Betriebssystemsicherheit:

Ein digitaler Airbag?!

Für den geneigten Autofahrer ist es bereits ein Automatismus, den Gurt anzulegen, die richtige Sitzposition einzunehmen und die Spiegel korrekt zu justieren. Durch die rasante Entwicklung sind es aber zum größten Teil die kleinen technischen Raffinessen wie Anti-Blockiersystem, ESP oder der Airbag, die die Sicherheit erhöhen. Sobald es brenzlig wird, reagieren diese Sicherheitssysteme und bewahren uns vor großen Schäden. Mechanismen mit so großem Potenzial, Werte zu beschützen, werden auch für heutige Betriebssysteme benötigt. Kleine Helfer wie Anti-Viren-Software und Firewalls reichen nicht mehr aus.

Eine Vielzahl von Sicherheitstools unterstützt Anwender dabei, Schädlinge abzuwehren oder aufzuspüren. Virenscanner, Firewall und Anti-Malware-Tools müssen aber auch gut konfiguriert und gewartet werden. Sie bieten keine automatisierte Sicherheit. Während Autofahrer im Straßenverkehr selten direkt angegriffen werden, sind permanente Angriffe auf alle Rechnersysteme, die an das Internet angeschlossen werden, in der IT-Welt alltäglich. Heutzutage dauert es im Durchschnitt keine sechs Minuten, bis ein ungeschütztes Rechnersystem von Malware befallen wird.

Vergleich: IT-Sicherheit – Sicherheit im Auto

Die Problematik verschärft sich zusätzlich dadurch, dass die Entwicklung im IT-Bereich um ein Vielfaches schneller voranschreitet als in der Automobilindustrie. So steigt die Komplexität etablierter Betriebssysteme permanent, um neuen Anforderungen der Informations- und Wissensgesellschaft gerecht zu werden. Gleichzeitig aber wächst auch ihre Fehleranfälligkeit, und zwar überproportional. Diesen Umstand unterstreicht die tägliche Masse an Patches und Sicherheitsupdates.

Das eigene Auto lässt sich an Farbe, Marke, Form und Nummernschild jederzeit gut erkennen; letztendlich ist der verwendete Schlüssel das Mittel zur Authentifizierung des Autos.
In der IT-Welt nutzen wir zwar Passwörter oder Sicherheitstoken, um uns gegenüber Rechnersystemen zu authentifizieren. Aber: Die Rechnersysteme ihrerseits authentifizieren sich nicht uns gegenüber. Das entspricht einer Situation im Verkehr, in welcher der Fahrer nicht feststellen kann, ob er im richtigen Auto sitzt und ob der Wagen auch anhält, wenn er das Bremspedal tritt. Es müssen Lösungen geschaffen werden, die das digitale Leben sehr gut schützen.

Definition und Funktionsweise von Trusted Computing

Trusted Computing ist der Begriff für die Idee, Computertechnologie grundsätzlich vertrauenswürdiger zu machen. Forciert werden die damit einhergehenden Sicherheitstechnologien von einem Industriekonsortium mit über 120 internationalen Mitgliedern. Die Ergebnisse dieser Zusammenarbeit sind offene Spezifikationen, die grundsätzlich zum Ziel haben, die Basis für die vertrauenswürdige IT zu bilden. Insbesondere die Sicherheit verteilter Anwendungen soll mit wirtschaftlich vertretbarem Aufwand verbessert werden, d. h. es soll keine massive Veränderung existierender Hard- bzw. Software notwendig sein. Eine der Hauptideen ist die Nutzung einer manipulationssicheren Hardware-Komponente, des sog. Trusted Platform Module (TPM). Sie soll softwarebasierten Angriffen entgegenwirken. Die TPM-Spezifikationen wurden bereits von vielen Herstellern umgesetzt. Sie sind aktuell in über 200 Millionen Rechnersystemen zu finden. Fast jedes aktuelle Notebook, das Sie erwerben, beinhaltet einen solchen Sicherheitschip.

Das TPM wirkt als vertrauenswürdiger Anker in einem Rechnersystem (Root of Trust). Beginnend mit dem Startvorgang werden alle Hardwareelemente und Softwarekomponenten (BIOS, Betriebssystem, Anwendungsprogramme etc.) mit Hilfe von Hashfunktionen gemessen und ihre Zustände im Platform Configuration Register (PCR) des TPM gespeichert. Die Systemkonfiguration des Rechnersystems ist also jederzeit komplett mess- und damit auch überprüfbar. In der Automobilindustrie entspräche dem die Arbeit eines Kontrolleurs, der die gesamte Montage eines Wagens protokolliert und hinterher anhand einer zertifizierten Liste von Kontrollnummern aller Teile (z. B. des Fahrgestells) die „Integrität" des Autos beweisen kann. Wird ein Teil ersetzt, wäre das Auto nicht mehr im Originalzustand und im Vergleich mit der Liste nicht mehr vertrauenswürdig.

