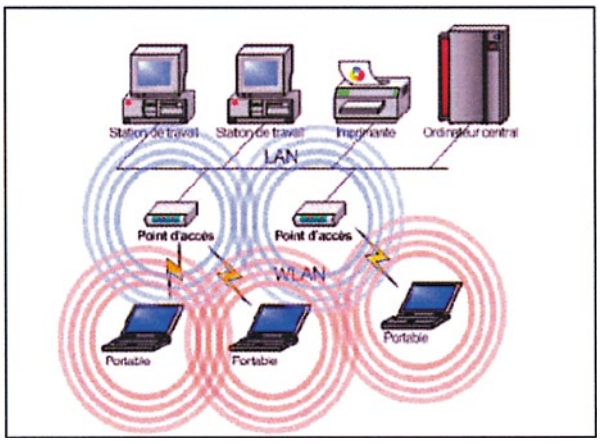
Réseaux sans fil, mais en sécurité

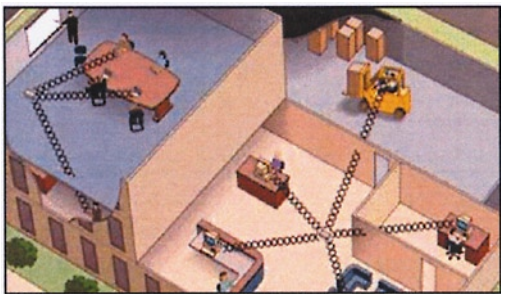
Les nouvelles solutions de réseaux sans fil, (Wi-Fi pour Wireless Fidelity) ou WLAN (Wireless Local Area Network), regroupées sous la norme 802.11, sont comparables à un segment Ethernet partagé grâce à une liaison de type radio.

Les applications sont multiples et variées puisqu 'elles permettent aussi bien la constitution de réseaux privés fermés que la mise en place de réseaux publics et ouverts. Il est alors impossible de parler de solution clé en main.
La grande particularité du Wi-Fi est d'être un système rapide à déployer, pour un coût raisonnable. De plus, il se déploie sans câblage ou presque de fils ou de prises, et permet de se connecter partout à l'intérieur de l'entreprise. Les avantages sont indéniables : mobilité, évolutivité, souplesse et coût réduit. Le phénomène est comparable au portable téléphonique, il envahit nos équipements informatiques (PC portable, PDA, équipements techniques…) et amplifie le mouvement nomade.

Les projets sont nombreux, ils vont de la borne d'information (hot spots) qui peut s'installer partout, à l'installation de systèmes radio dans les entrepôts afin de permettre à l'ERP de l'entreprise de connaître en temps réel les flux de produits… à l'accès en temps réel pour les réunions des groupes d'étude, entre le lit d'hôpital et les informations concernant le patient pour les médecins et le personnel hospitalier.. ou à cet homme d'affaire endormi sur son fauteuil d'avion devant son écran de PC où un message lui indique que l'on effectue la mise en place du dernier patch de sécurité….
Mais au même moment à proximité d'une entreprise, un mercenaire équipé d'un portable est enfin parvenu à capter les ondes du réseau sans fil sur son écran. Il commence à déchiffrer les trames qui lui permettront d'obtenir un mot de passe pour se connecter ensuite sur l'ordinateur central de l'entreprise. Il pourra ainsi mener à bien son « job d'ingérence économique » plus vite que la dernière fois, car il avait dû repérer furtivement les 4 touches un peu sale du clavier hexa du cariste pour trouver la bonne combinaison de connexion …

L'ouverture de nos moyens de communication n'est pas sans risques, car nos informations et nos connaissances peuvent si nous n'y veillons pas, être altérées par des phénomènes externes.
Ils proviennent de l'homme, de l'organisation, des procédures et des dispositifs à travers les erreurs, les pannes, les accidents et surtout, de façon majoritaire, à travers la malveillance qui représente les deux tiers des pertes induites par ce que l'on appelle la sinistralité informatique.



