



# CASES articles

Le Wifi : populaire, mais pas toujours sûr - les réseaux sans fil

## Les technologies sans fil et leurs risques

**Pour plus de sécurité, adoptez les réflexes CASES !**

### Les réseaux sans fil doivent faire l'objet de mesures de protection

**Dans les zones piétonnes, les aéroports et les gares, mais aussi à la maison – les points d'accès Wifi sont de plus en plus nombreux et les réseaux sans fil font désormais partie de notre quotidien. Ils permettent un accès aisé et sans fil à l'Internet. Ce qui semble bien pratique à première vue dissimule néanmoins certains risques : le vol de données ou l'exploitation de ces réseaux pour attaquer les ordinateurs d'autres utilisateurs en sont des exemples bien connus. Savoir comment fonctionne un réseau sans fil permet à son utilisateur de mieux comprendre les failles de sécurité potentielles et les mécanismes de protection qu'il convient d'adopter.**

Dans un réseau sans fil, les ordinateurs sont reliés entre eux sans câble de connexion. Sans perdre leur liaison avec l'Internet, les usagers sont ainsi en mesure de déplacer librement leur ordinateur, sans câble, dans un périmètre donné. La transmission des données est ainsi réalisée par liaison radio. De ce fait, les usagers peuvent aisément faire leurs achats sur Internet d'un simple clic de souris, lire les dernières nouvelles en ligne sur leur terrasse, ou s'informer des événements du week-end installés dans leur cuisine – le tout sans entraves.

C'est en l'an 2000 que les premiers ordinateurs ont été mis en réseau grâce à la technologie sans fil Wifi. Les ordinateurs ainsi reliés pouvaient se connecter librement et simultanément à l'Internet. Cette technologie fait aujourd'hui partie intégrante de notre quotidien. Outre les services proposés par les fournisseurs d'accès à Internet

aux utilisateurs privés, de plus en plus de villes et de communes offrent un libre accès à la toile depuis des endroits publics. Les cafés, restaurants, hôtels et autres boulangeries ont d'ailleurs également décidé de proposer ce service à leurs clients. La zone couverte permettant un accès à Internet dépend alors des fréquences radio et de la puissance utilisées, et peut être limitée à quelques mètres ou atteindre plusieurs dizaines de mètres.

La popularité croissante des réseaux sans fil repose essentiellement sur une installation simple et sur l'accès aisé et sans fil à l'Internet. En outre, lors de l'installation d'un réseau sans fil, peu, voire aucun câblage n'est nécessaire, (à l'exception de la station d'accueil). Il est ainsi par exemple possible de ne pas détériorer les bâtiments classés ou les logements loués.

Les réseaux sans fil ne sont toutefois pas sans inconvénients et leur utilisation peut engendrer certaines difficultés. Il est ainsi difficile, parfois même quasiment impossible, de contrôler la propagation du signal. Les ondes radio se propagent de façon rectiligne et sont réfléchies partiellement lorsqu'elles rencontrent un obstacle (en fonction du matériau et de la consistance de celui-ci). Cela a un effet direct sur le périmètre couvert : du béton armé, du carrelage ou du métal – comme une cage d'ascenseur par exemple – génèrent une importante atténuation du phénomène. Déterminer précisément le rayon d'action d'un réseau sans fil se révèle donc difficile. Or, la portée d'un réseau peut par exemple faciliter l'accès de tiers à celui-ci, et peut engendrer des problèmes de sécurité, tant pour l'exploitant du réseau que pour l'utilisateur. Il est également important de se conformer aux directives relatives aux transmissions radio, en particulier en rapport avec les effets que

peuvent avoir les ondes radio sur la santé.

#### Les types de réseaux sans fil

Diverses technologies ont été développées, adaptées à différentes portées et utilisations des réseaux sans fil. Quatre types principaux peuvent être distingués.

Les WPAN (wireless personal area network) comprennent tous les réseaux sans fil de faible portée. Ils sont destinés à relier quelques appareils entre eux ou à une unité centrale à connexion filaire. La distance entre les différents appareils est alors faible. Ces réseaux reposent par exemple sur la technologie Bluetooth ou sur le Wifi. Des applications populaires pour ce genre de réseau sont les micro-casques pour téléphone mobile ou encore les kits mains libres pour la voiture.

Si le périmètre couvert correspond à un réseau local d'entreprise, c'est-à-dire quelques centaines de mètres, l'on parle de WLAN (wireless local area network). Les appareils reliés par le biais de ce réseau sans fil se trouvent également dans une zone géographique restreinte. La principale technologie utilisée pour ces réseaux est également le Wifi.

