WebTimeMedias riviera

Avis d'Expert (Fortinet) : assurer la sécurité des villes intelligentes

Publié le 8 April, 2016 - 08:24 par Rédaction - Vu 1452 fois

Nice comme Barcelone, New York, Londres, Singapour se sont engagées dans le développement de "villes intelligentes" à travers les technologies de l'Internet des Objets et de l'analyse des données. Ce qui va créer aussi de nouvelles et redoutables vulnérabilités en matière de sécurité. L'avis d'expert de Christophe Auberger, Directeur Technique France de Fortinet à Sophia (leader mondial de la sécurité réseaux).

"Grâce aux données des capteurs installés sur les routes et véhicules, les systèmes de navigation embarqués dans les voitures peuvent signaler les embouteillages, leurs durées; les caméras repèrent les déchets dans les lieux publics et demandent l'intervention d'équipes de nettoyage ; les lampadaires de rue s'autorèglent...Voilà quelques-uns des scénarios qui pourraient se généraliser avec le développement des villes intelligentes au cours des prochaines années.

Poussées par une urbanisation croissante et alimentées par des technologies telles que l'Internet des objets (IoT) et l'analyse des données, les villes intelligentes sont sur le point de connaître une croissance exponentielle. Glasgow, Barcelone, Nice, New York, Londres et Singapour sont déjà engagées dans cette voie. D'après Navigant Research, le marché des technologies des villes intelligentes pourrait représenter 27,5 milliards de dollars annuels en 2023.

Le secteur public est souvent à l'origine des initiatives de villes intelligentes. Cependant, celles-ci vont avoir un fort impact sur les entreprises. Les DSI vont devoir apprendre à exploiter les nouvelles infrastructures connectées de leur ville pour leurs activités. Les technologies des villes intelligentes, telles que l'IoT et les analyses des données vont sans doute donner lieu à des idées commerciales innovantes dans le futur.

Mais la nouvelle vague de services et de technologies des villes intelligentes va probablement aussi créer de nouvelles vulnérabilités en matière de sécurité. Voici les CINQ zones à surveiller par les DSI.

1. Davantage de fragmentation de l'IT

Ces dernières années, nous avons assisté à une prolifération rapide des services cloud et à l'adoption des appareils mobiles au travail. Cette tendance a bouleversé la productivité de l'entreprise. Mais elle a également mis à mal le contrôle très rigoureux exercé jusqu'alors par les DSI sur leurs systèmes informatiques.

Les DSI doivent désormais se faire à l'idée que les employés peuvent utiliser des services cloud non autorisés, via des téléphones non sécurisés, pour accéder aux serveurs de l'entreprise et aux données sensibles de l'entreprise. L'explosion attendue des appareils IoT — les chercheurs estiment qu'en 2020, le nombre d'appareils actifs connectés sans fil sera de plus de 40 milliards dans le monde — entraînera davantage de fragmentation de l'IT dans l'entreprise.

Au lieu de s'engager dans une bataille perdue d'avance, les DSI doivent veiller à protéger les données. Ils doivent rechercher des appareils IoT capables d'offrir un chiffrement d'appareil à appareil ; envisager de mettre en place — et de renforcer — des systèmes de chiffrement complets afin de protéger les données stockées dans les réseaux, services cloud et terminaux.

2. Vulnérabilités des appareils

L'année dernière, des chercheurs en matière de sécurité ont trouvé des failles situées dans les poupées Barbie connectées en Wi-Fi, les voitures Jeep Cherokee, les dispositifs de suivi d'activités physiques et autres appareils connectés dernier cri. FortiGuard Labs de Fortinet constate déjà des attaques ciblant les appareils IoT à travers le monde. Cela montre les risques inhérents au fait de connecter des jouets, dispositifs wearables, voitures et réseaux électriques à des capteurs reliés à un réseau commun et au Web.

