Une plateforme de sécurité de nouvelle génération

Les cybermenaces sont de plus en plus complexes, fréquentes et sophistiquées. Dès lors, seule une solution de sécurité complète offrant des fonctions intégrées nativement pour chaque domaine permet une riposte efficace.

Avec PAN-OS 8.0, Palo Alto Networks a lancé plus de 70 nouvelles fonctionnalités.

Les cybercriminels ont recours à des outils toujours plus sophistiqués pour voler des données et perturber l'activité informatique. Ainsi, des méthodes automatisées permettent de conduire des attaques à une cadence élevée, face auxquelles une équipe de sécurité ne peut assurer la détection et la riposte que très difficilement.

Les offres de sécurité classiques, qui proposent des fonctionnalités ponctuelles et qui nécessitent souvent des interventions manuelles, ne peuvent pas détecter et bloquer à temps les attaques complexes. A contrario, une plateforme de sécurité intégrée nativement, capable de coordonner et d'automatiser les mécanismes de protection, pourra bien mieux les contrer. La plateforme de nouvelle génération développée par Palo Alto Networks met à disposition, avec sa nouvelle version, des capacités supérieures de protection contre les menaces actuelles et futures.

Une prévention des menaces multi-méthode

Afin de reconnaître les logiciels malveillants, les outils de sécurité les font souvent tourner dans un environnement *sandbox* protégé. Cependant ces bacs à sable virtuels étant souvent composés d'éléments standardisés, les assaillants ont mis au point des méthodes de contournement sophistiquées. C'est pourquoi Palo Alto Networks offre désormais un environnement hyperviseur complètement défini par l'utilisateur. Au moyen d'une analyse *bare metal* embarquée directement au niveau matériel, il détecte les logiciels malveillants capables de reconnaître une virtualisation et de la contourner. Une autre innovation propose la possibilité de bloquer les tentatives adverses de *phone home* par reconnaissance automatique de leurs signatures *command and control.*

Prévention du vol d'identifiants

La plupart des violations de sécurité sont basées sur le vol d'informations d'identification telles que l'ID utilisateur et le mot de passe. Grâce aux informations dérobées, les attaquants peuvent en effet pénétrer profondément dans les systèmes. PAN-OS 8.0 prémunit triplement contre ce cas de figure. Premièrement, les sites de hameçonnage sont automatiquement identifiés et bloqués. Deuxièmement, si un utilisateur soumet tout de même des informations d'identification à un tel site, l'exécution est détectée et empêchée. Enfin troisièmement, même si un assaillant dispose d'informations d'identification volées, l'authentification multifacteur basée sur des stratégies déterminées l'empêche de se mouvoir sur le réseau.

Sécurité du cloud

Les entreprises stockent toujours plus de données et d'applications dans le cloud. Or, avec sa nouvelle version, PAN offre une sécurité accrue pour les clouds publics et privés: ainsi, les mesures de sécurité employées dans des environnements physiques peuvent aussi être appliquées sur Azure, AWS et autres. En outre, la possibilité d'utiliser de manière sûre et transparente des services SaaS tels que Dropbox et Salesforce a été fortement optimisée. OneNote et Slack sont désormais pris en charge et la prévention de pertes de données (DLP) supporte maintenant les contenus en allemand et en japonais. Par ailleurs, les VM de la série des pare-feux virtuels, comptent des débits allant jusqu'à 16 Gbit/s et fournissent les fonctionnalités de la nouvelle génération de PAN au cloud.

Gestion à l'échelle

Grâce à la version 8.0, les administrateurs disposent aussi d'informations plus précises et dans un délai plus rapide, le tout dans un environnement familier: ainsi, la solution de gestion de sécurité Panorama, qui fait partie de la plateforme Palo Alto Networks, délivre désormais des informations provenant de Traps, la solution de protection des terminaux. Elle transmet également les journaux détaillés du pare-feu, duquel elle garantit des mises à jour très rapides par des actions automatiques et des opérations à vitesse démultipliée.

Nouveau matériel

Les pare-feux matériels de PAN sont encore plus puissants. La série PA-5200 comprend trois modèles jusqu'à 72 Gbit/s de performance relative à l'ID de l'application et 30 Gbit/s de performance sur la prévention des menaces. En comparaison des autres fabricants, cela représente un rapport bien meilleur lors de la prévention des menaces entre le rendement «brut» et les performances réelles. Quant à la série PA-800, plus petite, elle fournit des débits allant jusqu'à 1,9 Gbit/s et 780 Mbit/s. Enfin, le modèle d'entrée de gamme PA-220 embarque toutes les fonctionnalités de PAN-OS dans un petit boîtier de bureau, idéal pour les succursales et les petites entreprises.

Les points forts de la nouvelle plateforme Palo Alto Networks

- Plateforme de sécurité de nouvelle génération intégrée nativement
- Blocage des méthodes de contournement des *sandboxes* et prévention des tentatives *phone home*
- L'outil de gestion Panorama présente désormais les données des journaux provenant de Traps, la solution de protection des terminaux.
- Pour la prévention des menaces, l'outil open source MineMeld travaille étroitement avec Autofocus, service de *threat intelligence* de PAN.
- Sécurité accrue pour les clouds publics et privés
- Nouvelles fonctionnalités pour l'utilisation en toute sécurité de SaaS
- Nouveaux modèles de pare-feux (matériels et virtuels) aux performances accrues

BOLL
IT Security Distribution

BOLL Engineering SA

En Budron H15
1052 Le Mont-sur-Lausanne
Tél. 021 533 01 60
contact@boll.ch
www.boll.ch | www.boll.ch/info/PAN-8-FR