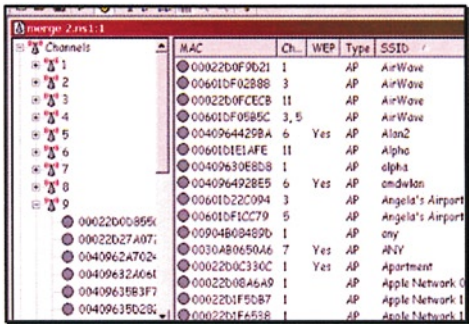


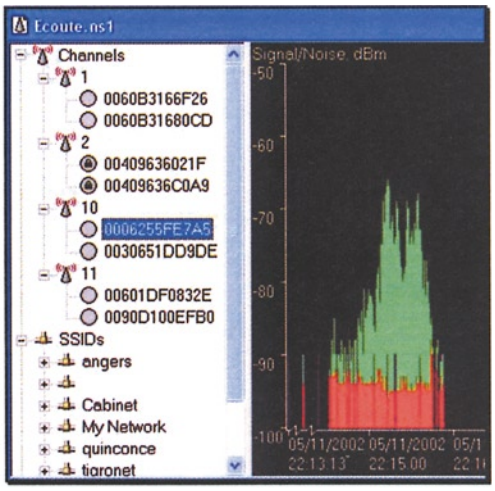
Les WiFi n'y échappent pas. Au contraire leurs déploiements faciles facilitent les vulnérabilités. Un réseau sans fil non sécurisé revient schématiquement pour l'entreprise

à installer dans la rue une prise réseau brassée sur son réseau interne.

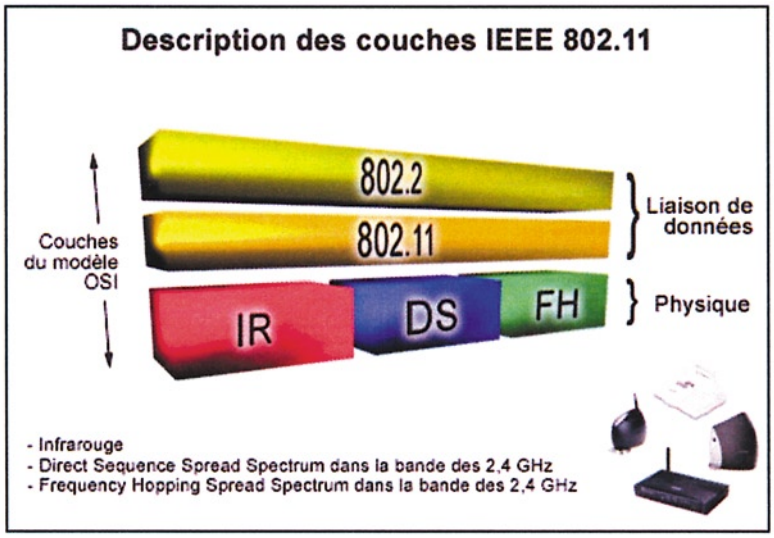
Les normes WiFi

Aujourd'hui, on parle des normes 802.11, car il en existe plusieurs versions, pas forcément compatibles entre elles. Par abus de langage (et pour des raisons de marketing) le nom de la norme se confond aujourd'hui avec le nom de la certification délivrée par la WECA (Wireless Ethernet Compatibility Alliance). C'est en réalité un réseau répondant à la norme 802.11., noté Wifi ou parfois Wi-Fi.





Les différents constructeurs émulent ce marché, bien que les différences majeures concernent les fréquences utilisées et les débits et portées atteints. Les caractéristiques des normes 80.11i et 802.11g précisent et enrichissent l'offre WiFi.



Caractéristiques de toutes les évolutions actuelles de la norme. La norme 802.11b, la plus utilisée actuellement, permet de couvrir autour d'un point d'accès une zone d'environ 100 mètres avec un débit de 11Mbps. Cette zone de couverture va varier en fonction des obstacles rencontrés par l'onde radio, de la puissance d'émission des points d'accès ainsi que de la sensibilité des antennes. Typiquement, un client et un point d'accès vont décider en fonction de la distance les séparant de l'encodage et du débit avec lesquels ils vont communiquer.

Les débits choisis seront : 11Mbps, 5,5Mbps, 2Mbps et 1Mbps. Avec un débit de 1Mbps, la zone de couverture que l'on va couvrir sera d'environ 1km en extérieur. S'il faut atteindre des distances supérieures, des antennes directionnelles seront nécessaires.

Pour indiquer sa présence, un point d'accès va annoncer, par l'envoi d'une trame précise à destination de tous les clients de la zone de couverture un SSID (Service Set Identifier) 10 fois par seconde, représentant le nom du réseau. Tous les clients qui appartiennent à ce nom de réseau pourront donc s'associer avec le point d'accès et communiquer.

