Blick in die Zukunft der Virtualisierung

Cyberangriffe werden immer komplexer und sind oft selbst von Sicherheitsverantwortlichen nicht mehr zu durchschauen. Welche Entwicklungen im Bereich der IT-Sicherheit könnten Abhilfe schaffen? Zusammen mit dem Institut für Technikfolgenabschätzung und Systemanalyse (ITAS) wirft funkschau einen Blick in die Zukunft.

Viren und Trojaner sind seit jeher Probleme für Computer-Anwender, egal ob privat oder dienstlich. Dabei werden Angriffe zunehmend komplexer und können gerade Unternehmen etliche Millionen kosten, von Folgeschäden wie Image-Einbußen ganz zu schweigen.

Wie könnte eine Lösung aussehen?

Ein uneingeschränkt sicheres Betriebssystem wird aufgrund der Komplexität und Ausbaubarkeit des Systems nicht umsetzbar sein; auch der Ansatz, Computer von Grund auf neu zu entwerfen ist nicht sinnvoll, da bestehende Anwendungen und Daten schlichtweg nicht mehr verwendet werden könnten. Die ständige Verwendung einer separaten Maschine, beispielsweise eines Smartcard-Lesers mit Display, ist allenfalls praktikabel, wenn höchste Sicherheit gefordert ist, wie bei militärischen Aktivitäten.

Eine mögliche Lösung, die auch von den Forschern des ITAS verfolgt wird, ist der Einsatz von Hypervisoren. Diese sorgen dafür, dass ein Betriebssystem nur mit der virtuellen Hardware kommuniziert, die ihm vom Hypervisor zur Verfügung gestellt wird. Das System wiederum ist unterteilt in verschiedene Bereiche (so genannte Compartments), die jeweils über ein eigenes Betriebssystem verfügen und komplett von den anderen Compartments isoliert sind.

Hypervisoren müssen also einen zuverlässigen Schutz bieten, selbst wenn ein Compartment mit Schadsoftware infiziert ist. Anwender sollen damit in der Lage sein, beliebige Webseiten zu besuchen oder Programme zu testen, ohne ein Risiko einzugehen. Korrumpierte Bereiche werden einfach gelöscht und neu installiert.

Rechte und Policies

Darüber hinaus soll die Möglichkeit, Rechte und Policies frei zu vergeben, die Sicherheit, aber auch die Usability zusätzlich erhöhen. Das Ziel ist, dass Nutzer und Administratoren frei Compartments kreieren können, die jedes Betriebssystem beinhalten, das sie haben möchten. Eine Firma könnte Rechte an einigen Compartments erhalten, während Nutzer die vollen Rechte an anderen bekommen. Die Idee ist, dass ein Privatnutzer einen Hypervisor für jeden Zweck verwenden kann, vom Isolieren sensibler Daten bis zum Betrachten riskanter Programme.

Ein Beispiel: Ein Arbeitgeber ist Eigentümer eines Laptops. Der Angestellte erhält

Was ist das ITAS?

Das Institut für Technikfolgenabschätzung und Systemanalyse (ITAS) erarbeitet Wissen über die Folgen und Gestaltungsoptionen technischer Entwicklungen. Es erstellt Analysen und Bewertungen technischer Systeme in interdisziplinärer Zusammenarbeit. Das ITAS berät unter anderem den Deutschen Bundestag und das Europaparlament. Das Institut ist Teil des KIT, des Zusammenschlusses der Universität Karlsruhe mit dem Forschungszentrum Karlsruhe.

funkschau Expertenkommentar

Bild: ITAS

Arnd Weber, Senior Researcher beim Institut für Technikfolgenabschätzung und Systemanalyse

