règle n°26

sont particulièrement explicites et imposent de maitriser le déploiement, la configuration et l'usage des réseaux sans fil.

La réalisation de ces objectifs passe par :

- une analyse de risque spécifique
- le confinement, il faut s'assurer d' « un cloisonnement du réseau d'accès Wifi du reste du réseau : l'interconnexion au réseau principal doit se faire au travers d'une passerelle maitrisée permettant de tracer les accès et de restreindre les échanges aux seuls flux nécessaires »
- l'interdiction de réseaux sans-fil sur des SI manipulant des données jugées sensibles

De plus selon l'ANSSI « quel que soit le niveau de sécurité des réseaux WiFi pouvant etre mis en oeuvre, il reste préférable d'utiliser des connexions filaires ».

Au sein du ministère, **le courrier[5] du 18 mai 2006 émis par les services de la DPMA[6] du MEN** constitue la référence en ce qui concerne la mise en œuvre de la technologie WiFi ouvrant des accès aux ressources internes de notre système d'information (SI).

Les préconisations décrites dans ce document spécifient que les personnes juridiquement responsables des établissements de l'Education Nationale se doivent « de limiter l'utilisation des réseaux aux seules personnes habilitées ainsi que d'assurer la confidentialité des traitements ». Dans ce cadre « les réseaux WiFi ne devraient pas être utilisés pour constituer une liaison d'importance vitale ou pour véhiculer des informations pouvant être critiques pour le fonctionnement de la structure ».

La mise en œuvre de bornes d'accès WiFi engendre **des contraintes de sécurité spécifiques sous peine de fragiliser l'ensemble du système d'information académique**. Elles impliquent la mise en œuvre d'équipements, d'opérations d'administration et de maintenance dans le respect des standards académiques.

Dans la continuité des préconisations nationales, le Responsable Sécurité des Systèmes d'Information (RSSI) et l'Ingénieur Sécurité Racine (ISR) ont établi des normes destinées à garantir le niveau de sécurité du SI académique.

LES RISQUES

Le périmètre d'application de la présente recommandation est constitué par les réseaux sans fil utilisés comme alternative aux réseaux informatiques filaires d'entreprise (réseaux locaux LAN). Ils ne nécessitent aucune déclaration à l'ARCEP[7] puisqu'il s'agit de réseau interne à l'inverse des

---

[1] Agence Nationale de la Sécurité des Systèmes d'Information

[2] http://http://www.ssi.gouv.fr/IMG/pdf/pssie_anssi.pdf

[3] http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-des-liaisons-sans-fil/recommandations-de-securite-relatives-aux-reseaux-wifi.html

[4] http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/l-anssi-publie-la-version-finalisee-du-guide-d-hygiene-informatique.html

[5] « Mise en œuvre de bornes WiFI ouvrant des accès aux ressources internes du systéme d'information (SI) » M D ANTOINE directeur des personnels, de la modernisation et de l'administration

[6] Direction des Personnels, de la Modernisation et de l'Administration

[7] Autorité de Régulation des Communications Electroniques et des Postes

réseaux indépendants destinés à relier plusieurs services ou établissements.
Ces réseaux, communément appelés WiFi ("Wireless Fidelity"), respectent la norme IEEE 802.11.
La facilité de déploiement, le faible coût d'investissement et la mobilité qu'offrent les réseaux WiFi en font une alternative attrayante vis-à-vis des réseaux filaires. De plus, le WiFi est interopérable avec les réseaux filaires et garantit une grande souplesse sur la topologie du réseau.

Cette technologie s'appuie sur un support de transport radio nécessitant une attention particulière sur trois aspects de sécurité :
- la **disponibilité** du réseau : interférences, brouillage, partages des ressources
- la **confidentialité** des échanges
- le **contrôle** et la **traçabilité** des connexions au réseau sans fil, et au-delà, sur Internet

Sur le plan juridique, les risques se concentrent à la fois sur
- le **secret de la correspondance**
- l'**atteinte aux systèmes de traitement automatisé de données** (STAD).

Une réflexion conduite avant l'installation d'un réseau sans fil dans le respect des préconisations de cette recommandation conduit à minimiser les risques.

Des dispositifs de sécurité doivent être mis en place, imposant des caractéristiques pour les matériels déployés, et des règles d'usage respectées suivant le degré de sensibilité du réseau connecté et des usages. Cette recommandation tient compte de la diversité des environnements constituant notre SI.

