L'internet des objets, la grande attraction du MWC 2017

● L'internet des objets (IoT) a été la grande attraction technologique du dernier Mobile World Congress (MWC 2017). De l'enseignement à l'automatisation industrielle, en passant par l'énergie, les transports et la signalétique numérique, aucun secteur n'est épargné. Réunis autour de l'«IoT Cybersecurity Alliance», six grandes entreprises IT explorent déjà les problèmes de sécurité de ce secteur.

PAGE 12

Condor dévoile sa stratégie Android au MWC 2017

● Le président du conseil d'administration de Condor Electronics, M. Abderrahmane Benhamadi a annoncé lors du Mobile World Congress 2017 (MWC) qui s'est tenu à Barcelone du 27 février au 2 mars, un partenariat avec Google pour fournir le service de la nouvelle génération des services de la messagerie SMS baptisée Android Message.

PAGE 12

Quand l'Algérie porte l'ambition de vendre de la bande passante pas chère en Afrique

PAGE 13

● L'Algérie s'est résolument tournée vers l'Afrique en matière de développement des télécommunications, après l'installation en février dernier du Comité de liaison de la dorsale transsaharienne à fibre optique (CLDT). Mais pour revendre de la bande passante internationale, l'Algérie doit renforcer ses capacités à l'international.

L'accès au monde de la data, quelle sécurité pour demain ?

Par Farid Farah

Cela fait plus d'un demi-siècle que le premier message électronique a été envoyé via l'Arpanet, le réseau pionnier de l'Internet d'aujourd'hui. A cette époque, le besoin de surveiller une activité suspecte était quasiment nul. La confiance régnait dans l'environnement du Net, et aucune inquiétude concernant le piratage des données, n'était visible sur la toile. Cependant, au cours de cette période, les nouvelles technologies ont envahi peu à peu le Net pour le transformer en une véritable machine de l'économie numérique. Ainsi, l'intégralité des données stockées dans les ordinateurs des internautes est convoitée par des hackers et les structures gouvernementales de la sécurité numérique.

Ce flux data devient intéressant pour l'ensemble des acteurs de l'économie réelle comme les agences de marketing et les sociétés spécialisées dans la publicité digitale, ainsi que les agences de renseignement qui s'intéressent au sujet de l'espionnage de masse des populations du monde entier. Les spécialistes de la sécurité numérique recensent une moyenne de 30 vulnérabilités par terminal connecté. Ces vulnérabilités concernent des aspects liés à la collecte des données de consommation telles que nom, adresse électronique, adresse du domicile, date de naissance et informations d'identification des cartes de crédit et de santé.

Ces failles sécuritaires sont également aggravées par le manque de chiffrement dans le transport des données sur la toile. Plus de la moitié des terminaux n'utilisent pas le cryptage lors du téléchargement des mises à jour logicielles et aucune précaution n'est relevée pour éviter une interception massive des données par les pirates informatiques. C'est pourquoi, l'intervention humaine dans la surveillance de l'Internet commence à montrer ses limites. Des voix d'experts proposent l'alternative de la machine intelligente pour effectuer cette épineuse tâche. Les ordinateurs sont beaucoup plus rapides et les logiciels sont de plus en plus performants. Migrer vers la sécurisation numérique par une automatisation du procédé peut s'avérer plus efficace. Automatiser la sécurité du Net est un domaine à expertiser dans les plus brefs délais. A l'avenir, tout internaute aura sa clé de chiffrement automatisée, la manière de l'utilisation de son terminal est dictée par un logiciel automate et même le développement d'applications risque d'être encadré par un automate.

F. F.