Télégrammes : Pentagone et cyber-attaques, Wifi calling et 5G chez Ericsson, IBM décèle le Shadow Cloud, Chères Attaques DDoS

Le Pentagone veut automatiser les réponses aux cyber-attaques. En début d'année, un rapport mettait en évidence *« d'importantes vulnérabilités »* informatique qui touchaient les systèmes de défense américains. Et poussait le Pentagone dans un vaste projet pour corriger le tir. Si l'idée de départ était d'identifier les faiblesses des armes et réseaux informatiques du pays, le Pentagone veut aujourd'hui aller plus loin, rapporte nos confrères de *ZDNet*. Notamment en étudiant la façon dont les données évoluent entre les différentes branches de l'armée. D'autre part, si le travail de détection de failles et de correction est aujourd'hui manuel, le centre de défense entend développer, à terme, un système de réponse entièrement automatisé aux cyber-attaques. Le programme prévoit également la création de 133 équipes de cyber intervention (dont la moitié aurait déjà été créée) dans lesquelles travailleront 6 200 experts. Le tout devant être opérationnel pour fin 2016.

5G européenne et Wifi calling chez Ericsson. Ericsson élargit son offre de Wifi calling à tous les terminaux Wifi et non plus seulement aux smartphones. Le Wifi calling permet de passer des appels voix depuis un réseau Wifi ce qui peut s'avérer particulièrement utile lorsque le signal cellulaire est trop faible pour assurer une communication de qualité, dans les bâtiments par exemple ou bien depuis un pays étranger. Il ouvre également le service voix aux appareils qui ne sont pas dotés de l'application adéquate, comme c'est le cas de la plupart des tablettes. Le Wifi Calling pourrait bien figurer comme une fonction de base que gérera la 5G à l'horizon 2020. Ericsson y travaille, comme sur bien d'autres technologies, avec un parterre de partenaires locaux que l'équipementier suédois vient d'étendre au reste de l'Europe. Son programme « 5G for Europe » entend intégrer de grands secteurs verticaux dans les développements des technologies 5G auxquels participeront plusieurs universités en Italie, Allemagne, Espagne et en Angleterre. L'automobile, les transports, l'Internet des objets (IoT), les services publics et de santé, la sécurité ou encore le commerce sont concernés. *« En élargissant notre programme 5G pour inclure les principaux partenaires à travers l'Europe, nous allons acquérir de précieuses connaissances qui permettront aux industries d'assurer facilement leur transformation digitale, de créer une nouvelle valeur et de renforcer la position concurrentielle de l'industrie européenne »*, a déclaré Ulf Ewaldsson, responsable technologique en chef d'Ericsson.

IBM contre le shadow IT. La firme américaine a présenté la solution Cloud Security Enforcer qui a pour vocation de débusquer les applications Cloud non autorisés au sein des entreprises. Le phénomène de shadow Cloud est souvent perçu comme un risque de fuites des données sensibles. D'autres sociétés fournissent des solutions similaires pour détecter l'utilisation des applications Cloud personnelles au sein des entreprises. Gartner a même défini une catégorie pour ce type de logiciel, « Cloud Access Security Brokers ». IBM souligne que son service va au-delà de la simple

découverte de ce type d'applications, pour aller jusqu'à la sécurisation des accès.

Les attaques DDoS masquent des intrusions plus sérieuses. Tel est l'enseignement d'une étude réalisée par Kaspersky. 74% des entreprises ayant subi des attaques par déni de service ont également remarqué une perturbation d'autres services. L'enquête montre que les infections par malwares sont le principal effet secondaire (45% des sondés) des attaques DDOS. 32% évoquent des intrusions expérimentées sur le réseau ou d'autres types de piratage. La durée des attaques est variable et elles ont aussi un coût. En moyenne, les grandes entreprises ont perdu environ 417 000 $ (365 000 €) par attaque, tandis que les petites et moyennes entreprises ont perdu 53 000 dollars (46 400 euros)

Crédit Photo : Juefraphoto-Shutterstock