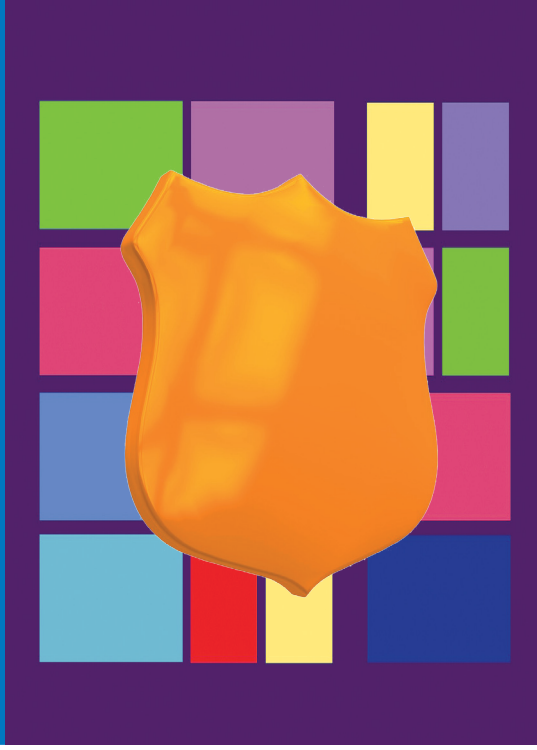
Die Zukunft beim Schutz vor **Malware** liegt in der **Micro-Virtualisierung**



Von Jochen Koehler

Klassische Sicherheitssysteme im Finanzwesen stoßen zunehmend an ihre Grenzen. Denn sie sind auf die Erkennung von Malware angewiesen, aber ein hundertprozentiges Erkennen derselben ist und bleibt eine Utopie, so der Autor. Die Zukunft der Sicherheitslösungen sieht er deshalb in der Micro-Virtualisierungstechnologie, bei der nicht das Aufdecken von Schadcodes oder Angriffen, sondern die in der Hardware stattfindende Isolierung gefährlicher Aktivitäten im Vordergrund steht. Red.

Der Finanzsektor gehört zu den drei Hauptzielen der Cyberkriminalität. Betroffen sind unter anderem Banken, Kreditinstitute, Versicherungen oder Investmentunternehmen. Die Cyberangriffe auf die Finanzindustrie werden dabei immer raffinierter und haben deutlich zugenommen.

So wurde beispielsweise im November 2015 aufgedeckt, dass Cyberkriminelle dem Finanzunternehmen Scottrade 4,6 Millionen Kundendaten gestohlen haben und im März 2016 wurde bekannt, dass die Bangladesh Central Bank von einer unbekannten Hackergruppe um rund 80 Millionen US-Dollar erleichtert wurde. Dabei hatte die Bank noch Glück im Unglück. Ein simpler Rechtschreibfehler verhinderte, dass die Cyberkriminellen mit der angestrebten Gesamtsumme von einer Milliarde US-Dollar abziehen konnten.

Herkömmliche Lösungen bieten keinen ausreichenden Schutz

Es zeigt sich, dass heute gängige Client-Sicherheitslösungen, die für die Abwehr von Angriffen, Signaturen, Verhaltensanalysen oder heuristische Methoden nutzen, keinen zuverlässigen Schutz vor der wachsenden Anzahl an polymorphen Cyber-Bedrohungen, Zero-Day-Attacken und Advanced Persistent Threats bieten. Das liegt daran, dass herkömmliche Lösungen wie Intrusion-Prevention-Systeme oder Antiviren-Software, aber auch Next-Generation-Firewalls auf die Malware-Erkennung angewiesen sind.

Unternehmen nutzen deshalb auch zunehmend Sandboxing-Lösungen, bei denen Applikationen in einer isolierten virtuellen Umgebung ausgeführt werden. Aber auch die Sandbox-Analyse bietet keinen ausreichenden Schutz, denn auch sie erkennt neue zielgerichtete Attacken in der Regel nicht. Außerdem gibt es inzwischen zahlreiche Methoden für ein erfolgreiches Umgehen des Sandbox-Schutzes. Zum Beispiel statten Malware-Entwickler ihren Schadcode mit einer Zeitverzögerung aus, so dass er von der Sandbox nicht sofort zu erkennen ist.