Caractéristiques de toutes les évolutions actuelles de la norme 802.11

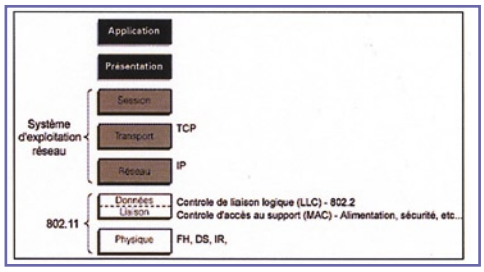
Normes 802.11	Caractéristiques
802.11a	Haut débit (30 Mbit/s effectifs) sur la bande des 5 GHz
802.11b	Haut débit (6 Mbit/s effectifs) sur la bande des 2,4 GHz
802.11c	Travaux suspendus
802.11d	Travaux suspendus
802.11e	Travaux sur la qualité de service (QoS) dans les normes existantes. Par exemple, la transmission synchrone (voix)
802.11f	Travaux sur le protocole Inter Access Point Protocol, qui doit permettre aux bornes d'accès de dialoguer entre elles
802.11g	Haut débit (54 Mbit/s théoriques) sur la bande des 2,4 GHz
802.11h	Adoption des technologies DFS (Dynamic Frequency Solution) et TPC (Transmit Power Control), pour une conformité avec les normes européennes
802.11i	Travaux sur la sécurité des transmissions sur les bandes de fréquence 2,4 GHz et 5 GHz. Amélioration de l'algorithme WEP
802.11j	Convergence des standards américain 802.11 et européen Hiperlan, tous deux fonctionnant sur la bande de fréquence des 5 GHz

En France, l'ART (Autorité de Régulation des Télécommunications) permet d'utiliser 13 canaux de 22 Mhz chacun dans la bande des 2,4 Ghz. L'ART (Autorité de Régulation des Télécommunications) vient de libérer l'ensemble des départements français pour l'utilisation du WiFi, en intérieur comme en extérieur, avec des limites de puis-

sance d'antenne (100 mW sur la plupart des canaux).

Pour bien comprendre les réseaux sans fil, il est nécessaire de remarquer que ces normes concernent les couches basses 1&2 du modèle ISO.

La couche physique (1) définit la modulation des ondes radio-électriques (initialement deux techniques radio à étalement de spectre et une spécification d'infrarouge), et les caractéristiques de la signalisation pour la transmission de données, tandis que la couche liaison de données (2) définit l'interface entre le bus de la machine et la couche physique, notamment une méthode d'accès proche de celle utilisée dans le standard Ethernet et les règles de communication entre les différentes stations.



La couche Liaison de données de la norme 802.11 est composée de deux sous-couches : la couche de contrôle de la liaison logique (Logical Link Control, notée LLC) et la couche de contrôle d'accès au support (Media Access Control, ou MAC).

Les normes 802.11 apparues en 1997, traduisent des caractéristiques de type liaison, et n'intègrent pas nativement de fonction de continuité de liaison (liaison rattachée à une station), ni de fonction de routage.

Le standard 802.11 définit deux modes opératoires :
· Le mode infrastructure dans lequel les clients sans fil sont connectés à un point d'accès. Il s'agit généralement du mode par défaut des cartes 802.11b.

· Le mode ad hoc dans lequel les clients sont connectés les uns aux autres sans aucun point d'accès et constituant ainsi un réseau point à point (peer to peer en anglais), c'est-à-dire un réseau dans lequel chaque machine joue en même temps de rôle de client et le rôle de point d'accès.

Sur le plan sécurité, il est important de signaler, que ces réseaux sans fil présentent des spécificités physiques (ondes radio) et logiques sur les couches 1&2 du modèle ISO, mais rejoignent parfaitement les concepts pour les autres couches du modèle.

S'il est vrai que la sécurité n'est pas garantie pour une installation Wireless par défaut, il faut néanmoins noter que des mécanismes allant du plus simple jusqu'au plus complexe permettent de fournir le niveau de sécurité requis.

Parmi ceux-ci, il faut noter :
· La modification du SSID par défaut,
· L'utilisation du Wep (Wired Equivalent Privacy) qui permet de chiffrer les communications entre les AP(points d'accès) et les clients.
· 802.1x/EAP/Radius : amélioration de l'authentification des utilisateurs.
· Utilisation de VPN pour les clients sans fil, permettant d'isoler les WLAN du LAN comme Internet.

Principes de sécurité informatique

La sécurité informatique repose sur une adéquation entre la protection physique (accès) et logique (autorisation), et s'intègre à la sûreté de fonctionnement du système d'information global.

De nombreux facteurs entrent en jeu, mais il s'avère que la réussite d'une politique de sécurité passe par la mobilisation et l'adéquation des moyens matériels et organisationnels face à ce que l'on appelle le RMT (Risque Maximal Tolérable).

La tâche est particulièrement délicate, car nos systèmes informatiques confinés à nos espaces de travail, se sont ouverts et interconnectés à des services distants privés ou publics, pour créer de vastes communautés communicantes. Nos organisations, à fonction pyramidale dédiée, n'ont pas encore intégré que le système informatique s'est fondu dans un vaste système d'information intégrant des technologies différentes, (notamment informatiques & télécommunications) qu'il convient de connaître pour en assurer la maîtrise.

Intégrer aujourd'hui, dans une entreprise des téléphones portables, des réseaux sans fil, une imprimante auto maintenue par liaison IP, ou une machine outil pose le problème de la sûreté de fonctionnement de l'ensemble du système d'information.