Die Systemkonfigurationsüberprüfung durch das TPM erfolgt in identischer Weise. Damit können sich Rechnersysteme gegenüber einem Benutzer oder anderen Rechnersystemen hinsichtlich ihrer Systemkonfiguration „ausweisen". Dieser Vorgang wird Attestation genannt.

Außerdem bietet das TPM die Möglichkeit, Daten zu versiegeln und vertraulich zu speichern. Dabei werden die Daten während der Verschlüsselung an die Systemkonfiguration gebunden. Dieser Vorgang wird Sealing genannt. Er stellt sicher, dass auf versiegelte Daten nur wieder zugegriffen werden kann, wenn sich das Rechnersystem in einem bekannten Zustand (Systemkonfiguration) befindet. Dem entspricht im übertragenen Sinn die Möglichkeit, genau zu prüfen, ob z. B. das Bremssystem unverändert und damit funktionsfähig ist.

Die Sicherheitsplattform als Teil der Trusted-Computing-Idee

Trusted-Computing-Funktionen lassen sich bisher nur als Werkzeuge verwenden, um mehr Vertrauenswürdigkeit in Rechnersystemen zu generieren. Der Begriff steht allerdings nicht nur für Sicherheitschips wie das TPM. Es ist vielmehr ein Oberbegriff für sämtliche Funktionen, die mit Hilfe neuer Methoden größere Sicherheit herstellen. Ein TPM-Modul allein bringt noch keine höhere Sicherheit, sondern ist im Prinzip ein passives Bauteil, welches Sicherheitsdienste bietet. Um es vertrauenswürdig zu nutzen, wird eine Sicherheitsplattform benötigt, die genau diese Eigenschaft garantiert. In der Analogie sind dies die Mitarbeiter, die den Aufbau des Wagens überwachen, zusammen mit den Testingenieuren, die die Echtheit und Funktionstüchtigkeit überprüfen. In der IT entsteht auf diese Weise eine betriebssystemähnliche Sicherheitsplattform.

Aktuelle Betriebssysteme können nicht als Sicherheitsplattform genutzt werden, da sie durch ihren monolithischen Aufbau einfach zu kompromittieren sind, wobei Viren und Trojaner vertrauenswürdige Zustände vortäuschen können, die nicht den realen Zuständen entsprechen. Eine Sicherheitsplattform setzt somit oberhalb der Hardware und unterhalb der herkömmlichen Betriebssysteme an und hat die Aufgabe, selbst möglichst unanfällig gegen Angriffe zu sein und auf dieser Grundlage sicherheitskritische Vorgänge zu kontrollieren.

Um diese Vorgaben zu erfüllen, sollte eine Sicherheitsplattform aus einer sehr geringen Codebasis bestehen und weit weniger komplex sein als etablierte Betriebssysteme. Diese „Minimalisierung" senkt die Fehlerwahrscheinlichkeit wesentlich und erhöht gleichzeitig die Vertrauenswürdigkeit, nicht zuletzt, da bei dieser Codebasis auch eine Zertifizierung beispielsweise nach Common Criteria durchgeführt werden kann. Durch Virtualisierungstechniken ist eine Sicherheitsplattform in der Lage, mehrere Applikationen und/oder Betriebssysteme parallel, vollständig in ihren Speicherbereichen getrennt auszuführen.

Es ist also möglich, einzelne sichere Applikationen in sogenannten Compartments – d.h. vollständig vom etablierten Betriebssystem abgeschottet – parallel auszuführen. Die Vertrauenswürdigkeit der Applikationen wird durch die Messmöglichkeit des TPM überprüfbar. Mit anderen Worten: Auch wenn das etablierte Betriebssystem durch Malware kompromittiert ist, droht keine Gefahr, da alle sicherheitskritischen Vorgänge in isolierten Bereichen von sicheren Anwendungen ausgeführt werden. Die Compartments können entweder reine sichere Applikationen enthalten, die an die Sicherheitsplattform angepasst wurden, oder schlanke Betriebssysteme mit Standardapplikationen. Im zweiten Fall misst das TPM das Betriebssystem zusammen mit der Anwendung, um jederzeit die Integrität nachweisen zu können (siehe Abb. 1).

