Containment-Technologie von Comodo erstickt Malware-Attacken im Keim

Containment-Technologie von Comodo erstickt Malware-Attacken im Keim

Schadsoftware präventiv isolieren statt auf Erkennungsmechanismen vertrauen
IT-Security-Experte Comodo dreht den Spieß um: Statt wie andere Marktbegleiter in puncto Virenschutz auf Erkennung mittels Blacklisting zu setzen, vertraut der Hersteller auf Prävention und Isolierung. Nur bekannte Elemente erhalten Zugriff aufs Netzwerk, unbekannte werden über die eigens entwickelte Containment-Technologie in eine gesicherte virtuelle Umgebung verschoben. Hier werden sie isoliert ausgeführt und überprüft. Damit entsteht ein Malware-Schutzschild für die gesamte IT-Infrastruktur. Die Containment-Technologie ist in alle Security-Lösungen des Entwicklers, darunter der Comodo Endpoint Security Manager (CESM), integriert.
Mit seiner Herangehensweise ist Comodo dem Markt einen Schritt voraus. Denn herkömmliche Antivirenlösungen basieren auf dem Erkennungsprinzip ("detection"), bei dem sie Elemente gegen eine "Blacklist" prüfen. Sie enthält alle bekannten infizierten Dateien und Bedrohungen. Auf Grundlage dieses "Default Allow"-Standards (standardmäßig erlaubter Zugriff) wird festgestellt, welche Programme oder Dateien sicher ausgeführt oder für den Systemzugriff zugelassen werden können. Das Problem: Alle Bedrohungen müssen bekannt sein, damit der Schutz zuverlässig gewährleistet ist. Zero-Day-Angriffe, die erstmalig auftreten, sind ggf. noch nicht registriert und werden damit im schlimmsten Fall ausgeführt. Eine Blacklist zu 100 % aktuell zu halten ist bei der heutigen Masse und schnellen Vermehrung von Schadsoftware nicht möglich.
Malware-Verbreitung ausgeschlossen
Aus diesem Grund hat Comodo seine Next-Level-Security-Lösungen auf dem Prinzip der "Default Deny Protection" aufgesetzt. Statt Blacklist-Gegenprüfung erfolgt eine standardmäßige Abwehr aller unbekannten Dateien und Anwendungen, unter der Annahme, dass sie möglicherweise Bedrohungen darstellen. Ausschließlich bekannte, als sicher eingestufte Elemente werden ausgeführt. Nicht vertrauenswürdige Dateien verschiebt die Containment-Technologie in eine virtuelle Betriebsumgebung und führt sie dort, abgeschirmt vom restlichen System, aus. Sollte es sich tatsächlich um Viren oder andere bösartige Software handeln, können sie keinen Schaden im Netzwerk anrichten oder sich weiterverbreiten. Darüber hinaus werden verdächtige Dateien automatisch in die Valkyrie Malware Labs von Comodo hochgeladen, einer cloud-basierten Verhaltensanalyse zur Überprüfung der Vertrauenswürdigkeit. Alle Prozesse finden ohne Unterbrechung für den Endnutzer statt.
"Nur unser ?Default Deny-Ansatz gewährleistet sichere IT-Umgebungen und bringt Endpoint Security auf einen neuen Level", kommentiert Karl Hoffmeyer, Senior Channel Sales Manager DACH bei Comodo. "Denn betrachten wir den Sachverhalt, übertragen in die Realität: Niemand würde Fremde einfach so in sein Haus bitten, wie konventionelle Antivirenlösungen unbekannten Dateien den Netzwerkzugang erlauben. Nur als vertrauenswürdig eingestufte Whitelist-Einträge oder mittels einer Erlaubnis des Nutzers bestätigte Dateien und Programme werden ausgeführt. Alle weiteren Elemente überprüft unsere Technologie zunächst. Wenn nötig, kann der User innerhalb der isolierten Umgebung mit den Dateien arbeiten - ohne seinen Rechner oder gar das ganze Netzwerk zu gefährden. Die Integrität des Betriebssystems und der Benutzerdaten wird permanent sichergestellt."
Ein YouTube-Video veranschaulicht die Funktionsweise des Comodo-Prinzips. Auf der Comodo-Website können sich Interessierte für kostenlose Tests der Enterprise-Produkte registrieren. Die Security-Lösungen von Comodo werden in Deutschland über die VADs Intellicomp GmbH und sysob vertrieben.
Über Comodo:
Comodo wurde im Jahr 1998 gegründet und hat sich zunächst einen Namen als Anbieter von SSL-VPN-Technologien gemacht. Mit seinen SSL-Lösungen verfügt Comodo mittlerweile über einen weltweiten Marktanteil von etwa 40 Prozent. Heute entwickelt das Unternehmen zudem innovative Antivirus-Lösungen für Endanwender und den professionellen Einsatz. Durch das patentierte Auto-Sandbox-Verfahren lässt sich nachweislich ein fast einhundertprozentiger Schutz vor Malware garantieren. Das US-amerikanische Unternehmen befindet sich in Privatbesitz und beschäftigt weltweit über 1.350 Mitarbeiter an Standorten in den USA, China, UK, Italien, Rumänien, der Ukraine sowie der Türkei und in Japan. Mehr als 75 Prozent der Comodo-Mitarbeiter sind in der Forschung und Entwicklung tätig. Verteilt auf die unterschiedlichen Zeitzonen, betreibt Comodo acht Virenlabore. Diese so genannten Comodo ValkyrieTM Labs gewährleisten rund um die Uhr die zuverlässige Erkennung und Bekämpfung von Schädlingen aus dem Internet. Weitere Informationen unter: www.comodo.com .

