PRESSEMITTEILUNG

Haben wir von Locky, Cerber & Co nichts gelernt?

Warum klassischer Endpoint-Schutz heutzutage nicht mehr ausreicht

***Duisburg, den 05. April 2017* – Verschlüsselungstrojaner wie Locky und Cerber – aber auch diverse andere fortschrittliche Malwaretypen - bereiten Unternehmen aller Größenordnungen bereits seit Monaten Kopfzerbrechen. Denn obwohl fast alle angegriffenen Firmen eine oder sogar mehrere Antimalware-Lösungen im Einsatz hatten, konnten sie sich gegen die immer raffinierteren Hackermethoden nicht schützen. Es stellt sich also die Frage, warum die etablierten Endpoint-Schutzmechanismen den Angriff nicht verhindert haben?**

Das Problem ist: Klassischer Endpoint-Schutz arbeitet nach dem Blacklisting-Prinzip. Das bedeutet, dass die Bedrohung bzw. das Verhaltensmuster der Malware bekannt sein muss, damit sie erkannt und blockiert werden kann. Zwar suggerieren die Testberichte renommierter Institute mit Erkennungsraten von bis zu 100 Prozent eine vermeintliche Sicherheit vor Cyberangriffen; schlussendlich handelt es sich dabei jedoch um eine Illusion, da bei den Tests immer ein mehrere Stunden alter Viren-Pool verwendet wird.

Hacker können jedoch innerhalb von Minuten in IT-Systeme eindringen und Daten stehlen. Laut Data Breach Investigations Report 2016 geschehen 93 Prozent der Cyberangriffe innerhalb von Minuten nachdem die Schadsoftware erstmals aufgetreten ist. Von der klassischen Virenschutz-Software werden jedoch überhaupt nur ca. 80 Prozent der Malware innerhalb der ersten 24 Stunden erkannt. Fast ein Prozent der Malware-Exemplare bleibt von den Antivirenscannern sogar ein Jahr nach ihrer Entdeckung unerkannt.

Im Kampf gegen Cyberkriminalität geht es jedoch um Minuten. Dies haben diverse Ransomware-Angriffe der letzten Monate belegt. So infizierte ‚Locky' trotz bestehender Schutzmechanismen in den ersten Tagen nach seinem erstmaligen Erscheinen über 5.000 Endpoints pro Stunde. Auch ‚Cerber' blieb durch die Änderung seines Hashwerts im 15-Sekunden-Rhythmus für traditionelle AV-Lösungen zunächst unsichtbar.

Wer den Kampf gegen moderne Hacker gewinnen will, muss neue Wege gehen

„Klassischer Endpoint-Schutz reicht nicht mehr aus. Intelligente Systeme, die mithilfe cloudbasierter Scan-Technologien alle laufenden IT-Prozesse kontinuierlich überwachen, analysieren und klassifizieren, sind heute alternativlos." Diese These

vertritt Jan Lindner, deutscher Geschäftsführer des IT-Sicherheitsspezialisten Panda Security. "Wenn wir diese intelligenten Schutzsysteme ergänzend einsetzen, dann sind erfolgreiche Angriffe durch Cryptolocker und andere moderne Malwaretypen heute vermeidbar und keinesfalls mehr akzeptabel“, erklärt Lindner weiter.

Wie sollte also eine moderne Abwehrtechnologie aussehen, die es mit den fortschrittlichen Angriffen moderner Hacker aufnehmen kann? Laut Jan Lindner bedarf es heute wesentlich mehr als eine klassische, signaturbasierte Antimalware-Lösung, um im aktuellen Cyberkrieg bestehen zu können. „Wir brauchen heute eine Kombination aus traditionellen Antiviren-Lösungen und modernen Schutzmechanismen wie Endpoint Dectection and Response, um neuartige Bedrohungen abzuwehren“, erläutert Lindner.

Die IT-Sicherheitsexperten von Panda Security setzen dabei auf ihre neuentwickelte ‚Adaptive Defense‘-Lösung, einen Managed Service, der permanent alle Anwendungen und Prozesse, die auf den Endpoints oder Servern ausgeführt werden, überwacht. Dieses permanente Prozess-Monitoring, in Verbindung mit einer intelligenten Big-Data-Analyse in der Cloud, ermöglicht die nahezu automatische Klassifizierung aller laufenden Prozesse. Jede Applikation, die nicht automatisch klassifiziert werden kann, wird zudem von IT-Experten analysiert. Alle unbekannten Anwendungen wie Cryptolocker und Zero-Day-Exploits werden aufgrund ihres Verhaltens automatisch blockiert und können keinen Schaden an den Endpoints und Servern anrichten.

Diese Fähigkeit, absolut alles zu kontrollieren, was auf den Computern der Anwender passiert, bietet einen bisher unerreichten Schutzlevel – und zwar auch schon in der Sekunde, in der der Cyberangriff passiert, und nicht erst mehrere Stunden später.

Weitere Informationen von Panda Security zum diesem Thema finden Sie unter http://pandainside.de/endpoint-protection-ist-nicht-genug/

Über Panda Security

Seit seiner Gründung 1990 in Bilbao kämpft Panda Security gegen jedwede Bedrohung der IT-Infrastrukturen von Unternehmen bis zu Heimanwendern. Als Pionier der IT-Security-Branche gelang es dem Entwicklerteam immer wieder, mithilfe bedeutender technologischer Meilensteine den Sicherheitslevel seiner Kunden entscheidend zu erhöhen. So gilt Panda heute als ‚Entwickler des Cloud-Prinzips bei der Malware-Bekämpfung'.(Quelle: Magic Quadrant for Endpoint Protection Platforms, Gartner, 2012)
Basierend auf seinen Entwicklungen stellt das Unternehmen heute eine einzigartige Plattform zur Verfügung, die unter der Bezeichnung Adaptive Defense verschiedenste Technologien wie EDR (Endpoint Detection and Response), EPP (Endpoint Protection Platform), SIEM (Security Information and Event Management) und DLP (Data Loss Prevention) verbindet. Dadurch wird ein zuverlässiger Schutz wie zum Beispiel vor Ransomware (Cryptolocker) auf den Endpoints realisiert.
Das Unternehmen Panda Security mit Hauptsitz in Spanien ist aktuell in über 50 Ländern präsent, schützt weltweit mehr als 30 Millionen Anwender und stellt seine Lösungen in 23 Sprachen zur Verfügung.

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