McAfee Application Control verlängert die Lebensdauer älterer Microsoft Windows XP-Systeme

Zum 8. April 2014 wird Microsoft den Support für das Betriebssystem Windows XP einstellen. Nach diesem Datum werden in Windows XP entdeckte Schwachstellen nicht mehr durch die Sicherheitsaktualisierungen von Microsoft abgedeckt. Die Einstellung des Supports ist ein Problem für Kunden, da Windows XP-Systeme ohne den Support von Microsoft anfälliger für Zero-Day-Schwachstellen werden. Über 30 % der Unternehmen benutzen immer noch Windows XP-Systeme. Sie werden sich nun in zunehmendem Maße auf zusätzliche Vorsichtsmaßnahmen in puncto Sicherheit verlassen müssen, um Bedrohungen einen Schritt voraus sein zu können.

Obwohl Microsoft Kunden empfohlen hat, rechtzeitig zum 8. April 2014 eine Strategie zur Migration von Windows XP auf ein aktuelleres Betriebssystem zu entwickeln, bedeuten die dazu erforderlichen IT-Ressourcen, dass dies für viele Organisationen ein unrealistischer Vorschlag ist. Aber nicht von Windows XP wechseln zu können oder dieses weiter benutzen zu wollen, bedeutet nicht unbedingt, dass Windows XP-Nutzer Sicherheitslücken ausgeliefert sind. McAfee® Application Control bietet eine effektive Möglichkeit, die Ausführung unautorisierter Anwendungen zu verhindern, und wird auch nach Inkrafttreten der Einstellung des Microsoft-Supports Windows XP unterstützen. Zur Verhinderung von Zero-Day-Angriffen bedient sich McAfee Application Control einer dreistufigen Verteidigungsstrategie, die auf einer Whitelist-Lösung aufbaut, die bei minimaler Belastung der Systemressourcen Schutz bietet.

Dynamische Whitelists

Whitelists stellen ein recht einfaches, jedoch effektives Konzept dar. Sie erstellen Listen vertrauenswürdiger Programme, die für den alltäglichen Betrieb benötigt werden, und stellen sicher, dass nur diese bestimmten Anwendungen ausgeführt werden dürfen. Die Funktion sorgt für eine Reduktion des Aufwands, indem sie den Scan jeder einzelnen Anwendung überflüssig macht.

Speicherschutz

In einer Whitelist verzeichnete Programme, die Schwachstellen aufweisen, können nicht über einen Pufferüberlauf angegriffen werden. Diese Funktion verhindert, dass komplexe Bedrohungen die Whitelist umgehen.

McAfee Global Threat Intelligence

McAfee Global Threat Intelligence ist ein Cloud-basierter Service, der auf Grundlage der von McAfee Application Control verwendeten Dateireputation Anwendungen als sicher oder gefährlich einstuft. Diese Funktion zeigt an, ob aus Versehen Malware auf die Whitelist gelangt ist. Sie zeigt ebenfalls Dateien ohne Reputation auf, die individuell untersucht werden müssen.

Zusammenarbeitende Stufen zur Verhinderung von Zero-Day-Bedrohungen

Ein typischer Zero-Day-Angriff weist eine Vielzahl von Faktoren auf. Zunächst nutzt er eine Schwachstelle in einer bereits auf dem System installierten Software aus. Anschließend versucht er, die Schwachstelle zugunsten des Angreifers auszunutzen. Abschließend ist es sehr wahrscheinlich, dass die angreifende Malware einen Teil ihrer selbst zurücklässt, um eine dauerhafte Präsenz selbst bei einem Neustart aufrechtzuerhalten.

Schwachstellen schließen

McAfee Application Control reduziert in dieser Hinsicht das Risiko, indem es Administratoren ermöglicht, eine Untergruppe von Binärdateien festzulegen, die zur Ausführung autorisiert sind. Durch Kontrolle der Anwendungen wird die potenzielle Angriffsfläche für unbekannte oder unautorisierte installierte Anwendungen erheblich reduziert.

McAfee Application Control schließt nicht von sich aus Schwachstellen, sorgt jedoch dafür, dass eine Ausnutzung dieser Schwachstellen weitaus schwieriger ist, wenn nicht gar unmöglich wird. Obwohl nur ein Patch den Code reparieren kann, können mögliche Schwachstellen so geschützt werden, dass das Risiko ihrer Ausnutzung durch einen Angreifer erheblich reduziert wird.

Kompromittierungen stoppen

McAfee Application Control nutzt seinen Speicherschutz zur Verhinderung der meisten Arten der Ausnutzung eines Pufferüberlaufs. Dies verringert die Chance, dass Zero-Day-Schwachstellen bei der Ausführung von Codes effektiv ausgenutzt werden können, erheblich. Hinzu kommt, dass viele Angriffe von außen Binärdateien aufrufen. Indem nur festgelegte Binärdateien ausgeführt werden dürfen, wird der Angriffstechnik, bei der ein neuer Code in ein System geladen und ausgeführt wird, automatisch begegnet.

Spätere Probleme vermeiden

Da nur festgelegte Binärdateien ausgeführt werden können, wird ein Versuch, eine vorher nicht genehmigte und festgelegte Binärdatei auszuführen, scheitern. Dies funktioniert in derselben Sitzung, in der auch der Angriff stattfindet, oder nach einem Neustart. Durch einen Angriff kann keine neue, auf eine Festplatte heruntergeladene Binärdatei ausgeführt werden. Mc Afee Application Control verhindert auch, dass bestehende Binärdateien überschrieben werden.

Fazit

Die Einstellung des Supports für Windows XP erzeugt ein erhöhtes Sicherheitsrisiko für viele Organisationen, die immer noch dieses Betriebssystem verwenden. Windows XP-Nutzer erhalten keine Sicherheits-Patches mehr und sind daher anfälliger für gezielte Angriffe. McAfee Application Control bietet über die Einstellung des Microsoft-Supports hinaus weiterhin Schutz für Windows XP-Systeme, indem bei nur geringer Belastung der Systemressourcen unautorisierte Anwendungen an der Ausführung gehindert werden. Mithilfe einer effektiven Whitelist-Lösung können IT-Administratoren ohne ein vollständiges Upgrade des Betriebssystems gegen Sicherheitsbedrohungen vorgehen.

McAfee GmbH
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.mcafee.com/de

60752brf_xp-app-control_1213_fnl_ETMG