Eine Sicherheitsplattform in Kombination mit der Trusted-Computing-Technologie (TPM und dessen Funktionalitäten) bietet ein breites Spektrum an Gestaltungsmöglichkeiten für vertrauenswürdige Anwendungen. Auf diese Weise lassen sich z. B. Endbenutzersysteme einrichten, die Daten sicher verwalten und speichern. Schadsoftware kommt gar nicht erst in Berührung mit sicherheitsrelevanten Daten. Server- und Clientsysteme lassen sich zuverlässig authentifizieren; so kann beispielsweise der Bank-Server beim Online-Banking jederzeit seine Identität nachweisen, was die Gewähr bietet, dass die Bankdaten vertrauenswürdig verarbeitet werden.

Ein Airbag für Betriebssysteme

Das Forschungs- und Entwicklungsprojekt EMSCB (European Multilaterally Secure Computing Base), an dem mehrere Hochschulen und IT-Sicherheitsfirmen beteiligt waren, stellt mit Turaya bereits eine vertrauenswürdige, faire und offene Sicherheitsplattform zur Verfügung, die auf Trusted-Computing-Technologie aufbaut. Sie bietet zusätzlich die Möglichkeit, Rechte und Regeln durchzusetzen (Policy Enforcement), wodurch sich neue Möglichkeiten des digitalen Rechtemanagements ergeben. Dadurch lassen sich klassifizierte Dokumente auf verschiedenen Rechnersystemen unterschiedlich behandeln: Beispielsweise können sie mit den Systemen einer Gruppe angeschaut und gedruckt, mit anderen lediglich betrachtet werden.

Ziel von Turaya ist, eine Sicherheitsplattform mit offener Architektur und geeigneten Schnittstellen zu schaffen, die als Basis für vertrauenswürdige IT-Systeme dient – sozusagen ein Airbag für vertrauenswürdige IT-Systeme. Sie lässt sich an die Erfordernisse von PCs, PDAs, Mobiltelefonen sowie Embedded-Systemen anpassen und ermöglicht innovative Geschäftsmodelle.

Dass das „Airbag-Konzept" eine Lösung für aktuelle und zukünftige Bedrohungen darstellt, lässt sich daraus ableiten, dass dieser Ansatz jetzt auch in den USA und in anderen Teilen der Welt verfolgt wird. Deutschland hat ähnlich wie in der Automobilindustrie auf diesem Feld einen technologischen Vorsprung, den es auszubauen gilt, indem die Industrie auf die Forschungsergebnisse aufbaut und sie in ihre Produkte integriert.

Weitere Informationen über das Projekt finden Sie unter www.internet-sicherheit.de oder www.turaya.de.

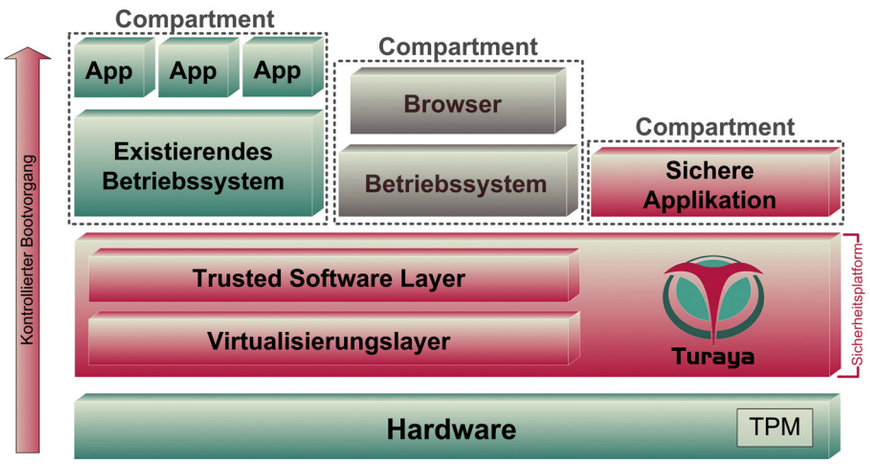

Abb. 1: Systemarchitektur der Sicherheitsplattform Turaya

Autoren

Prof. Dr. Norbert Pohlmann ist Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen (www.internet-sicherheit.de)

Markus Linnemann ist Geschäftsführer des Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen.