PRESSEMITTEILUNG

EDR-Technologie – Gegenwart und Zukunft der IT-Security

Duisburg, den 31. August 2015 - Traditionelle Viren, die als ausführbare Programme definiert sind und massenweise verschickt werden, um in großem Stil Infektionen zu verursachen, werden bereits seit Jahren erfolgreich von Endpoint Protection Plattformen (EPPs) kontrolliert. Dies sind gemeinhin bekannte Antiviren-Programme, die die Endgeräte der Nutzer schützen. Allerdings haben sich die Cyberkriminellen in den letzten Jahren stark weiterentwickelt und ebenso ihre Angriffsmethoden.

Moderne Hacker ändern täglich ihre Ziele, fortgeschrittene anhaltende Bedrohungen (Advanced Persistent Threats) gehören inzwischen zum Hauptfokus ihrer Aktivitäten. Gezielte Angriffe, Ransomware (wie zum Beispiel Cryptolocker, der Informationen auf infizierten Computern verschlüsselt und für die Daten ein Lösegeld fordert), Zero-Day-Attacken… - sie alle breiten sich in unserem digitalen Leben aus. Unternehmen und Heimanwender sind gleichermaßen bedroht, nicht nur von Datendiebstahl, sondern damit verbunden auch von wirtschaftlichem Schaden.

Mittlerweile hat die IT-Sicherheitsindustrie angefangen zu reagieren und viele Big Player in diesem Bereich haben Plattformen veröffentlicht, die weit über den einfachen Schutz eines digitalen Systems hinausgehen – sie können fortgeschrittene Bedrohungen erkennen und gleichzeitig auf eventuelle Vorfälle reagieren. Wir sprechen von der „Endpoint Detection and Response Technologie“ oder kurz: EDR-Technologie.

Geprägt wurde dieser Begriff seit 2013 von dem Gartner-Sicherheitsanalysten Anton Chuvakin. EDR definiert dabei eine Kategorie von Methoden und Lösungen, die darauf abzielen, verdächtige Aktivitäten und Vorkommnisse auf Servern und Endpoints zu entdecken und zu untersuchen. Diese aufstrebende Technologie hat Panda Security mit seinem Managed Service **Adaptive Defense 360** aufgegriffen und durch die Kombination mit Pandas klassischem Endgeräte-Schutz in eine derzeit einzigartige Security-Lösung verwandelt.

„Der Schutz, den EPP-Lösungen bieten, reicht heute für viele Unternehmen nicht mehr aus“, erklärt Eduardo Fernández Canga, Global Marketing Manager bei Panda Security in Spanien. „Antiviren-Programme sind immer noch wichtig. Sie schützen vor bekannten Bedrohungen und blockieren einen Großteil der im Umlauf befindlichen Malware. Das Problem ist jedoch, dass es einige neue Malware-Generationen

dennoch schaffen, in die geschützten Systeme einzudringen. Daher benötigen gerade mittlere und große Firmen, die vermehrt im Fokus von Hackerattacken stehen, Tools bzw. Technologien, die auch die neuesten Bedrohungen erkennen und auf diese reagieren können.“, fügt er hinzu.

Adaptive Defense 360: moderne, maßgeschneiderte Security-Lösung

Pandas Antwort auf die jüngsten Entwicklungen im Bereich der Cyberattacken heißt Adaptive Defense 360. Über einen Zeitraum von ca. fünf Jahren haben Panda-Experten diese moderne und derzeit einzigartige IT-Security-Lösung entwickelt. Sie basiert auf den neuesten Entwicklungen im Bereich der EDR-Technologie, ist kompatibel mit allen Windows-Betriebssystemen und wird auch bald für Android-Geräte erhältlich sein.

