Protection progressive pour les terminaux

Une lutte efficace contre les attaques connues et inconnues

Compte tenu de leur comportement réactif, les solutions d'antivirus actuelles ne sont pas en mesure d'identifier les codes malveillants dans les terminaux et d'empêcher l'introduction de logiciels malveillants. TRAPS, la solution «Advanced Endpoint Protection» de Palo Alto Networks, propose une solution à ce problème.

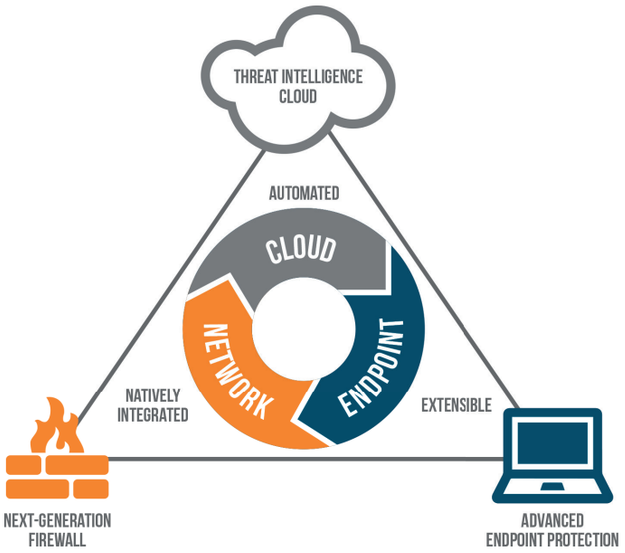
Cyber-attaques ultra-perfectionnées, «logiciels malveillants modernes», Exploits, attaques Zero-Day…: ce sont autant de menaces auxquelles sont exposés les PC, ordinateurs portables, tablettes et smartphones. Mais les solutions de sécurité des points d'accès et d'antivirus actuelles ne sont pas en mesure, malgré des mises à jour de signatures en temps réel, d'identifier des codes malveillants inconnus et d'empêcher l'introduction de logiciels malveillants dans l'informatique des entreprises.

Pour combler cette faille de sécurité des terminaux et lutter efficacement contre des attaques inconnues, Palo Alto Networks a lancé le logiciel innovant de sécurité des points d'accès TRAPS (Targeted Remote Attack Prevention System). Cette plate-forme hautement efficace et peu gourmande en ressources identifie à la fois les menaces connues et inconnues sans utiliser les méthodes d'identification des signatures ou d'analyses de comportements classiques. TRAPS identifie plutôt des techniques permettant d'utiliser les points faibles et protège les points d'accès des logiciels malveillants à l'aide de pièges très efficaces (Traps).

Lutte contre les Exploits

Dans la lutte contre les Exploits, TRAPS profite du fait qu'un pirate doit utiliser toute une série de techniques Exploit pour réussir une attaque. TRAPS est en mesure d'identifier ces techniques d'attaque et de les repousser immédiatement, sans connaître les points faibles existants, indépendamment de patchs, de signatures nécessaires ou mises à jour de logiciels.

L'intégration de TRAPS est efficace et nécessite peu de ressources. Lorsqu'un nouveau processus utilisateur est démarré, les modules de sécurité s'enclenchent automatiquement afin d'empêcher les manipulations dangereuses. Lorsqu'une attaque est lancée, TRAPS identifie les techniques utilisées, bloque l'attaque, met fin au processus concerné et informe l'utilisateur et l'administrateur de l'incident. Par ailleurs, TRAPS recueille des données d'investigation et les transmet immédiatement au gestionnaire de la sécurité des points d'accès concerné.



Le logiciel de sécurité des points d'accès TRAPS fait partie intégrante de la «Plate-forme de sécurité de nouvelle génération» de Palo Alto Networks.

Aperçu des caractéristiques

TRAPS, le «Targeted Remote Attack Prevention System» de Palo Alto Networks, peut être considéré comme la solution ATP (Advanced Threat Prevention) la plus révolutionnaire. Il

- empêche les Exploits à tous les points faibles,
- repousse les attaques basées sur les logiciels malveillants,
- fournit immédiatement des données d'investigation sur les attaques contrées,
- autorise une intégration parfaite dans les infrastructures de sécurité du réseau et du cloud,
- est modulable à volonté,
- séduit par une consommation de ressources extrêmement faible (env. 25 Mo de mémoire, 0.1 % CPU).

Protection contre les logiciels malveillants

TRAPS est également compatible avec des directives définies à l'avance pour empêcher les attaques de logiciels malveillants et garantir une protection complète efficace des terminaux. Des restrictions basées sur une politique permettent par exemple de contrôler via quels médias et répertoire externes des codes exécutables peuvent être démarrés ou quels processus peuvent se dupliquer d'eux-mêmes. Grâce à d'autres mécanismes pris en charge par TRAPS pour lutter contre les logiciels malveillants, on peut par ailleurs empêcher qu'un code Java potentiellement malveillant soit exécuté dans le navigateur. En outre, il est également possible d'identifier une «corruption de mémoire» et d'empêcher l'échange de bibliothèques dynamiques infectées par un code malveillant (DLL Hijacking) ou l'injection de codes.

BOLL
IT Security Distribution

BOLL ENGINEERING SA

En Budron H15, 1052 Le Mont s. Lausanne
Tél 021 533 01 60, contact@boll.ch,
www.boll.ch