***Les rÃ©seaux virtualisÃ©s, meilleure rÃ©ponse aux problÃ©matiques de sÃ©curitÃ©â¦!***

**Internet**

PostÃ© par : JPilo
PubliÃ©e le : 22/5/2014 13:00:00

Devant la multiplicitÃ© des types dâattaques â de plus en plus difficilement dÃ©tectables avec les attaques Ã  signature faible -, devant les scandales qui ont Ã©mergÃ© ces derniÃ¨res semaines comme le montre la faille gÃ©nÃ©ralisÃ©e Â« Heartbleed Â» ou Â« les rÃ©vÃ©lations de lâaffaire Snowden Â», notre Ã©tude globale sur la sÃ©curitÃ© informatique dans le monde (Global Threat Intelligence Report â GTIR, page 52) fournit quelques conseils.

JÃ©rÃ´me Totel â Directeur technique â NTT Communications, France, nous explique :

-Mettre en place les normes ISO 27001 et PCI/DSS et impliquer tous les collaborateurs,
-ConnaÃ®tre en permanence tous ses actifs informatiques,

-Mettre en place un systÃ¨me de surveillance et dâanalyse de la sÃ©curitÃ© de son informatique rÃ©actif, en quasi-temps-rÃ©el : on favorisera lâutilisation dâune plateforme SIEM (Security Information and Event Management) basÃ©e sur un moteur de corrÃ©lations dâÃ©vÃ©nements comme SPLUNK.

Mais, je pense que la refonte des rÃ©seaux mondiaux qui sâamorce sous le nouveau paradigme oÃ¹ le logiciel dÃ©finit lâensemble du monde IT (SDE : Â« Software Defined Everything Â» ) va faire Ã©merger de nouvelles stratÃ©gies de dÃ©fense.

Les rÃ©seaux virtualisÃ©s vont permettre une avancÃ©e significative dans la sÃ©curitÃ©. Â« Software Defined Everything Â» se dÃ©cline dans le monde des rÃ©seaux par Â« Software Defined Network Â» ou SDN.

Des groupes de travail divers tels que I2RS (Â« Interface to the Routing System Â» : Interface avec le systÃ¨me de routage), IRTF (Internet Research Task Force) travaillent sur la standardisation du modÃ¨le SDN .

Il existe aussi des organisations comme EWSDN (European Workshop on SDN), lâETSI (European Telecommunications Standard Institute) ou encore NFV WG (Network Function Virtualization WorkGroup) qui se focalisent sur les services et les fonctions que peuvent porter les rÃ©seaux Â« logiciels Â» avec comme acronyme NFV (Network Function Virtualization).

Il y a donc de nombreux efforts de normalisation en cours. Lâ□□ONF (Open Networking Foundation) se concentre sur la normalisation du protocole OpenFlow, protocole qui vise Ã  contrÃ´ler les Ã©lÃ©ments du rÃ©seau en charge du transport de donnÃ©es Ã  partir dâ□□un serveur distant.

Des efforts similaires sont rÃ©alisÃ©s par l'IETF (Internet Engineering Task Force). Ils sâ□□efforcent de standardiser les interfaces programmables (ou API : Application Programming Interface) que lâ□□on trouvera dans les Ã©quipements rÃ©seaux.

Or, il y a tant de travaux de recherche, quâ□□il est difficile de suivre tout ce quâ□□il se passe. Mettre en lumiÃ¨re les trois moteurs de cette innovation nous permettra de mieux comprendre le paysage :

-PremiÃ¨rement, les opÃ©rateurs de rÃ©seaux et de services informatiques, sous la pression de la concurrence, veulent des infrastructures suffisamment souples pour pouvoir sortir rapidement de nouveaux services, de nouvelles fonctionnalitÃ©s. Or, prendre un an Ã  deux ans pour concevoir un nouveau service et le lancer commercialement est trop long.

-DeuxiÃ¨mement, les clients veulent des services sur-mesure, tout en bÃ©nÃ©ficiant dâ□□un prix moindre, en gardant une indÃ©pendance vis-Ã -vis du fournisseur de services choisi et en ayant la main sur la gestion des changements. En effet, au travers dâ□□un portail, les clients seront capables de provisionner eux-mÃªmes de nouveaux services (circuits VPN, firewalls et leurs rÃ¨gles, priorisation des fluxâ□¦etc..). Lâ□□objectif Ã©tant de permettre aux clients un gain de temps et donc dâ□□argent.

-TroisiÃ¨mement, si les opÃ©rateurs travaillent ensemble sur OpenFlow par exemple, câ□□est pour mieux crÃ©er lâ□□Ã©mulation entre les constructeurs de matÃ©riels IT et pour sâ□□affranchir de certaines positions monopolistiques. GrÃ¢ce Ã  ces modÃ¨les ouverts, il sera plus facile, pour un client, de migrer d'un fournisseur de services Ã  un autre.

Aujourdâ□□hui, ces travaux ont dÃ©jÃ  produit de nouveaux services. Un exemple est lâ□□automatisation des passerelles dâ□□accÃ¨s (Access Point Gateway Automation) entre les rÃ©seaux et le cloud. Ce projet consiste Ã  automatiser les connexions des rÃ©seaux privÃ©s aux data centers.

Le logiciel ici est encore le roi et lâ□□acronyme en vigueur est le SDDC comme Â« Software Defined Data Center Â» pour aider Ã  gÃ©rer le data center (pour en finir peut-Ãªtre avec les cross-connects).

Un autre exemple est de remplacer les Â« appliances Â» - de sÃ©curitÃ©, de gestion dâ□□optimisation des flux..etc.. - par des services dÃ©matÃ©rialisÃ©s fonctionnant sur des clouds privÃ©s virtuels directement connectÃ©s aux rÃ©seaux privÃ©s des entreprises. Plus besoin de ces installations fastidieuses dâ□□appliances.

Lâ□□interconnexion avec des services dÃ©matÃ©rialisÃ©s dans le cloud en connexion directe avec ses infrastructures donnera aux clients un accÃ¨s Ã  de trÃ¨s nombreux services : câ□□est ce nouveau modÃ¨le que nous proposerons bientÃ´t grÃ¢ce Ã  lâ□□intÃ©gration des services de Virtela.

Ceci permettra au rÃ©seau dâ□□aller Ã  la mÃªme vitesse que le Cloud en termes de dÃ©lais de livraison et dâ□□adaptation.

Cela nous donnera aussi la possibilitÃ© de dÃ©velopper de nouveaux services innovants et uniques sur le marchÃ©. Les rÃ©seaux peuvent dÃ©sormais Ãªtre paramÃ©trÃ©s par des applications comme des ressources logiques.

Enfin, concernant la sÃ©curitÃ©, SDN sous-entend la programmation et lâ□□orchestration de la couche Â« control plane Â» afin de faciliter les opÃ©rations.

Nous pourrons alors modifier le comportement des rÃ¨gles au sein mÃªme de la couche Â« Data Plane Â» et dans le cas de failles du type Â« heartbleed Â» / Open SSL, nous faciliterons le rejet des requÃªtes offensives ce qui empÃªchera en cÅ□ur de rÃ©seaux de dÃ©voiler des informations confidentielles des clients.