Si cette fonction de sécurité, forcément transversale, exige une réflexion organisationnelle de l'entreprise sur les choix de son infra structure, la sécurité des données garantie par une info structure repose sur des concepts identifiés par l'ISO, regroupé sur quatre items D.C.I.P (Disponibilité, Confidentialité, Intégrité, Preuve) . Assurer la sécurité logique du SI (Système d'information) revient alors à prendre toutes les mesures de prévention et de précaution pour assurer un risque résiduel.

Les fonctions de sécurité réseau identifiées par l'ISO

Référence ISO TR 13335-1 :
• Confidentialité : Propriété qu'une information ne peut être accédée ou divulguée par des personnes, entités ou processus non autorisés.
• Intégrité des données : propriété qui garantit qu'une donnée ne peut être altérée ou détruite d'une façon non autorisée.
• Intégrité des systèmes : propriété qui garantit qu'il sera exécuté la fonction attendue de façon complète sans manipulation non autorisée volontaire ou accidentelle.
• Authentification : ce service permet de s'assurer de l'origine d'un message.
• Preuve ou non-répudiation (ou imputabilité) : ce service assure la preuve de l'authenticité d'un acte, d'une communication ou d'une transaction.
• Disponibilité : ce service permet d'assurer l'accessibilité des informations.

L'analyse des risques préalable, afin d'obtenir les RMT, détermine les solutions à mettre en œuvre, y compris les plans de secours ou de continuité de services. La responsabilité juridique de l'exploitant peut être rapidement engagée, car les systèmes d'information constituent de véritables actifs, et la sécurisation des données appartient en premier lieu à leurs dépositaires.

A ce stade, il est donc primordial de considérer que l'installation d'un réseau sans fil, peut constituer ou pas un risque pour le système global d'information. Les différents projets WiFi envisagés peuvent en effet avoir des objectifs de sécurité bien différents, qu'ils s'agissent d'une borne isolée d'information ou d'un terminal d'entrée/sortie d'une gestion logistique d'entrepôt reliée à l'ERP de l'entreprise.

Il devient alors possible dans ce cas, pour une personne malveillante, d'obtenir un login&password sur l'ordinateur central par un simple stationnement à proximité de l'entreprise. La sécurité, c'est avant tout la perception de l'existence du risque.

Ceci paraît évident, mais force de constater que de tels projets se développent sans une réflexion globale de sécurité car ils sont menés indépendamment du service informatique, répondant avant tout à des préoccupations d'exploitation. De même, les intégrateurs de tels services, n'intègrent pas toujours toutes les règles de l'art des possibilités de paramétrage de tels réseaux, qui installés par défaut ne présentent pas toujours la solution conforme au sens de la sécurité.

Menaces et vulnérabilités sur les réseaux sans fil

On peut distinguer trois classes de vulnérabilités :

· Liées aux normes :
Leurs spécificités physiques et logiques induisent des vulnérabilités propres qu'il convient de prendre en compte. L'onde radio est par nature captable.

· Liées aux produits :
Tout produit (matériel & logiciel) comporte des failles ou bugs. L'interopérabilité et la sophistication des solutions induisent implacablement des aléas de fonctionnement qu'il convient de suivre et de corriger.

· Liées à l'introduction de ces technologies dans les réseaux d'entreprise :
Tous ces îlots de technologies de communication qui s'intègrent et coopèrent, doivent l'être suivant une infra structure et une info structure (usage de l'information) puis une organisation conforme aux directives de sécurité énoncées.

L'optimisation du rayonnement des antennes, par exemple, dépend de nombreux paramètres bien éloignés des préoccupations des informaticiens. Nous sommes en présence d'un média de type «rayonnant», présentant des spécificités physiques propres. Tout élément placé dans le champ balayé par l'onde reçoit passivement le signal.

En intérieur, les ondes doivent affronter des «ennemis», qui s'opposent à leur propagation. Le plus redoutable reste le métal… S'y ajoute un problème spécifique au WiFi, dont la fréquence (2,4 Ghz) est très voisine de la fréquence de résonance de l'eau (et des fours à micro onde …). Tout élément constitué d'eau, végétaux ou êtres vivants, absorbe les ondes…

Le WiFi est très sensible au brouillage. Cette vulnérabilité est intrinsèque à toutes les techniques de réseaux sans fil, techniques qui se prêtent aux attaques ou destructions en déni de service sur les équipements de réseau.

Tout ordinateur équipé d'une carte 802.11 et d'un logiciel spécialisé disponible sur Internet, est capable d'écouter des transmissions de données dès qu'il se situe dans le périmètre du RLR (Réseau local radio). Il est alors possible de les falsifier ou de porter atteinte à la confidentialité ou à l'intégrité des échanges.