Lorsque tout un quartier ou un campus universitaire est couvert par un réseau sans fil, l'on parle de WMAN (wireless metropolitan area network). Dans celui-ci, plusieurs réseaux câblés ou sans fil sont reliés entre eux. Un exemple pour ce genre d'infrastructure constitue l'offre d'accès sans fil à l'Internet de la Ville de Luxembourg. Si la zone couverte s'étend sur plusieurs kilomètres, l'on parle de WWAN (wireless wide area network), ou de réseau mobile cellulaire. Les principales technologies mises en œuvre dans ce cas sont GSM, GPRS et UMTS.

En raison de sa grande popularité, tant auprès des entreprises que des ménages privés, il convient tout particulièrement de bien comprendre la technologie Wifi et ses points faibles potentiels.

### **Comment fonctionne le Wifi ?**

Les appareils connectés à un réseau Wifi communiquent entre eux par le biais de signaux radio émis par des antennes. Chaque appareil doit donc disposer d'une antenne, laquelle est qualifiée de carte réseau.

Les appareils permettant l'accès au réseau Wifi sont appelés points d'accès (ou « access points »). Si plusieurs points d'accès sont disponibles, ceux-ci sont généralement reliés entre eux par câble.

Chaque ordinateur connecté à un point d'accès est qualifié de station dans la technologie Wifi. Le point d'accès et ses stations constituent un réseau : le Basic Service Set ou BSS. Afin d'identifier précisément le réseau, un numéro d'identification, appelé BSS ID, lui est attribué. Le BSS ID peut être comparé à un code postal : il permet d'identifier précisément chaque réseau. Lorsque plusieurs réseaux sont connectés pour en former un plus grand, celui-ci se voit également attribuer un numéro d'identification, dénommé ESS ID.

Un point d'accès à Internet transmet son numéro d'identification (BSS ID ou ESS ID) toutes les 0,1 seconde. Cela fonctionne pour ainsi dire comme un crieur : l'utilisateur allumant par exemple son ordinateur portable dans un café, reçoit tous les numéros d'identification des points d'accès se trouvant à portée. Il peut ensuite se connecter au réseau de son choix (dans la mesure où il dispose des droits d'accès). De nombreux réseaux ne disposant pas de dispositifs de protection, cette opération s'avère souvent très aisée.

### **Les risques des réseaux Wifi**

Les réseaux sans fil tels que Wifi n'ont besoin ni de portes, ni de fenêtres, mais les ondes émises heurtent des obstacles, tels que des piliers métalliques, des cages d'ascenseur, des meubles, des surfaces vitrées ou des murs. Ceci provoque des atténuations et des réflexions. En effet, lorsque le

point d'accès se trouve par exemple dans une cage d'escalier, il se peut que la connexion à Internet soit possible dans de très bonnes conditions dans le salon et dans le jardin et qu'elle soit impossible dans le bureau situé au deuxième étage. Si l'on augmente alors la puissance d'émission, il se peut que la réception dans le bureau reste mauvaise alors que les cinq maisons voisines pourront accéder au réseau (dans la mesure où celui-ci n'est pas protégé). Le vol de données ou l'utilisation abusive du réseau sont ensuite possibles. Il faut également tenir compte de certains aspects liés à la santé ; à cet égard, il est recommandé de maintenir la puissance d'émission d'un réseau sans fil la plus faible possible.

La technologie Wifi repose sur l'utilisation d'ondes radio, or, celles-ci sont très sensibles aux perturbations. Il est ainsi assez simple d'interrompre la liaison : mettre en marche son four à micro-ondes peut suffire. La technologie Wifi et les procédés d'enregistrement qu'elle utilise au niveau des points d'accès sont très simples. La transmission de données spécifiques peut permettre aux pirates d'interrompre la liaison entre les différentes stations.

Il est de plus très difficile de calculer précisément la zone de propagation du signal. Si celle-ci est trop étendue, les pirates peuvent facilement obtenir l'accès à un réseau s'il n'est pas protégé, et le vol de données sensibles devient possible. Les entreprises ainsi que les personnes privées, ne sont pas toujours conscientes de la valeur des informations qui peuvent être interceptées sur un réseau Wifi.

Si une entreprise ou une organisation propose un point d'accès Wifi à ses clients, celui-ci peut également faire l'objet d'une utilisation abusive. Si ces entités omettent par exemple de stipuler clairement le nom du point d'accès Wifi à leurs clients, des pirates peuvent en aménager un second à proximité et lui donner un nom ressemblant. Les clients ainsi bernés se connectent à Internet par le biais du point d'accès contrôlé par le pirate ; ce dernier est ensuite en mesure d'obtenir l'accès à leurs ordinateurs.

Si le point d'accès se trouve à portée de main, les pirates n'auront également aucun mal à l'utiliser à leurs fins : ils pourront réinitialiser le point d'accès en question et le reconfigurer selon

leurs besoins. Les clients se connectant à l'Internet par le biais de ce point d'accès Wifi modifié deviennent les victimes des pirates.

