

PRESSEMITTEILUNG

Neue Herausforderungen brauchen neue Antworten - Panda Security launcht Adaptive Defense 360

- Adaptive Defense 360 ist der erste und derzeit einzige IT-Security-Service, der eine Kombination aus EDR- und EPP-Technologien gegen APTs, Zero-Day-Attacks und Cryptolocker bietet.
- Adaptive Defense 360 klassifiziert alle laufenden Prozesse und gewährleistet so die proaktive Erkennung und Blockierung von ungewöhnlichem Verhalten und fortschrittlichen Bedrohungen.
- Adaptive Defense 360 bietet Funktionen zur Sperrung und Desinfektion von infizierten Anwendungen und nicht klassifizierten Prozessen.

Duisburg, den 15. Oktober 2015 - Heutzutage gibt es immer größere und vielfältigere Sicherheitshürden für Unternehmen: Mit täglich mehr als 230.000 neuen Malware-Exemplaren und stetig ausgereifteren Infektionstechniken sind die vertraulichen Daten, mit denen Firmenmitarbeiter täglich umgehen, zunehmend gefährdet. Als Antwort auf die steigenden Anforderungen an die IT-Sicherheit in Unternehmen präsentiert Panda Security Adaptive Defense 360, einen IT-Security-Service, der weit über die Leistungen blacklistbasierter Antimalware-Lösungen hinausgeht.

Adaptive Defense 360 kombiniert zwei von Panda Securitys Premium-Lösungen für den IT-Schutz in Unternehmen in einer einzigen Konsole:

- Panda Endpoint Protection Plus ist Pandas führende EPP (Endpoint Protection Platform)-Lösung, die alle Funktionen einer klassischen Schutzsoftware bietet: Antivirus, Antimalware, Personal Firewall, Web- und E-Mail-Filter sowie Device Management.
- Panda Adaptive Defense, Pandas EDR (Endpoint Detection & Response)-Lösung, bietet Erkennung und automatische Reaktion, lückenlose

Überwachung sowie, dank des integrierten SIEM-Tools, forensische Analysen in Echtzeit.

Dieser innovative Service bietet somit einen neuartigen **Endpoint Detection Service**, der in der Lage ist, jede einzelne Anwendung innerhalb eines Firmennetzwerkes genau zu klassifizieren, sodass nur vertrauenswürdige Prozesse ausgeführt werden. Genau das unterscheidet Adaptive Defense 360 von blacklistbasierten Antimalware-Lösungen.

Ein weiterer Vorteil von Adaptive Defense 360 ist, dass es Bedrohungen in realen Umgebungen entdeckt, unabhängig von der Quelle und dem angeschlossenen Device (z.B. USB-Laufwerk). Das geschieht bei den meisten ATD (Advanced Threat Detection)-Lösungen nicht, da sie häufig nur solche Bedrohungen lokalisieren, die in das Netzwerk und in virtualisierte Umgebungen eindringen.

Die **direkt auf den Endpoints** ausgeführten Funktionen von Adaptive Defense 360 basieren auf drei Prinzipien:

1. Ständige Überwachung und Analyse aller laufenden Anwendungen des Unternehmens
2. Automatische Klassifizierung mit Hilfe von selbstlernenden Systemen auf Pandas Big-Data-Plattform ‚Collective Intelligence‘
3. Analyse und manuelle Klassifizierung von Anwendungen, die nicht automatisch klassifiziert werden konnten, durch Techniker der PandaLabs, um das Verhalten von laufenden Anwendungen zu erkennen

Mit dieser Art von unmittelbarem Schutz und Reaktion auf den Endpoints liefert Panda Security eine umfassende IT-Security-Lösung, die sowohl gegen klassische Malware kämpft als auch präventiv gegen fortschrittliche und zielgerichtete Angriffe (APTs) schützt.

„Adaptive Defense 360 ist eine derzeit einzigartige Kombination aus EDR- und EPP-Technologien zur Bekämpfung von traditionellen Bedrohungen, gefährlichen Anwendungen oder fortschrittlichen Bedrohungen. Das Besondere ist die Analyse aller Computeraktivitäten, um jeden einzelnen Prozess entweder als Goodware oder als Malware zu klassifizieren. Um den Erkennungszyklus zu vervollständigen, enthält Adaptive Defense 360 außerdem integrierte Wiederherstellungsfunktionen“, erklärt Juan Santesmas, Vizepräsident für Produktmanagement & Business Development bei Panda Security.

Schutz für veraltete Systeme

Das Fehlen von Updates auf älteren Systemen ist ein wichtiger Einfallstor für Malware in Unternehmen. Adaptive Defense 360 enthält einen Funktionsbereich gegen Schwachstellen. Dieser nutzt Kontext- und Verhaltensregeln, sodass Firmen in einer sicheren Umgebung arbeiten können, auch wenn ihre Systeme nicht auf dem neuesten Patch-Stand sind oder vom Hersteller keine Sicherheits-Patches mehr erhalten (z. B. Windows XP).

Echtzeit-Informationen dank integriertem SIEM-Tool

Adaptive Defense 360 beinhaltet ein komplettes SIEM-Tool zur Visualisierung und forensischen Analyse dessen, was alle Prozesse im System bzw. Netzwerk auslösen. Die Daten erlauben nicht nur eine statistische Auswertung, sondern ermöglichen darüber hinaus eine detaillierte Übersicht sämtlicher ausgeführter Aktionen wie beispielsweise die Erstellung von Dateien, Interaktionen von Prozessen und deren Kommunikationswege.

Auf Grundlage dieser Daten liefert Adaptive Defense kontinuierlich Informationen über den Netzwerkstatus, sendet sofort Warnmeldungen, wenn eine Malware in das Netzwerk gelangt, und informiert über die ausgeführten Aktionen, um diese zu bekämpfen.

Einhundertprozentig gemanagter Service

Mit Adaptive Defense 360 brauchen Unternehmen keine Ressourcen in technisches Personal zu investieren, um Quarantäne, verdächtige Dateien sowie die Neuinstallation oder Desinfektion von infizierten Computern zu managen.

Adaptive Defense 360 klassifiziert automatisch alle Anwendungen mit Hilfe von selbstlernenden Systemen in Big-Data-Umgebungen und unter ständiger Aufsicht von spezialisierten Technikern der PandaLabs, die den gesamten Prozess managen.

Über Panda Security

Seit seiner Gründung 1990 in Bilbao kämpft Panda Security gegen alle Arten von Internet-Angriffen. Als Pionier der Branche reagierte das IT-Sicherheitsunternehmen mit verhaltensbasierten Erkennungsmethoden und der Cloud-Technologie auf die neuen Anforderungen des Marktes. Dank der speziellen Cloud-Technologien greifen User via Internet auf die weltweit größte Signaturdatenbank zu und erhalten schnellen und zuverlässigen Virenschutz ohne lokales Update. Das Unternehmen hat seinen Hauptsitz in Spanien und direkte Präsenzen in mehr als 80 Ländern sowie Millionen von Kunden auf der ganzen Welt. Die Produkte werden in über 23 Sprachen übersetzt. Die Mission des Unternehmens ist es, die Komplexität zu vereinfachen sowie neue und verbesserte Lösungen zu entwickeln, um das digitale Leben der Anwender zu schützen.

Pressekontakt:

Kristin Petersen
Presse & PR

PAV Germany GmbH
Dr.-Alfred-Herrhausen-Allee 26
47228 Duisburg

Tel: +49 2065 961 352
Fax: +49 2065 961 195
Kristin.Petersen@de.pandasecurity.com
www.pandanews.de
www.pandasecurity.com/germany/