Réseau - Sécurité - Métrologie - Data Center

IPenergy Fédérateur de la convergence IP

Energy News

1er trimestre 2013

Edito

Dans le précédent Energy News de janvier, nous avons donné un aperçu de l'évolution des technologies Réseau, avec des architectures à 2 niveaux plus simples et plus fiables qui sont les premiers éléments de modifications encore plus structurelles de la conception des réseaux LAN autour de SDN et d'OpenFlow.

Nous allons aborder dans ce numéro certains aspects du périmètre Sécurité dont l'évolution est tout aussi marquante, avec des solutions qui permettent de mieux prendre en compte les nouveaux risques et de tester et patcher la vulnérabilité de son S.I.

Le premier thème abordé concerne les firewalls multi-fonctions (UTM) de nouvelle génération, pour lesquels, lors des analyses techniques et commerciales que nous faisons régulièrement, nous avons décidé d'introduire l'offre UTM de Sophos. Suite au rachat il y a environ 1 an du leader allemand des firewalls, Astaro, Sophos a intégré à son offre des firewalls multi-fonctions présentant un niveau technique et fonctionnel que nous avons jugé très élevé, doublé d'une interface utilisateur simple et instinctive et d'outils de pilotage permettant une vraie gestion centralisée des différentes briques de sécurité, avec la possibilité d'une intégration avancée avec les briques historiques de l'éditeur (anti-virus, protection des mobiles...).

Pour le second thème, nous vous présentons les évolutions de l'offre d'un de nos partenaires historiques, DenyAll, qui a interfacé son offre d'outils de test de vulnérabilités acquis il y a un an avec ses firewalls applicatifs qui protègent les applications Web. Le couplage de ces outils permet d'appliquer directement les filtrages adaptés sur les flux Web dès qu'une vulnérabilité a été détectée.

Le coin des infos: Agenda

Université Prospectives et Technologies:

Comment maîtriser les réseaux de nouvelles générations ? Exploitation et performance.

Comment définir votre protection péri-métrique et gérer vos vulnérabilités applicatives?

IPenergy, DenyAll, HP et Sophos vous apporte les réponses lors de deux journées à Aix en Provence et Sophia Antipolis

INSCRIPTION

22 mai 2013 à Aix en Provence
Mas d'Entremont

23 mai 2013 à Sophia Antipolis
Terrasses de Sophia

CoTer Club
LES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION AU SERVICE DES COLLECTIVITES LOCALES

4 et 5 juin 2013 à Saint-Etienne

CoTer Club Saint Etienne

Pour la troisième année consécutive, IPenergy participera au salon dédié aux collectivités territoriales.

Rendez vous le 4 et 5 juin 2013 au Centre des Congrès de Saint Etienne sur le stand P9 où vous pourrez retrouver IPenergy et Modul'Data Center.

En savoir plus

Le coin des technos

Sophos : le leader du marché allemand des UTM débarque en France avec des arguments forts !

- Sécurité de la messagerie, pare-feu, prévention des intrusions et contrôle du Web intégrés
- Protège les succursales de votre entreprise grâce à notre solution RED (Remote Ethernet Device).
- Protège les réseaux sans fil et permet un accès WiFi sécurisé

Disponible sous forme d'appliance matérielle, virtuelle ou uniquement logicielle

Avec Sophos UTM, vous bénéficiez d'un logiciel de sécurité complet, intégré à une seule et même appliance. Il vous permet de ne choisir que les solutions qui vous sont utiles, au moment où vous les exigez. Il peut être déployé sur la plate-forme la plus adaptée à votre entreprise : logicielle, matérielle ou virtuelle. Les mêmes fonctionnalités sont disponibles quel que soit le nombre d'utilisateurs à protéger. Enfin, il permet de gérer l'ensemble de la sécurité informatique de votre entreprise en toute simplicité, depuis une console Web unique.

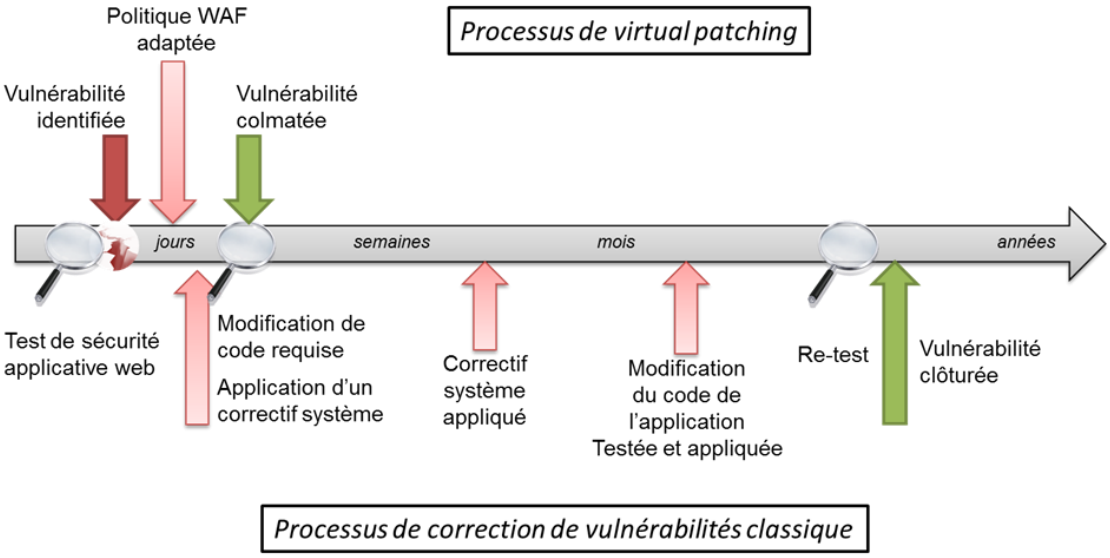
Lire la suite...

DenyAll : Patching Virtuel des Vulnérabilités Applicatives : Intégration entre pare-feu web et scanner de vulnérabilités pour améliorer la sécurité des applications web.

Toute application web peut présenter des vulnérabilités, qu'elles soient au niveau du développement de l'application (par exemple, des failles d'injection SQL ou XSS) ou du serveur web supportant l'application (par exemple, un serveur Apache et un moteur de script PHP).

Ces brèches sont causées par un manque de temps pour prendre en compte la sécurité dans les développements, une compétence insuffisante en sécurité ou des erreurs de développement. La mise à jour du serveur web lui-même nécessite également une supervision régulière et un suivi des dernières vulnérabilités découvertes pour appliquer les mises à jour et correctifs nécessaires.

Dans un contexte extrêmement évolutif où les applications web se multiplient, une vérification régulière et automatique de la sécurité applicative apparaît nécessaire et incontournable. A cette fin, un scanner de vulnérabilités applicatives (DAST, Dynamic Application Security Testing) tel que DenyAll Detect apportera aux responsables de la sécurité la possibilité de détecter automatiquement les vulnérabilités applicatives.



Lire la suite...