Doch was ist das Besondere an Adaptive Defense 360? Eduardo Fernández Canga erläutert: „IT-Schutzlösungen, die eine Bedrohung erkennen, generieren immer ein Identifizierungszeichen und setzen dieses auf eine Blacklist. Problematisch daran ist jedoch Folgendes: Steht eine ausführbare Datei nicht auf dieser Blacklist, dann betrachtet die Lösung diese als Goodware und unternimmt nichts gegen sie. Adaptive Defense 360 verlässt sich hingegen nicht nur auf eine derartige Blacklist. Es ist gegenüber allen auf den Endpoints laufenden Prozessen grundsätzlich misstrauisch.“

Wie funktioniert Adaptive Defense 360 also? Zuerst wird ein Agent auf dem Gerät des Nutzers installiert. Dieser kontrolliert und sammelt Informationen über das Verhalten jeder einzelnen auf dem System laufenden Anwendung. Die generierten Verhaltensinformationen werden an die Panda Collective Intelligence gesendet. Mit Hilfe von Big Data und Data-Mining-Tools kann Panda 99,6 Prozent aller dieser Informationen automatisch klassifizieren, einschließlich Goodware und Malware. Die verbleibenden 0,4 Prozent werden durch eine Gruppe von erfahrenen Analysten in den PandaLabs analysiert und klassifiziert.

Ein wichtiger Unterschied zwischen Adaptive Defense 360 und anderen derzeit erhältlichen Security-Lösungen ist, dass „Adaptive Defense 360 eine Whitelist für den Kunden erstellt, die wir zur Analyse der Executables nutzen“, sagt Fernández. Zudem klassifiziert die Plattform die ausführbaren Dateien nicht nur, sondern überwacht, dass sich ihr Verhalten nicht ändert. „Normalerweise sind Whitelist-Lösungen nicht in der Lage, eine Veränderung zu erkennen, wenn sie ein ausführbares Programm einmal als Goodware klassifiziert haben. Adaptive Defense 360 generiert jedoch ein Verhaltensmuster für jede ausführbare Datei. Wenn diese das Muster verlässt, wird ein Alarm ausgelöst und der entsprechende Prozess wird automatisch geblockt“, ergänzt der Panda Security Experte.

Die beschriebene Funktionsweise von Adaptive Defense 360 ermöglicht es Panda-Kunden, mit gefährdeten Applikationen, wie zum Beispiel alten Versionen von Java, Chrome oder dem Internet Explorer, zu arbeiten und trotzdem vor IT-Bedrohungen geschützt zu sein. „Viele Unternehmen arbeiten noch immer mit alter Software oder alten Betriebssystemen, wie beispielsweise Windows XP, die von den Herstellern nicht mehr mit den neuesten Sicherheits-Updates unterstützt werden. Doch selbst bei der Verwendung von aktueller Software ergibt sich häufig das Problem, dass Sicherheits-Updates nicht immer zeitnah eingespielt werden können. Unternehmen können sich daher heutzutage nur dann absolut zuverlässig gegen Hackerangriffe schützen, wenn sie ein System wie Adaptive Defense 360 als IT-Sicherheitslösung verwenden“, so Fernández.

Absolute Kontrolle über den Datenfluss in der Organisation

Ein anderer Vorteil von Adaptive Defense 360 ist, dass der Systemadministrator genau nachvollziehen kann, welchen Weg der Datenfluss auf den Computern eines Netzwerkes genommen hat. Die Administratoren können also jederzeit sehen und kontrollieren, welcher Prozess auf welche Daten zugreift.

Eduardo Fernández Canga: „Adaptive Defense 360 ein derzeit einzigartiges, leistungsstarkes und für jeden Kunden maßgeschneidertes Tool, mit dem man sowohl den Informationsfluss innerhalb der Organisation als auch den eingehenden und abgehenden Datenverkehr präzise analysieren, verstehen und visualisieren kann. Mit Adaptive Defense 360 weiß der Administrator genau, welcher Prozess wie und wann auf Daten zugreift und hat somit die absolute Kontrolle über den gesamten Informationsfluss innerhalb seiner Organisation.“

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/