Certains collaborateurs procèdent également à l'installation de points d'accès non autorisés à l'Internet sur le réseau de leur entreprise. Leur but est alors d'instaurer une meilleure mobilité entre les différents bureaux. Ces personnes oublient que l'entreprise cesse ainsi d'être protégée contre les accès de personnes étrangères, le pare-feu étant en effet contourné. La connexion de réseaux Wifi non protégés avec le réseau principal est également possible dans les hôpitaux. Les données très sensibles des patients sont ainsi librement accessibles pour les pirates.

Les grands magasins qui disposent des caisses dans les zones d'entrée de leur bâtiment les relient parfois à leur système informatique par le biais d'un réseau sans fil. Si celui-ci n'est pas protégé, des personnes étrangères peuvent obtenir les données de transaction des paiements effectués par carte bancaire.

Il est à noter que dès qu'un réseau Wifi non protégé est connecté à un réseau câblé, les pirates peuvent obtenir l'accès aux ordinateurs reliés à ce réseau câblé.

Les médias parlent souvent de « war-driving ». Ce terme qualifie l'action de rechercher des réseaux sans fil au volant de sa voiture et à l'aide d'un ordinateur portable. Des logiciels spécifiques, disponibles gratuitement sur Internet, permettent en effet la détection et la localisation géographique de tels réseaux. Les pirates ont même développé un code permettant de signaler les réseaux non protégés à l'aide de signes appliqués à la craie sur les trottoirs. Mais l'accès à un réseau Wifi étranger, même non protégé, est prohibé et passible de poursuites, conformément à l'article 509 du Code pénal luxembourgeois.

De nombreux utilisateurs privés ignorent que leur point d'accès est également accessible pour d'autres personnes. Ce ne sont d'ailleurs pas seulement les cybercriminels qui profitent de ces réseaux— des hommes d'affaires les utilisent par exemple pour consulter leurs e-mails. Si le propriétaire du réseau est soumis à un contrat fixant des limites de temps ou de volume, cette utilisation frauduleuse

se peut occasionner des pertes financières. Les conséquences sont encore plus graves lorsque le point d'accès est exploité pour des actes criminels, comme la transmission de contenus pornographiques à caractère pédophile par un tiers ou l'utilisation du point d'accès par le voisin pour fabriquer des copies pirates. Dans ce cas, les services de police ne disposent que de l'adresse du réseau non protégé, et il sera très délicat pour la victime de prouver son innocence. La technologie Wifi rend très difficile, voire impossible, l'identification du responsable des préjudices et chaque utilisateur peut, de plus, être tenu pour responsable en cas de préjudice.

Or, la possession d'un réseau non protégé peut être considérée comme une négligence : ceci peut, en effet, être comparé à laisser la clé d'un véhicule sur le démarreur.

#### **Conseils de sécurité :**

Les entreprises installées au Luxembourg peuvent obtenir le label « Wifi sécurisé suivant les réflexes CASES ». Ce label est valable pour une durée maximale de deux ans. À cette fin, CASES a défini une série d'exigences minimales devant être appliquées aux réseaux Wifi dans le domaine de la sécurité de l'information et des communications. Ce label peut être demandé gratuitement sur simple justification du respect desdites exigences minimales. Les entreprises peuvent également intégrer les exigences relatives à l'assurance qualité à leur cahier des charges. Les utilisateurs déclarent que les zones bénéficiant de ce label respectent les mesures de protection élémentaires de la sécurité de l'information. De plus amples informations relatives au label « Wifi sécurisé suivant les réflexes CASES » peuvent être obtenues à l'adresse e-mail suivante : [label@cases.lu](mailto:label@cases.lu).

La puissance des réseaux Wifi devrait toujours être adaptée à la portée requise. Les entreprises devraient procéder à un contrôle permanent des réseaux afin de détecter les éventuelles intrusions de cybercriminels. Le contrôle des réseaux Wifi est une tâche ardue, et ces réseaux – tout comme l'internet – devraient être traités avec vigilance. Les réseaux sans fil devraient être installés au même niveau que l'accès à internet, donc à l'extérieur des dispositifs de protection usuels. Toutes les données doivent ainsi passer le pare-feu et le logiciel anti-virus correspondant.

Les réglages standards des appareils devraient également être modifiés. Il s'agit en particulier de modifier le mot de passe du point d'accès et le nom du réseau, et donc également les BSS ID ou ESS ID. La diffusion automatique du nom du réseau devrait de plus être désactivée. Toutes les données transmises par le biais du réseau devraient être chiffrées à l'aide d'un procédé de chiffrement spécifique, dénommé technologie WPA.

En 2004, CASES a testé les stations d'accès (ou routeurs) disponibles sur le marché luxembourgeois afin d'évaluer leurs points faibles. Ces produits sont toujours en vente en 2008 et les résultats de ces tests peuvent être consultés sur le site <http://www.cases.public.lu/fr/publications/dossiers/dsl>.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

[www.cases.lu](http://www.cases.lu)