L'Internet des objets (IoT) va démultiplier les surfaces soumises aux attaques. Les pirates vont utiliser les appareils IoT comme tremplin pour des attaques de grande ampleur. Par exemple, les pirates profitent des vulnérabilités des appareils connectés grand public pour pénétrer dans les réseaux des entreprises et les matériels auxquels ils se connectent.

Alors, comment les DSI peuvent-ils se protéger contre les risques des appareils connectés ? À défaut de pouvoir séparer physiquement ces appareils de tous les autres systèmes du réseau, ils peuvent envisager de déployer des systèmes de protection réseau. Les pare-feux de segmentation interne (ISFW), par exemple, peuvent limiter la prolifération des menaces à l'intérieur du réseau de l'entreprise. Ils doivent également employer une solution de sécurité réseau pour l'IoT capable de limiter l'exploitation de cette surface d'attaque croissante et vulnérable.

Les fournisseurs d'IoT doivent renforcer leurs produits et avoir une équipe d'intervention en cas d'incidents relatif à la sécuritté des produits (Product Security Incident Response Team, PSIRT).

3. Les passerelles IoT peuvent être exploitées

Dans un déploiement IoT typique, la majorité des appareils sont et seront connectés en permanence. Contrairement aux téléphones mobiles et aux ordinateurs portables, ces appareils bénéficient d'une authentification unique pour des multiples sessions. Cela les rend particulièrement attractifs aux yeux des pirates souhaitant s'infiltrer dans les réseaux d'entreprise. Le renforcement de la sécurité des passerelles qui connectent les appareils IoT est donc indispensable. Les DSI doivent cartographier la localisation et les liaisons de ces passerelles — qui peuvent se trouver en interne ou en externe, et même être connectées aux fabricants des appareils IoT. Un solide plan de mises à jour avec des correctifs de sécurité doit également être établi sur ces passerelles comme sur les appareils IoT.

4. Big data, plus de risques

L'une des constantes dans le déploiement des villes intelligentes est que cela va générer plus de données, qu'il faudra traiter et stocker. Les dispositifs connectés vont générer d'énormes répertoires de données. Les entreprises qui adoptent le big data assisteront à un déluge encore plus impressionnant de données. Malheureusement, ces données constitueront également des cibles attractives pour les pirates. Pour protéger ces quantités de données associées à d'importants flux en entrée comme en sortie, les capacités en bande passante des dispositifs de sécurité seront primordiales. Et en matière d'analyse des données, il ne s'agira plus de traiter une simple série de données, mais de multiples répertoires de données qui devront pouvoir être combinés et analysés ensemble par différents groupes de personnes. Par exemple, les recherches d'un laboratoire pharmaceutique devront être accessibles aux employés, aux sous-traitants et aux stagiaires. Cela implique autant de droits d'accès et d'audit individuels.

5. Une nouvelle boîte de Pandore

De nouveaux vers, conçus pour les appareils IoT vont émerger — et ils pourraient faire encore plus de ravages étant donné la portée étendue des nouveaux réseaux convergents. Conficker est un exemple de ver qui s'est répandu sur les PC en 2008 et dont la présence persiste toujours en 2016. De la même manière, on peut s'attendre à ce qu'apparaissent des vers et virus capables de se propager d'appareil en appareil — notamment avec les appareils mobiles et le système d'exploitation Android. Les vers se répandront en exploitant les vulnérabilités d'une surface d'attaque mobile et IoT croissante. Le plus grand botnet constaté par FortiGuard Labs a atteint environ 15 millions de PC. Grâce à l'Internet des objets, celà pourrait facilement en atteindre plus de 50 millions si la propagation des vers sur IoT n'est pas correctement limitée. La gestion des correctifs et les inspections de sécurité basées sur les réseaux — notamment, les systèmes de prévention d'intrusion (IPS) — capables de bloquer les vers sur IoT sont incontournables."

Christophe Auberger