Schutz gegen aufwendige Angriffe erfordert sichere Hard- und Software

Die Speicherung verschlüsselter Informationen zur späteren Dechiffrierung durch die NSA, der aufwendig konstruierte Stuxnet-Wurm und die langfristig vorbereitete Nutzung von Zero-Day-Exploits durch staatliche Stellen zeigen, dass unsere IT-Infrastruktur tiefgreifenden Angriffsmöglichkeiten durch staatliche, aber auch durch potente private und kriminelle Organisationen ausgesetzt ist. Die globalen Wertschöpfungsketten in Hard- und Software eröffnen vielfältige Möglichkeiten, versteckte Funktionen einzubauen. Auf die Frage, was er zum Schutz vertraulicher Daten heute empfehlen kann, konnte der US-Sicherheitsspezialist Bruce Schneier deshalb kürzlich nur noch sagen: „I have no idea."

Heute können Hersteller im harten Preiswettbewerb von sich aus nur inkrementell Ansätze zur Erhöhung der Sicherheit berücksichtigen. Wenn wir mittelfristig sensible Informationen zuverlässig isolieren und kommunizieren wollen, müssen letztlich alle Computer, Smartphones, etc. intensiv auf Fehlerfreiheit getestet, wenn nicht sogar bewiesenermaßen sicher sein. Das US-Militär erforscht mit dem CRASH-Programm genau diesen Pfad. Die europäischen Regierungen könnten beschleunigend eingreifen, wenn sie Anforderungen stellen würden, wie gut Computer sein müssen, wenn man sie in Bereichen wie E-Health, E-Banking oder im Smart-Grid verwenden will. Was ist unser Äquivalent zum CRASH-Programm?

volle Rechte in Bezug auf den Hypervisor, aber nicht in Bezug auf jedes Compartment. Die Firma erhält volle Rechte in Bezug auf ihr Compartment und verlässt sich insofern auf den Hypervisor. Der Angestellte kann das ganze Firmen-Compartment löschen, aber die Rechte und Policies dieses Compartments nicht ändern. Derselbe Mechanismus könnte für Digital-Rights-Management (DRM) genutzt werden und auch für Homebanking oder um private Daten vertraulich zu halten.

Architektur und Trusted-Computing

Elementar für die korrekte Funktion des Hypervisors ist gegen Manipulation geschützte Hardware, die verhindert, dass der Hypervisor von außen verändert werden kann. Die Hardware zu kontrollieren ist beispielsweise über einen zusätzlichen Chip, dem Trusted-Computing-Module (TPM), möglich, das sämtliche Komponenten beim Booten validiert und bei Änderungen warnt.

Wesentliche Charakteristik eines solchen Systems ist, dass der Eigentümer des Hypervisors alle Rechte in Bezug auf die Hardware und den Hypervisor behält und somit eine nicht richtig funktionierende Fassung eines Betriebssystems oder ein ungewolltes DRM-System löschen kann, ohne dass Reste im Hypervisor bleiben. Auch der Eigentümer eines Compartments hat alle Rechte an diesem. Die beiden Eigentümer müssen aber nicht identisch sein.

Fazit

Erste Prototypen dieses Systems wurden bereits entwickelt und haben bewiesen, dass Hypervisoren in Kombination mit dem Trusted-Platform-Module hilfreiche Sicherheits-Anker sind. Ein Video findet sich auf www.open-hypervisor.org/index.php/HPvisor/news/31/ .

Die Herausforderung besteht nun zum einen darin, einen Hypervisor zu entwickeln, der zuverlässig Schadprogramme isoliert, als auch eine Nutzerschnittstelle bereitzustellen, die eine unkomplizierte und auch für den privaten Anwender verständliche Nutzung ermöglicht. Eine Investition, die sich lohnen könnte, schließlich könnte der Ansatz nicht nur für PCs, sondern auch für Server und mobile Geräte genutzt werden. (AP)

Arnd Weber
Senior Researcher, KIT-ITAS

Axel Pomper,
Redaktion funkschau

Quelle: Der Artikel basiert auf dem Whitepaper „Verifizierte Virtualisierung für mehr Sicherheit und Komfort“ von Arnd Weber und Dirk Weber