Traditionell genutzte Lösungen sind somit unzureichend. Abgesehen davon, dass ihre „mangelnde Treffsicherheit" zu einer hohen Zahl von False Positives und False Negatives führt, können sie auch das Unternehmensnetz nicht zuverlässig schützen.

Hundertprozentiges Erkennen von Malware ist eine Utopie

Das zentrale Problem bisheriger Ansätze in der IT-Sicherheit ist, dass ein hundertprozentiges Erkennen von Malware eine reine Utopie ist und auch bleiben wird. Ein gänzlich anderes Lösungsmodell verfolgt die Micro-Virtualisierungstechnologie. Das zugrunde liegende Konzept dabei lautet: Es steht nicht die Detektion von Schadcode oder das Aufspüren von Angriffen im Vordergrund, sondern der gezielte Schutz vor Malware, wobei diese nicht zwingend als solche erkannt werden muss. Realisiert wird dies durch die Isolierung aller potenziell gefährlichen Aktivitäten.

Vereinfacht ausgedrückt erfolgt bei der Lösung der Malware-Schutz direkt am Endpunkt durch Hardware-isolierte Micro-VMs, mit denen alle Anwenderaktivitäten gekapselt werden – zum Beispiel das Aufrufen

Zum Autor

Jochen Koehler, Regional Director DACH, Bromium, Heilbronn

einer Webseite, das Downloaden eines Dokuments, das Öffnen eines E-Mail-Anhangs oder der Zugriff auf die Daten eines USB-Geräts. Eine Kompromittierung des Endpunkts über einen dieser Angriffswege ist damit ausgeschlossen.

Mit diesem Lösungsansatz werden Hardware-isolierte Micro-VMs für alle Anwenderaktivitäten mit Daten aus unbekannten Quellen realisiert. Jeder einzelne Task läuft dabei in einer eigenen Micro-VM – und zwar strikt getrennt voneinander, vom eigentlichen Betriebssystem und vom verbundenen Netzwerk. Konkret heißt das, dass alle einzelnen – auch mit nur einer Applikation verbundenen – Aktivitäten voneinander isoliert werden, zum Beispiel unterschiedliche Seitenaufrufe in einem Browser oder das Öffnen verschiedener Dokumente mit Word, Excel oder anderen Anwendungen. Damit wird zuverlässig verhindert, dass sich Schadprogramme ausbreiten.

Die potenzielle Angriffsfläche wird minimiert

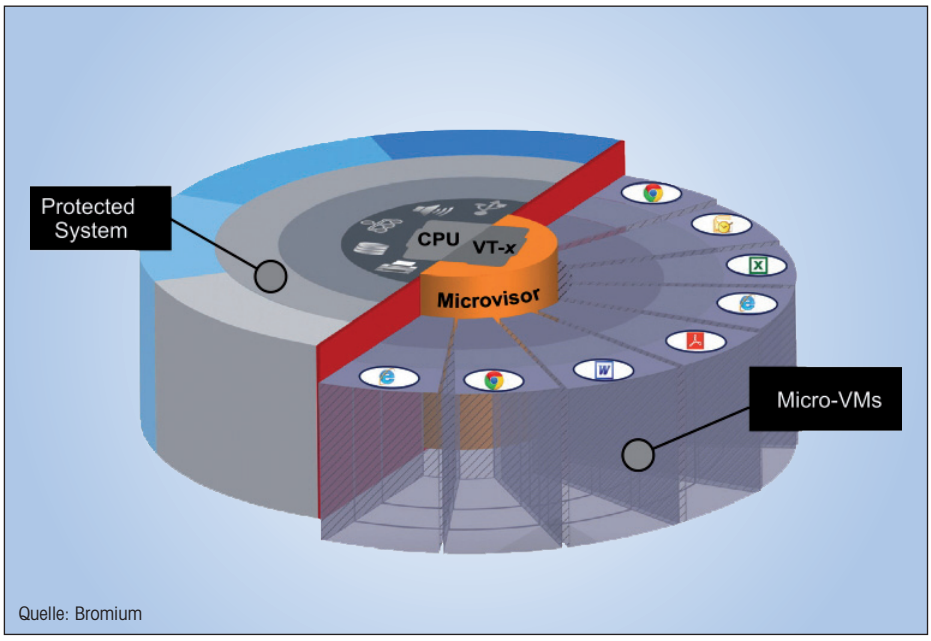
Unter technischen Gesichtspunkten kennzeichnen die Lösung drei zentrale Komponenten: die geringe Anzahl von Lines of Code (LOC), der Least-Privilege-Ansatz und das Copy-on-Write-Verfahren. Alle drei Elemente sind darauf ausgerichtet, die potenzielle Angriffsfläche auf ein Minimum zu reduzieren.