Le WiFi comme l'ensemble des technologies radio s'appuie sur les **rayonnements électromagnétiques** ; à ce titre les effets sur l'**intégrité des personnes** ne peuvent être négligés. Cependant les puissances considérées en font une technologie moins agressive que la téléphonie mobile (antenne relais et téléphone). Un certain nombre d'avis d'organismes référents (ANSES [8], OMS[9], SCENIHR[10] ...) sont collectés sur le site SSI académique[11] afin d'aider la PJR du site à évaluer les risques encourus.

TECHNOLOGIES ET STANDARDS

Le mode infrastructure :
Un réseau sans fil est fondé sur une architecture cellulaire où chaque cellule est contrôlée par un point d'accès (AP Access Point). Les points d'accès peuvent être reliés entre eux par des liaisons radio ou filaires constituant un réseau appelé ESS (Extended Service Set). Un terminal peut alors passer d'un point d'accès à un autre en restant sur le même réseau (mobilité).
Pour s'identifier auprès d'un réseau, les utilisateurs d'un réseau sans fil utilisent un identifiant de réseau appelé « SSID ». Les AP émettent au choix sur l'un des 13 canaux possibles de la bande de fréquence de 2.4Ghz ou sur les 8 canaux de la bande de fréquence de 5GHz. Chaque terminal sans fil reçoit donc tout le trafic circulant sur le réseau. Si ce terminal scrute simultanément plusieurs canaux, il recevra alors le trafic de tous les réseaux qui l'entoure.

[8] Agence Nationale de Sécurité Sanitaire de l'Alimentation, de l'Environnement et du Travail
[9] Organisation Mondiale de la Santé
[10] Scientific Committee on Emerging and Newly Identified Health Risks
[11] http://ssi.ac-bordeaux.fr

Le mode ad-hoc :
Il existe un mode de communication « point à point » entre des équipements sans fil. Ce mode appelé « ad-hoc » permet de connecter des postes entre eux sans utiliser de point d'accès.
Il est possible d'offrir un service d'accès WiFi sans intervention préalable sur les postes utilisateurs tout en imposant une authentification. Ce procédé, appelé « **portail captif** » est basé sur la redirection automatique vers une page web sécurisée avec authentification de l'utilisateur.

Les bornes WiFi (point d'accès AP)
Les points d'accès WiFi se divisent en deux grandes familles :
- les bornes dites « intelligentes », « lourdes » ou « actives », elles peuvent fonctionner de façon autonome ou parfois en groupement de quelques unités avec la notion de maitre et d'esclave qui permet une administration centralisée ; elles apportent une solution aux petites structures
- les bornes dites « passives » sont pilotées par un élément central (contrôleur radio, « switch wireless » ; cet équipement présente généralement des fonctionnalités avancées (passerelle VPN, portail captif, service radius ...)

La technologie WiFi ne cesse d'évoluer offrant toujours plus de débit et permettre une meilleure prise en charge de la sécurité. Voici **les principales normes** :

Norme	Date de validation	Débit théorique (Mbit/s)	Débit utile généralement observé (Mbit/s)	Fréquence (GHz)
802.11b	1999	11	4,5	2,4
802.11a	1999	54	23	5
802.11g	2003	54	20	2,4
802.11n	2009	600	> 100	2,4 et/ou 5
802.11ac	2014	6933 (8 canaux x 866,7 Mbps)	Retours d'utilisation insuffisants	5

Diverses solutions propriétaires dont les plus répandues sont MIMO (Multiple Input Multiple Output) et SuperG Elles consistent à accroître le nombre d'émetteurs/receveurs (d'antennes) et transmissions (plusieurs signaux sur le même canal) provenant d'un point d'accès pour démultiplier les performances.

Deux autres normes importantes viennent s'ajouter :
- **802.11i** : renfort des dispositifs de sécurité radio (contrôle d'intégrité, authentification et confidentialité). L'algorithme de chiffrement utilisé est nommé WPA2 (ou AES).
- **802.11e** : prise en compte d'objectifs liés à la QoS notamment afin de favoriser les usages autour du transport de la voix, de l'audio et de la vidéo

RECOMMANDATIONS DE SECURITE

La mise en œuvre d'une solution WiFi sur les sites Racine de l'académie doit s'effectuer sous le contrôle du RSSI et de l'ISR. Dans le cadre des établissements scolaires ce contrôle estdélégué à Scol-Teleservices qui s'assure du respect des règles de sécurité et prodigue un accompagnement dans le choix et l'installation des équipements.

Les services de la DSI du Rectorat de Bordeaux ont développé une solution technique de type portail captif (AMONet) assurant une cohérence avec l'environnement EOLE déployé dans l'ensemble des EPLE. Elle est basée sur un serveur informatique dédié et prend en compte les aspects d'authentification et de journalisation.

Dans tous les cas d'usages, il convient de respecter les recommandations suivantes :

Avant la mise en oeuvre :

- mener **une étude préalable au déploiement** : décrire la zone de couverture et ses spécificités (interférence, obstacles), optimiser l'emplacement des bornes et régler la puissance d'émission au minimum nécessaire – décrire les données et fonctions utilisées sur le réseau
- en fonction de la finalité envisagée pour l'utilisation du WiFi :
    - extension d'un réseau local
    - accès à des services
    - interconnexion de bâtiments distants au sein d'un même établissement déterminer

les objectifs de sécurité en termes de : disponibilité, intégrité, confidentialité, qualité des preuves techniques d'accès aux services et aux actions.

Cette phase a fait l'objet d'une étude en fonction des ressources accédées dans les différentes zones RACINE donnant lieu à des préconisations en termes de **chiffrement** des données et d'**authentification**. Les principales préconisations sont reproduites dans le tableau suivant.

Zone de confiance RACINE / Méthode de chiffrement / authentification	Racine AGRIATES : Etablissement scolaires, CIO, GRETA		Racine : services académiques du Rectorat, des Inspections Académiques, des Inspections de l'Education Nationale	Interconnexion de bâtiments au sein d'un même établissement
	Réseau administratif	Réseau pédagogique		
Cryptage WEP	Réseau WiFi interdits	insuffisant	insuffisant	insuffisant
Cryptage WPA-TKIP		insuffisant	insuffisant	insuffisant
Cryptage WPA2 (AES) / authentification basique (identifiant et mot de passe avec validation du certificat serveur)		admis sous conditions	insuffisant	insuffisant
Cryptage WPA2 (AES) / authentification forte par certificat (avec validation du certificat serveur)		préconisé	insuffisant	admis sous conditions
Cryptage WPA2 (AES) / authentification forte par certificat avec clef privée non copiable (avec validation du certificat serveur)		inutile	préconisé	préconisé
Cryptage WPA2 (AES) / authentification forte par clef OTP (avec validation du certificat serveur)		inutile	préconisé	sans objet

- Suivre la procédure de **déclaration de l'installation** : toute borne WiFi est soumise à l'accord de la PJR du site. Une déclaration écrite (fiche à télécharger sur le site http://ssi.ac-bordeaux.fr, SG-SSI-2009-FICHE-01) précisant l'emplacement et le nombre de bornes, les canaux utilisés, les dispositifs de sécurités et de conservation des log doit lui être remis. Une copie de ce document doit être communiquée au RSSI académique.

Principes techniques à respecter :

- **Contrôler les accès physiques** aux équipements
- **Modifier l'identifiant réseau des bornes** (SSID) par défaut, éviter les noms de SSID attractifs. Désactiver la diffusion de SSID ne peut être considéré comme une mesure de sécurité efficace
- **Changer les mots de passe** par défaut d'accès aux équipements et les modifier régulièrement
- **Désactiver les services non utilisés** (DHCP, SNMP, telnet,…).
- Procéder à la **mise à jour régulière du « firmware »** (logiciel d'exploitation) des bornes
- **Activer la conservation des traces des sessions sur 12 mois glissants**
- Préférer l'usage de commutateurs (switchs) plutôt que de concentrateurs (hubs)
- **Proscrire l'usage du mode « ad-hoc »** sur les postes de travail
- **Informer les utilisateurs** : la sécurité d'un réseau passe avant tout par la prévention et la sensibilisation des utilisateurs (cf charte d'usages des ressources multimédia)
- **Gérer et surveiller son réseau** : la gestion et la surveillance d'un réseau sans fil peut s'effectuer à deux niveaux. La surveillance au niveau IP avec un système de détection

d’intrusions classique (prelude, snort, ...) et la surveillance au niveau physique (radio) avec des outils dédiés (Kismet, certains contrôleurs ou outils d’administration de bornes WiFi, ...).
- **Auditer régulièrement son réseau sans fil** pour s’assurer qu’il ne couvre pas des zones non désirées et pour contrôler qu’il n’existe pas de réseau sans fil non désiré dans le périmètre à sécuriser (borne sauvage ou bornes de voisins).