Von RECHTSwegen sicher

Enterprise Rights Management mit einer Sicherheitsplattform

Markus Linnemann
markus.linnemann@internet-sicherheit.de

Prof. Dr. Norbert Pohlmann
norbert.pohlmann@informatik.fh-gelsenkirchen.de

Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen
Neidenburger Str. 43, D - 45877 Gelsenkirchen
www.internet-sicherheit.de

1993 bekam das TGV Konsortium in Nordkorea den Zuschlag für den Kauf von deren Bahntechnik. Das ICE-Konsortium um Siemens hatte das Nachsehen. Es war offenkundig, dass das TGV-Konsortium die Angebotshöhe des Konkurrenten durch Spionage ermitteln und ihn somit leicht überbieten konnte. Wirtschaftsspionage ist nach wie vor an der Tagesordnung und durch die weltumspannende Funktion digitaler und vernetzter Dienste noch einfacher geworden.

Die Übermittlung der Angebote erfolgt heute digital und der Schutz von Wissen und Eigentum ist für den wirtschaftlichen Erfolg eines Unternehmens eine zentrale Komponente. Egal, ob es sich um Erfindungen, Angebote oder Konstruktionsdaten handelt, ein Verlust dieser Informationen führt zu wirtschaftlichem Schaden. Enterprise Rights Management Systeme bieten Lösungsansätze, um die digitalen Werte/Dokumente eines Unternehmens zu schützen. In der bisherigen Ausprägung bieten sie aber keine optimale Sicherheit. Aus der Forschung kommt der entscheidende Ansatz, wie diese Systeme den Ansprüchen gerecht werden können.

1 Einleitung

Die Informationsverarbeitung in modernen Unternehmen erfolgt in verteilten und heterogenen IT-Systemen und -Netzen. Die Wartung und der Betrieb laufen zumeist unabhängig voneinander ab und die Konfiguration folgt unterschiedlichen Maßstäben.

Die Durchsetzung von Sicherheitsrichtlinien zur zuverlässigen Verarbeitung der eigenen Informationen und Daten birgt in diesem Umfeld eine Herausforderung, die mit herkömmlichen Sicherheitswerkzeugen kaum zu bewältigen ist. Der Schutz vor unkontrollierter Weitergabe von Unternehmens- und Behördendaten wird immer schwieriger. Aber nicht nur die eigene IT rückt dabei in den Vordergrund der Sicherheitsbetrachtung. Im Zeitalter des Outsourcing hängt der wirtschaftliche Erfolg in gleicher Weise von der Zuverlässigkeit und Sicherheit anderer IT-Systeme ab, beispielsweise der Zulieferer und Dienstleister, welche immer enger in die eigenen Unternehmensprozesse eingebunden sind.

Der zumeist betriebene „globale“ Schutz des Netzes durch die Absicherung der Transport-, bzw. Kommunikationswege, beispielsweise durch den netzübergreifenden Einsatz von VPN (Virtual Private Network) ist nicht ausreichend, da sowohl die Kommunikationswege angreifbar sind, als auch Gefahren aus den eigenen Reihen drohen.

Seit einigen Jahren werden als Lösung dieses Problems Enterprise Rights Management Softwarelösungen angeboten. Bei diesen Systemen wird die Sicherheit nicht mehr an die Wege der Daten, sondern an die Daten selbst gebunden. Dieses Konzept ermöglicht die Kontrolle von Daten sowohl im eigenen, als auch in fremden Netzen.

Aktuelle Computersysteme kämpfen jedoch mit einem grundsätzlichen Problem. Betriebssysteme, unabhängig, ob sie aus der Linux-, der Windows- oder der Apple-Welt stammen sind monolithisch aufgebaut. Die Menge an Funktionen und somit die riesige Anzahl von Codezeilen ermöglichen jede Menge Fehler im System – immer wieder eindrucksvoll durch die Vielzahl an Sicherheitspatches belegt. Die Isolation von Prozessen ist nur unzureichend gewährleistet und die Allmächtigkeit des Betriebssystems bringt jeden erfolgreichen Angreifer in die Position, die Kontrolle über das gesamte System zu erlangen. Intelligente ERM-Lösungen können in diesem Fall keinen Vorteil mehr bieten, da mit der Kontrolle über das Betriebssystem auch die Kontrolle über alle Schlüssel, Applikationen und ERM-Lösungen an den Angreifer übergehen. Abhilfe für die beschriebenen Probleme schafft eine aus der Forschung stammende Lösung, die eine Sicherheitsplattform und den Einsatz der Trusted Computing Technologie umfasst.