Erstens wird dies durch die minimale Anzahl von Codezeilen realisiert. Denn es liegt auf der Hand, dass mit einer höheren Anzahl von Codezeilen auch die Gefahr potenzieller Schwachstellen steigt, weil jede einzelne Codezeile letztendlich einen möglichen Angriffspunkt darstellt.

Nach dem Least-Privilege-Konzept werden in der Micro-VM immer nur diejenigen Systemressourcen wie Netzwerkservices oder Files verfügbar gemacht, die für einen bestimmten Prozess erforderlich sind. Sobald dieser Prozess beendet ist, zerstört sich die Micro-VM selbst – und zwar mit der gesamten Malware, die sie unter Umständen enthält.

Drittens werden im sogenannten Copy-on-Write-Verfahren alle erforderlichen Ressourcen und Daten geklont in der Micro-VM im temporären Speicher bereitgestellt. Das heißt, schadhafte Änderungen können auch nur isoliert in der Micro-VM durchgeführt werden. Damit haben sie keinerlei Auswirkung auf das Host-System und können sich auch nicht ausbreiten.

Funktions-Modell der Micro-Virtualisierung



Quelle: Bromium

Hardware-Virtualisierung bringt zusätzliche Sicherheit

Auch wenn die Micro-Virtualisierung im Prinzip das Sandboxing-Konzept aufgreift, so basiert sie doch auf einem völlig neuen technischen Fundament. Ein zentraler Unterschied liegt darin, dass Sandboxing eine softwarebasierte Lösung ist, während Micro-Virtualisierung im Prozessor und damit in der Hardware stattfindet. Das bedeutet auch, dass im Falle einer Sandbox-Software-Kompromittierung als einziger Schutzmechanismus die Standard-Betriebssystemsicherheit übrig bleibt. Die Hardware-Virtualisierung bringt im Gegensatz dazu ein erhebliches Sicherheitsplus, denn eine CPU-Kompromittierung dürfte für einen potenziellen Angreifer einen erheblichen Aufwand bedeuten.

Durch die Isolierung aller potenziell gefährlichen Prozesse erreicht Malware nie das eigentliche Betriebssystem und kann somit weder lokal noch im Netzwerk Schaden anrichten oder zu einem Datendiebstahl führen. Auch Systeme, die beispielsweise nicht auf aktuellem Upgrade- oder Patch-Stand sind, bleiben damit umfassend geschützt. Darüber hinaus macht die Lösung kein zeitaufwendiges und kostenintensives Neuaufsetzen von kompromittierten Rechnern erforderlich, da eine mögliche Schädigung auf die jeweilige Micro-VM beschränkt ist und diese automatisch nach Beendigung einer Aktivität, beispielsweise dem Schließen eines Files oder Browser-Tabs, gelöscht wird. Eine Ausbreitung von Schadcode ist damit ausgeschlossen.

Nicht zuletzt läuft die Lösung im Hintergrund, ohne dass der Nutzer Einschränkungen hinsichtlich Benutzerkomfort oder Systemperformance hat. Bei den heutigen Rechnergenerationen erfolgt das Laden einer Micro-VM in rund 20 Millisekunden.