Ansprechpartner Comodo Deutschland
Karl Hoffmeyer
Bleichstraße 3
D-33102 Paderborn
Tel.: +49(0)172 / 4351289
E-Mail: karl.hoffmeyer@comodo.com
Web: www.comodo.com
PR-Agentur Comodo:
Sprengel
 Partner GmbH
Nisterstraße 3
D-56472 Nisterau
Ansprechpartner:
Marius Schenkelberg
Tel.: +49(0)2661 / 912600
E-Mail: ms@sprengel-pr.com
Web: www.sprengel-pr.com
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=573202" width="1" height="1">

Pressekontakt

Comodo

33102 Paderborn

karl.hoffmeyer@comodo.com

Firmenkontakt

Comodo

33102 Paderborn

karl.hoffmeyer@comodo.com

Über ComodoComodo wurde im Jahr 1998 gegründet und hat sich zunächst einen Namen als Anbieter von SSL-VPN-Technologien gemacht. Mit seinen SSL-Lösungen verfügt Comodo mittlerweile über einen weltweiten Marktanteil von etwa 40 Prozent. Heute entwickelt das Unternehmen zudem innovative Antivirus-Lösungen für Endanwender und den professionellen Einsatz. Durch das patentierte Auto-Sandbox-Verfahren lässt sich nachweislich ein fast einhundertprozentiger Schutz vor Malware garantieren. Das US-amerikanische Unternehmen befindet sich in Privatbesitz und beschäftigt weltweit über 1. 350 Mitarbeiter an Standorten in den USA, China, UK, Italien, Rumänien, der Ukraine sowie der Türkei und in Japan. Mehr als 75 Prozent der Comodo-Mitarbeiter sind in der Forschung und Entwicklung tätig. Verteilt auf die unterschiedlichen Zeitzonen, betreibt Comodo acht Virenlabore. Diese so genannten Comodo ValkyrieTM Labs gewährleisten rund um die Uhr die zuverlässige Erkennung und Bekämpfung von Schädlingen aus dem Internet. Weitere Informationen unter: www.comodo.com.