2 Die Bedrohung

Die Art der Angriffe hat sich in den letzten Jahren verändert. Die größte Bedrohung für Unternehmensdaten geht vom eigenen Mitarbeiter aus. Hierbei muss es sich nicht zwingend um eine zielgerichtete kriminelle Aktion handeln. Kritische Unterlagen werden beispielsweise auf einem Netzwerkdrucker auf dem Büroflur ausgedruckt und dort vergessen. Sensible Daten gelangen also durch Unachtsamkeiten in falsche Hände. Sie werden an falsche Mail-Adressen gesendet, auf USB-Sticks oder Telefone geladen und verloren. Laut der <kes> Microsoft Sicherheitsstudie 2006 entsteht der größte Schaden im Unternehmen durch Irrtum und Nachlässigkeiten eigener Mitarbeiter. Erst an zweiter Stelle kommt Malware, wie Viren, Würmer und Trojaner. Auch die zweitplatzierte Gefahr hat immense Auswirkungen auf die Unternehmen, da als Folge der Malware die Kontrolle über das Rechnersystem zumeist von Angreifern übernommen wird.

3 Was ist ERM?

Definitionsvorschlag: ERM sorgt dafür, dass geschäftskritische Informationen nur nach vorgegebenen Regeln von den definierten Akteuren auf definierten Rechnersystemen eingesehen oder bearbeitet werden können. Daten wie Dokumente erhalten durch ERM eine mögliche Einschränkung in ihrer Verwendung. So kann beispielsweise das Ausdrucken oder das Weiterversenden von Daten reglementiert werden.

ERM ist ein relativ neuer technischer Ansatz um Informationsflusskontrolle auf sensitive elektronische Dokumente unternehmensweit und -übergreifend zu ermöglichen. Anwender können Zugriffsrechte für ihre Dokumente definieren und deren Durchsetzung erzwingen. Der Zugriff kann in Abhängigkeit von Rollen (z.B. „Finanzabteilung“), Nutzern („Margot Mus-

ter“) und Nutzergruppen („Steuerfahndung NRW“) erfolgen und wird in globalen oder lokalen Richtlinien („Policies“) festgehalten. ERM-Dokumente besitzen zusätzlich ein so genanntes Label, das die Policies enthält.

Der Schutz von Informationen wird durch ein ERM-System stark erhöht, da das Konzept keine Absicherung von Komponenten eines IT-Systems vorsieht, sondern den direkten Schutz einzelner Dokumente (Objekt-Sicherheit). Der Schutz ist also nicht mehr von der Sicherheit der unterschiedlichen Transportwege und im gewissen Maße der verarbeitenden Systeme abhängig.

Die Anforderungen an eine effektive Informationsflusskontrolle in einem ERM-System sind hoch: Jedes System *muss garantieren* können, dass es im Umgang mit Informationen vereinbarte Richtlinien einhält. Weder von eingefangener Schadsoftware, noch durch den Benutzer oder Betreiber des jeweiligen Systems darf die Vorgabe der Richtlinien ausgehebelt werden. So darf ein Zulieferer nicht in der Lage sein, die ihm für einen eingegrenzten Zweck bereitgestellten Daten anderweitig zu verwenden – auch wenn diese von der IT des Zulieferers verarbeitet werden.

Diese Vorgaben sind aufgrund der beschriebenen Fehleranfälligkeit und der gleichzeitigen Allmächtigkeit herkömmlicher Betriebssysteme durch aktuelle ERM-Systeme noch nicht erfüllbar. Sie sind bisher nur einsetzbar solange ein System noch nicht kompromittiert wurde, aber diese Voraussetzung besteht in den seltensten Fällen..

4 Sichere Informationsflusskontrolle

Eine sichere ERM-Lösung und IT-Infrastruktur muss zusätzliche Eigenschaften bieten, um eine wirklich vertrauenswürdige Informationsflusskontrolle zu bieten. Sollen alle Fehlerquellen und Sicherheitslücken eliminiert werden müssen folgende Ansprüche an das System gestellt werden:

- **Document Life-Cycle Protection**: Die garantierte Durchsetzung von dokumentenspezifischen Zugriffs- und Bearbeitungsregeln über Plattform- und Unternehmensgrenzen und über die gesamte Lebensdauer eines Dokumentes hinweg: Von der Erzeugung bis zur Vernichtung.
- **Überprüfbarkeit der verarbeitenden IT**: Nur IT-Systeme, die ihre Vertrauenswürdigkeit nachweisen können, erhalten Zugriff auf geschützte Dokumente.
- **Vertrauenswürdigkeit der verarbeitenden IT**: Vertrauenswürdige IT-Systeme bieten einerseits funktional eine richtlinienkonforme Verarbeitung der Dokumente und andererseits einen stark erhöhten Schutz gegen externe Manipulationen.

Da herkömmliche Systeme diesen Ansprüchen nicht gerecht werden können, wurde ein, vom BMWi gefördertes, dreijähriges Forschungsprojekt initiiert Ein Konsortium, bestehend aus dem Institut für Internet-Sicherheit der FH Gelsenkirchen, der Ruhr-Universität Bochum, der TU Dresden und den Firmen Sirrix AG und escrypt GmbH entwickelte dabei die Sicherheitsplattform Turaya.

5 Innovative Lösung

Um sensible Daten vor unrechtmäßigen Zugriffen zu schützen, ist eine geräte- und netzübergreifende Vertrauens- und Sicherheitsbasis für die Zukunft unabdingbar.

Die Sicherheitsplattform Turaya kann die Vertrauenswürdigkeit von Systemen nachweisbar machen. Mit Hilfe der Trusted Computing Technologie, die sich der Steigerung der Vertrauenswürdigkeit in Rechnersystemen und Netzen verschrieben hat, werden Rechnersysteme messbar. Durch eine kleine Hardwareerweiterung, wie sie aktuell in fast allen Laptops vom Werk ab verbaut ist, wird eine vertrauenswürdige Kette aller Komponenten in einem Rechnersystem aufgebaut.

Am häufigsten wird das so genannte Trusted Plattform Module (TPM) verwendet. Das TPM speichert unter anderem Messwerte die beim Starten eines Rechnersystems ermittelt werden. Jede Komponente wird vor der Ausführung gemessen und ein Hashwert ermittelt. So werden nacheinander das BIOS, der Bootloader, die Hardware und die Software gemessen. Diese Messwerte können beim nächsten Start verwendet werden, um Veränderungen der Systemkonfiguration festzustellen. Hierbei wird davon ausgegangen, dass ein Rechnersystem vertrauenswürdig ist, wenn es in einem bestimmten Zustand ist und dieser sich nicht verändert hat.

Im Gegensatz zu herkömmlichen ERM-Lösungen werden Sicherheitsrichtlinien bei Turaya nicht auf Anwendungsebene durchgesetzt, sondern in der Sicherheitsplattform, die zwischen Hardware und dem herkömmlichen Betriebssystem angesiedelt ist (vgl. Abbildung 1). Da die Sicherheitsplattform die Hardware kontrolliert, kann sichergestellt werden, dass weder das Betriebssystem noch die Anwendungen Richtlinien umgehen können.

