Von der Perimeter Sicherheit zum Enterprise Rights Management

Die Anforderungen an die Netzsicherheit haben sich in den letzten Jahren dramatisch geändert und werden sich in der Zukunft noch schneller ändern. Aus diesem Grund müssen neue zusätzliche IT-Sicherheitsmechanismen für eine angemessene IT-Sicherheit von Grenzen sorgen.

Perimeter Sicherheit

In den ersten Jahren des Internets haben sich Unternehmen ans Internet angeschlossen, um am E-Mail- und Web-System teilhaben zu können. Zusätzlich haben die Unternehmen die Möglichkeit genutzt, mit ihren Niederlassungen und anderen Organisationen über das Verbundnetz Internet einfach, schnell und preisgünstig kommunizieren zu können.
Das Abwehrmodell sah so aus, dass verhindert werden musste, dass Fremde aus dem Internet auf das eigene Unternehmensnetz zugreifen konnten und dass die ausgetauschten Daten nicht von anderen gelesen und manipuliert werden konnten. Die Sicherheitskonzepte folgten der Idee der Perimeter Sicherheit, d.h., die Organisationen haben sich durch zentrale Firewalls und VPNs von den anderen abgegrenzt.
Ein Firewall-System hat dabei das Ziel, die Kommunikation auf das Notwendigste für den eigentlichen Geschäftszweck des Unternehmens zu reduzieren. Es gilt zu definieren, welche Rechner, bzw. Personen zu welcher Zeit ins Internet dürfen und müssen, oder welche Internet-Dienste wirklich gebraucht werden [1].
Die IT-Sicherheit der Datenkommunikation von Niederlassungen über das Internet wird mit Hilfe von VPNs abgesichert. Dabei spielt der IPSec-Standard eine besondere Rolle. IPSec ergänzt das bestehende IPv4 um folgende Sicherheitsfunktionen: Jedes IP-Paket kann verschlüsselt sowie gegen Manipulation und Wiedereinspielung geschützt werden. Außerdem kann die IP-Kommunikation gegen Verkehrsflussanalyse geschützt und die Kommunikationspartner (Personen oder VPN-Gateways) authentisiert werden [2].

Vor welchen zusätzlichen Bedrohungen müssen wir uns heute schützen?

Dadurch, dass immer mehr PCs ans Internet angeschlossen sind, haben sich die Angriffsmodelle sehr stark verändert. Viele Angriffe finden über die erlaubte Firewall-Kommunikation auf der Anwendungsebene statt! Andererseits können die PCs, Notebooks, usw. zunehmend über Funkschnittstellen, wie GSM, UMTS, oder WLAN/Hotspot,an der zentralen Firewall vorbei mit dem Internet kommunizieren. Diese sogenannten Hintertüren (Back Door) stellen ein besonderes Risiko in Unternehmen dar [3].
Diese Rechnersysteme befinden sich wegen der erhöhten Mobilität der Mitarbeiter außerhalb der Kontrolle der Firmen und können kompromittiert werden! Beispiele sind

Außendienstmitarbeiter die ihre Rechnersysteme in wechselnden Umgebungen mit unterschiedlichen Sicherheitsanforderungen nutzen, Heimarbeiter die ihre PCs auch für private Zwecke verwenden und Mitarbeiter die ihre Firmen-Notebooks mit nach Hause nehmen. Dieser Trend setzt sich in der Zukunft noch schneller fort.

Sicherheitsplattform und Trusted-Computing

Die Angriffsmodelle haben sich im Laufe der Zeit verändert, z.B. ist die Entwicklung von verteilten Softwareangriffen sehr stark gestiegen. Dadurch, dass die Betriebssysteme und Anwendungen immer komplexer und dadurch die Anzahl der Softwarefehler immer größer werden, haben sich Viren, Würmer und Trojanische Pferde immer erfolgreicher, auch über Firewall- und durch VPN-Systeme, verteilen können.

Trusted Computing ist der Begriff für die Idee, IT-Technologie grundsätzlich vertrauenswürdiger zu machen. Eines der Hauptkonzepte ist die Nutzung einer manipulationssicheren Hardware-Komponente, dam sog. Trusted Platform Module (TPM). Das TPM mit seinen Funktionen soll softwarebasierten Angriffen entgegenwirken. Mit Hilfe eines TPMs kann die Systemkonfiguration des Rechnersystems gemessen und damit auch überprüfbar gemacht werden. Für die vertrauenswürdige Nutzung der Komponente, wird eine Sicherheitsplattform benötigt. Eine Sicherheitsplattform setzt 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 und die IT-Systeme robuster zu machen. 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. Durch die zusätzliche Nutzung einer Virtualisierungstechnik ist eine Sicherheitsplattform in der Lage, mehrere Applikationen und/oder Betriebssysteme parallel und vollständig in ihren Speicherbereichen getrennt auszuführen. Es ist also möglich, einzelne sichere Applikationen in so genannten Compartments – d.h. vollständig vom etablierten Betriebssystem abgeschottet – parallel auszuführen. Die Vertrauenswürdigkeit der Applikationen wird durch die Messmöglichkeit des TPMs 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. Das TPM misst das jeweilige Compartment, um jederzeit die Integrität nachweisen zu können [4].

Enterprise Rights Management (ERM)

Durch ein entsprechendes Rechte- und Regelmanagement auf der Basis einer solchen Sicherheitsplattform ist IT-Sicherheit auf Rechnersystemen im Unternehmensumfeld vertrauenswürdig realisierbar [5]. Die Rechnersysteme sind selbst so robust gegen Angriffe aus dem Internet, dass die Firewall-Systeme eine untergeordnete Rolle in der Zukunft spielen werden.

[1] N. Pohlmann: "Firewall-Systeme - Sicherheit für Internet und Intranet, E-Mail-Security, Virtual Private Network, Intrution Detection-System, Personal Firewalls", MITP-Verlag, Bonn 2003

[2] M. Campo, N. Pohlmann: "Virtual Private Network (VPN)“, MITP-Verlag, Bonn 2003

[3] N. Pohlmann: "Möglichkeiten und Grenzen von Firewall-Systemen". In Proceedings der GI-Fachgruppe Verlässliche IT-Systeme Konferenz - Kommunikationssicherheit im Zeichen des Internet, Hrsg.: Patrick Horster, Vieweg Verlag, März 2001

[4] M. Linnemann, N. Pohlmann: „Turaya - Die offene Trusted Computing Sicherheitsplattform", in "Open Source Jahrbuch 2007", Hrsg.: B. Lutterbeck, M. Bärwolff, R. Gehring, Lehmanns Media, Berlin, 2007

[5] N. Heibel, M. Linnemann, N. Pohlmann: „Dokumente sicher im Griff: Sicheres Enterprise Rights Management“, IT SECURITY, März/April, 02/2008