L'option de chiffrement proposée, le WEP (Wired Equivalent Privacy), ne remplit pas les garanties de sécurité attendues ; des outils libres ou gratuits sont à disposition sur Internet pour passer outre cette protection peu efficace.

Lorsqu'un point d'accès est installé sur le réseau local, il permet aux stations d'accéder au réseau filaire et éventuellement à Internet si le réseau local y est relié. Un réseau sans fil non sécurisé représente de cette façon un point d'entrée royal pour le pirate au réseau interne d'une entreprise ou une organisation.

Le système informatique est devenu rapidement le système d'information de l'entreprise, c'est à dire le système qui regroupe tous les moyens de communication de l'entreprise. Cette intégration s'est faite avant tout dans un objectif de réactivité et de compétitivité des entreprises. Or tout point d'entrée ou de sortie du système d'information peut présenter des failles de sécurité.

La notion de sûreté de fonctionnement, qui intègre les fonctions de qualité et de sécurité motive les entreprises à insérer dans tous les projets la composante sécurité.

L'insécurité informatique est souvent représentée par le pirate parfois même « bon enfant », or elle représente des sommes colossales de perte pour des sinistres comme :
· Virus informatiques
· Déni de service arrêts du système
· Perte, vol, altération d'information, usurpation d'identité...
· Ingérence économique, image de marque, nuisance...

C'est pour cela qu'il est important de garantir à un niveau suffisant :
· La disponibilité et la qualité de service face aux agressions en saturation.
· L'intégrité et la confidentialité des contenus face à des actes de malveillance.

Les audits de sécurité réalisés sur les systèmes d'information montrent que plus de 80% des problèmes viennent de failles non corrigées et appartiennent aux trois classes citées. La lutte contre la cyber criminalité est capitale, pour notre économie où le marché de la contrefaçon qui se nourrit de vols d'information a atteint 6% du commerce mondial.

Les méthodes de sécurisation d'un réseau sans fil

L'absence native de sécurité des WiFi, ne doit pas être un handicap à leurs nombreux avantages. D'ailleurs leur insécurité provient principalement de la non application de règles élémentaires de sécurité.

L'installation par «défaut» ou «méconnaissance» reste la principale cause d'insécurité. Sa nature technologique hybride «radio informatique» réclame des compétences diverses pour le déploiement de solutions éprouvées et conformes. Son attrait économique tente à banaliser les projets, trop rapidement menés.

Comme nous l'avons vu, l'installation d'un réseau WiFi, dès lors qu'il est rattaché à une informatique existante concoure à la sécurité globale du système. Si tel est le cas, son installation doit être conforme aux règles de sécurité informatique. Si ces règles prévoient que toute entrée sur le réseau local doit se faire par le firewall, alors le réseau WiFi devra se conformer aux règles générales prévues. Trop souvent, la sécurité est traitée à posteriori du projet. Elle coûte alors plus cher, et risque ne pas être adaptée.

Par nature, l'écoute passive est possible sur les réseaux WiFi, donc les couches basses sont fragiles à l'écoute, au brouillage, ou perturbation ; c'est donc par l'authentification et la protection des données que l'on pourra, si nécessaire, protéger les communications. Ces options sont actuellement proposées par la norme 802.11i.

Identifier le projet envisagé :

En milieu industriel, la perception du risque «matériel» est constante, car primordiale pour la qualité de production. Néanmoins, le risque «immatériel», comme le risque informatique est rarement perçu.

L'intégration des services informatiques à tous les niveaux de l'entreprise, se réalise par des îlots de technologie différente interconnectés. Chaque îlot contribue ou fragilise les règles globales de sécurité.

C'est ainsi, que l'on examinera le bien fondé des structures de sécurité WiFi à déployer, et que l'on décidera de sa connexion au reste du SI. Si l'entreprise est, par exemple, dotée d'un firewall garant des filtrages internes/externes, on peut décider alors de l'y connecter.

Notons, que tout projet qui touche à la sécurité du SI, doit être mené de façon transversale, et que la recette fonctionnelle d'un îlot d'automatisation doit intégrer une composante sécurité informatique.

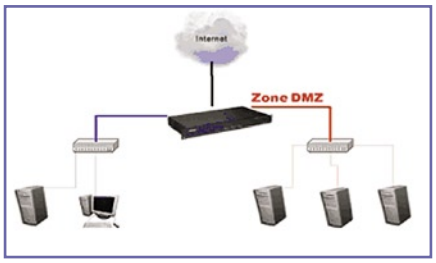
Si au contraire, le réseau WiFi est indépendant de toute autre connexion, c'est par une évaluation des risques sur sa disponibilité et éventuellement de sa confidentialité que les analyses devront être faites.

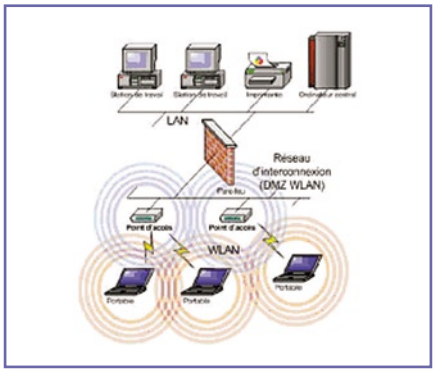
Adapter l'infrastructure :

Le SI d'une entreprise est aujourd'hui un vaste réseau public/privé qu'il convient de délimiter par des périmètres stricts de sécurité. Souvent au nombre de trois, que l'on repérera WAN (public) LAN (privé) et DMZ (zone démilitarisée d'échanges LAN/WAN), afin de veiller par un filtrage (firewall) l'étanchéité nécessaire entre les échanges LAN et WAN.

La mise en place d'un réseau sans fil consiste à positionner intelligemment les points d'accès selon la zone que l'on souhaite couvrir.

Rapidement les périmètres couverts peuvent être détectés et l'on peut ainsi s'assurer que les zones proches comme parking ou routes ne le sont pas. Le WiFi est une solution interne, souvent relié au réseau local de l'entreprise. Sa détection externe, peut être un risque important d'intrusion dans le réseau local de l'entreprise. De même l'accès





physique aux terminaux ou aux bornes peut être préjudiciable pour la configuration du WiFi mais aussi au réseau LAN sur lequel il peut être relié directement. En attendant que les règles de sécurité se durcissent, il faut veiller à ce que le WLAN puisse appartenir à la DMZ.

Les configurations par défaut :

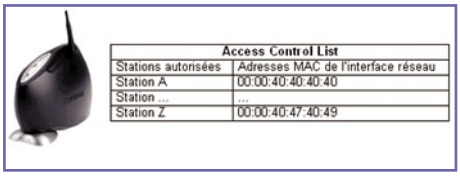
La première faille exploitée par le pirate est encore trop souvent la négligence de l'administrateur réseau de l'entreprise. En effet, la plupart des bornes WiFi sont livrées avec aucune sécurité activée par défaut, et sont installés tel quel. Il suffit alors de se connecter, et cela sans authentification (tout le monde peut se connecter) et sans chiffrement (tout le monde peut lire). Et tout ceci sans contrainte physique de devoir trouver une prise !!

La nature des projets WiFi en milieu industriel révèle que bien souvent les règles de sécurité existantes par défaut, n'ont pas été mises en oeuvre.

Lors de la première installation d'un point d'accès, celui-ci est configuré avec des valeurs par défaut, y compris en ce qui concerne le mot de passe de l'administrateur.

D'autre part, afin de se connecter à un point d'accès il est indispensable de connaître l'identifiant du réseau (SSID). Ainsi il est vivement conseillé de modifier le nom du réseau par défaut et de désactiver la diffusion (broadcast) de ce dernier sur le réseau. Le changement de l'identifiant réseau par défaut est d'autant plus important qu'il peut donner aux pirates des éléments d'information sur la marque ou le modèle du point d'accès utilisé.

Chaque adaptateur réseau possède une adresse physique qui lui est propre (appelée adresse MAC). Les points d'accès permettent généralement dans leur interface de configuration de gérer une liste de droits d'accès (appelée ACL) basée sur les adresses MAC des



Access Control List	
Stations autorisées	Adresses MAC de l'interface réseau
Station A	00:00:40:40:40:40
Station ...	...
Station Z	00:00:40:47:40:49

équipements autorisés à se connecter au réseau sans fil.

Cette précaution un peu contraignante permet de limiter l'accès au réseau à un certain nombre de machines. En outre cela ne résout pas le problème de la confidentialité des échanges.

Le WEP (Wired Equivalent Privacy) est un protocole chargé du chiffrement des trames 802.11 utilisant l'algorithme symétrique RC4 avec des clés d'une longueur de 64 ou 128 bits. La clé de session partagée par toutes les stations est statique, c'est-à-dire que pour déployer un grand nombre de stations WiFi il est nécessaire de les configurer en utilisant la même clé de session. Ainsi la connaissance de la clé est suffisante pour déchiffrer les communications.

De plus, 24 bits de la clé servent uniquement pour l'initialisation, ce qui signifie que seuls 40 bits de la clé de 64 bits servent réellement à chiffrer et 104 bits pour la clé de 128 bits.

Dans le cas de la clé de 40 bits, une attaque par force brute (c'est-à-dire en essayant toutes les possibilités de clés) peut très vite amener le pirate à trouver la clé de session. De plus une faille décelée par Fluhrer, Mantin et Shamir concernant la génération de la chaîne pseudo-aléatoire rend possible la découverte de la clé de session en stockant 100 Mo à 1 Go de trafic créés intentionnellement. Le WEP n'est donc pas suffisant pour garantir une réelle confidentialité des données. Pour autant, il est vivement conseillé de mettre au moins en œuvre une protection WEP 128 bits afin d'assurer un niveau de confidentialité minimum et d'éviter de cette façon 90% des risques d'intrusion.

Améliorer l'authentification :

La norme 802.11b ne permet pas l'authentification. Pour pallier cette lacune, la norme propose un protocole d'authentification modulaire EAP (Extensible Authentification Protocol). Utilisé conjointement avec le protocole TLS (Transport Layer Security) pour le transfert des communications d'authentification chiffrées. D'autres protocoles de transfert existent, et demandent une infrastructure de gestion de clés.

il est possible aussi de recourir à un serveur RADIUS (Remote Authentication Dial-In User Service). Le protocole RADIUS (défini par les RFC 2865 et 2866), est un système client/serveur permettant de gérer de façon centralisée les comptes des utilisateurs et les droits d'accès associés.

Pour toutes les communications nécessitant un haut niveau de sécurisation, il est préférable de recourir à un chiffrement fort des données en mettant en place un réseau privé virtuel (VPN).

S'appuyer sur une protection logique et organisationnelle :

Comme nous l'avons vu, la principale faille réside dans le fait que le projet WiFi, échappe lors de son installation à une réflexion sur la sécurisation du système d'information. L'intégration massive des moyens de communication autour des technologies Internet, et notamment Télécommunications&informatique, exige une organisation transversale pour la Sécurité des systèmes d'information.

Or, il reste bien souvent difficile de faire coopérer services généraux, services techniques et autres autour du même sujet, à savoir la sécurité des actifs qu'ils soient d'ailleurs humains, matériels ou immatériels … Le coût apparaîtra toujours dissuasif, mais pourtant les chefs d'entreprise reconnaissent aujourd'hui à plus de 68% être dépendants de leur système d'information…

Conseils pour le déploiement d'un WiFi en bonne sécurité :

Le bon sens …

o Prendre toutes les protections physiques sur les équipements qui disposent d'informations confidentielles sur le paramétrage te l'administration du réseau sans fil.
o Accéder physiquement à une borne permet d'atteindre le réseau local
o Vérifier le périmètre couvert par le réseau sans fil, et la qualité du signal.
o Configuration adaptée du réseau sans fil
- Modifiez le nom SSID par défaut et le modifier régulièrement
- Désactivez SSID Broadcasts (Diffusion du nom SSID)
- Modifiez le mot de passe par défaut du compte de l'administrateur.

Déclarer les postes autorisés…

- Activez MAC Address Filtering (Filtrage des adresses MAC).

Pour assurer confidentialité et intégrité

o Activez le cryptage WEP. (L'activation du WEP est un plus mais ralentit le débit d'information : temps de cryptage - décryptage).
o Modifiez les clés de cryptage WEP régulièrement, en attendant la solution WAP (WiFi protect Access) inclus dans la 802.11i (fin 2003) qui propose des clefs de cryptage plus longues et surtout, qui changent pour chaque paquet envoyé.

Pour que le WLAN soit séparé du réseau local

o Installez un firewall comme si le point d'accès était une connexion internet.
- Alors ce firewall pourra être le serveur ipsec (VPN) des clients sans fil.
- Possibilité de faire l'authentification grâce à un serveur LDAP (annuaire), Radius.

Le futur protocole IP ipv6 contient dans ses paquets la sécurisation ipsec. L'ipv6 peut être utilisé en wifi si les clients gèrent l'ipv6. Actuellement tous les Linux et Unix ont une pile ipv6 fonctionnelle. Sur windows 2000 et XP l'ipv6 est activable et utilisable mais sera proposé par défaut dans les prochaines versions.

Bien sûr, toutes les recommandations sont graduelles en fonction de la sensibilité du réseau sans fil. La tendance future apportera ces services au niveau des équipements, ce qui simplifiera les architectures mais rendra indispensables les bonnes configurations et leurs administrations régulières.

La sécurité d'un système reste un objectif, comme la qualité. C'est par une vigilance permanente que l'on maintient sa conformité. La prolifération des failles oblige à une veille et à des corrections rapides (patch correctif), au risque que cette vulnérabilité soit utilisée.

Il restera alors à travailler sur l'organisation, et notamment la politique de sécurité liée aux postes nomades. En ef-

fet, la sécurité physique et logique d'un système d'information repose sur des zones identifiables de protection.

Cette sécurité est mise en difficulté dès lors qu'un utilisateur mal intentionné, ou inconscient des risques, ajoute un point d'accès sur un réseau de son entreprise pour pouvoir bénéficier par exemple de la mobilité de son portable personnel.

Ce point d'accès représente en effet une porte ouverte sur le réseau entreprise depuis l'extérieur et ne passe par aucun pare feu ou dispositif de sécurité. Cette vulnérabilité est d'autant plus forte, que les nomades sont livrés de base avec tous les moyens de connexion y compris maintenant WiFi .

Il en est de même pour cet utilisateur qui travaille depuis son domicile, et qui dispose d'un accès sécurisé par un VPN, mais qui dispose chez lui d'un WiFi. Il risque alors de faire profiter son voisinage d'une connexion non protégé au réseau de l'entreprise.

Ces doubles attachements, non référencés, constituent une vulnérabilité forte pour la lutte antivirale, déni de service ou tentative d'intrusion, il convient de sensibiliser la totalité des utilisateurs et de surveiller en permanence les ajouts de matériels (apparition nouvelles adresses MAC). Il en est de même pour tous les équipements qui disposent d'une ligne dédiée pour la télémaintenance y compris celle du standard téléphonique…
Comme nous l'avons vu le pirate a une tendance lourde à être futé et paresseux, il cherchera toujours à briser la chaîne de sécurité par son endroit le plus faible.

La fonction de RSSI (Responsable Sécurité du système d'information) doit être une fonction reconnue et transversale dans l'entreprise et doit avoir pour objectif : **la garantie du Patrimoine informationnel de l'entreprise.**

Conclusion

La prolifération des connexions ou des postes nomades engendre des risques importants sur la qualité du SI. Tout dispositif atteignant le SI, doit être expertisé comme facteur de risque, car il participe à renforcer ou au contraire à affaiblir la sécurité globale. Il ne faut pas parler de "sur sécurisation", mais bien d'une cohérence de sécurité.

Les réseaux sans fil n'échappent pas à ce besoin de sécurité globale pour le système d'information de l'entreprise. Les solutions existent, mais ne sont pas mises en place. Suivant la nature du projet, on peut atteindre un niveau conforme de sécurité en commençant par initialiser les paramètres de configuration et la mise en place des solutions cryptées.

Ensuite, et c'est fondamental, toute connexion à risque d'intrusion externe devrait être filtrée et contrôlée (firewall) avant d'atteindre le réseau interne et local de l'entreprise.

Si la pertinence d'un système d'information est vitale pour l'entreprise, la sécurité n'est qu'un maillon de la sûreté de fonctionnement.
Assurer la disponibilité ou la restauration d'un service sont essentiels, mais la confidentialité et l'intégrité des données caractérisent immédiatement la qualité de ce service.

Aujourd'hui, surveiller, tracer et contrôler les informations est rendu nécessaires afin d'assurer la vigilance et la veille indispensables à un suivi de la sécurité.
On ne parle pas, ou peu, du risque d'usurpation d'identité préjudiciable à l'intégrité de la personne visée. Cette dimension humaine a son importance, car les règles de sécurité sont bien éditées, pour protéger les systèmes et leurs utilisateurs. Chacun se doit alors de comprendre et d'appliquer les règles.

Les nombreuses évolutions des technologies engendrent de nombreux correctifs à installer. C'est donc, par un suivi rigoureux et une organisation soucieuse de la sensibilisation de tous les acteurs que résident le comportement sécuritaire meilleur rempart à l'imprévisible.

Les WiFi avec leurs forces et faiblesses appartiennent à cet univers. Les avantages de ces technologies ne doivent pas être altérés par leurs éventuels défauts de sécurité. Les normes 802.11 sont récentes, et les travaux actuels apporteront les compléments indispensables notamment pour la sécurité des échanges. Pour l'heure, il faut être attentif au choix de matériels qui pourront profiter de l'apport de ces évolutions, et mettre en œuvre et dans les règles de l'art les dispositifs de sécurité proposés face aux risques identifiés.

L'intégration actuelle de nos moyens de communication fait appel à de nombreuses compétences d'électronique, de physique, d'informatique…, et bouleverse rapidement nos méthodes de travail. La sécurité doit s'inscrire dans le schéma de la qualité, car elle en est la composante indispensable. Une recette fonctionnelle n'est pas suffisante, c'est la notion d'audit sécurité qui est primordiale car elle permet de tester la solution en situation de menaces.

La technologie nous offre ce paradoxe : plus elle nous libère, plus nous devons apprendre à la maîtriser.

Jean-Marc CHARTRES
ingénieur CNAM
LEXSI

REFERENCES (sites institutionnels)

http:// www.ssi.gouv.fr/
http://www.art-telecom.fr/
http://www.cnil.fr/