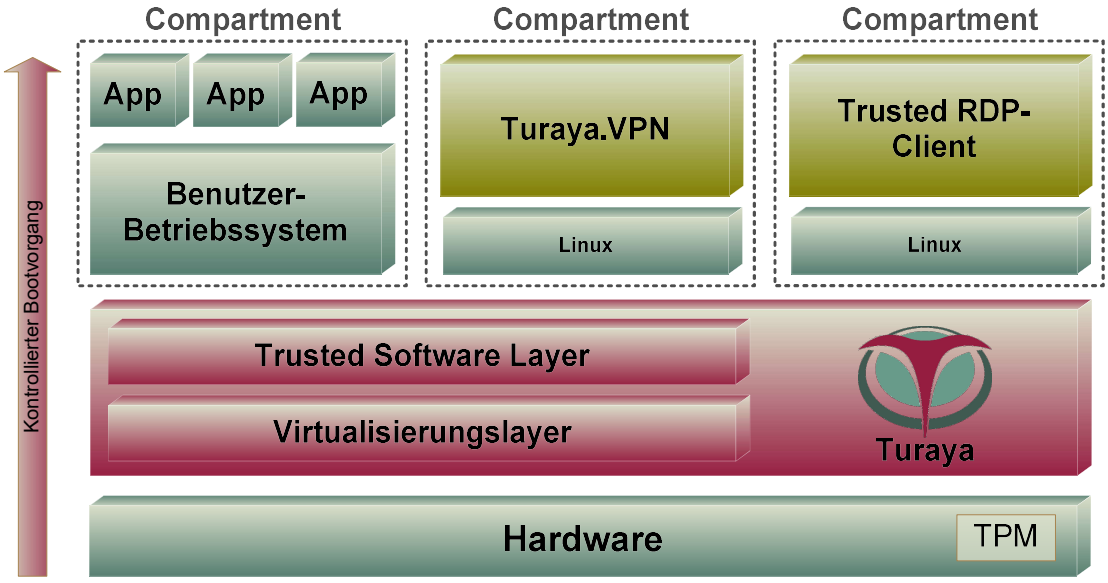

Abbildung 1: Turaya Architektur mit TPM-Support und ERM-Anwendung

Die Sicherheitsplattform nutzt Virtualisierungstechnologien, um mehrere voneinander isolierte Bereiche (Compartments) auszuführen, die vollständig voneinander isoliert werden können. Jedes dieser Compartments kann ein eigenes Betriebssystem, oder auch lediglich eine be-

stimmte Anwendung beinhalten. Die Compartments können mit entsprechenden Bereichen anderer IT-Systeme über eine abgesicherte Netzwerkleitung verbunden werden.

Manipulationen und Fehlkonfigurationen von lokalen und entfernten IT-Plattformen führen zum Verlust der Vertrauenswürdigkeit. Solchen Systemen wird der Zugang zu anderen IT-Systemen verwehrt und eine Verarbeitung von ERM geschützten Dokumenten untersagt. Auf diesem Wege lässt sich die Sicherheit von Dokumenten während ihres gesamten Lebenszyklus sicherstellen.

6 Sicheres ERM am Beispiel Turaya.WTS

Die Sicherheitsanwendung Turaya.WTS zeigt in Zusammenarbeit mit dem Projektpartner SAP, dass es möglich ist Dokumente vertrauensvoll zu reglementieren. Im SAP-Umfeld gehört die Ausgabe von Schulungsunterlagen für die unterschiedlichen Anwendungen, die im Firmenportfolio enthalten sind, zum Geschäftsmodell. Ein Zugangsschutz, bestehend aus dem Benutzernamen und einem Passwort ermöglichte bisher eine anwenderabhängige Zugangskontrolle für einen Terminalserver. Die Weitergabe dieser Daten kann jedoch zu Missbrauch führen. Außerdem können die Dokumente natürlich auch ausgedruckt, kopiert und in Papierform weiter verteilt werden.

Zur Vermeidung von wirtschaftlichem Schaden, muss eine gesicherte Informationsflusskontrolle installiert werden, die genau diese Missbrauchsmöglichkeiten verhindert. Die Anforderung umfasst, dass die Authentifizierung eines Nutzers nur dann möglich ist, wenn ein bestimmtes Rechnersystem verwendet wird, das keine Möglichkeit erhält die Dokumente über eine Schnittstelle weiterzugeben. Es gibt für dieses Szenario bereits reine Online-Lösungen die einen Terminalserver verwenden, aber eine Offlineverarbeitung benötigt ein System, wie Turaya.WTS.

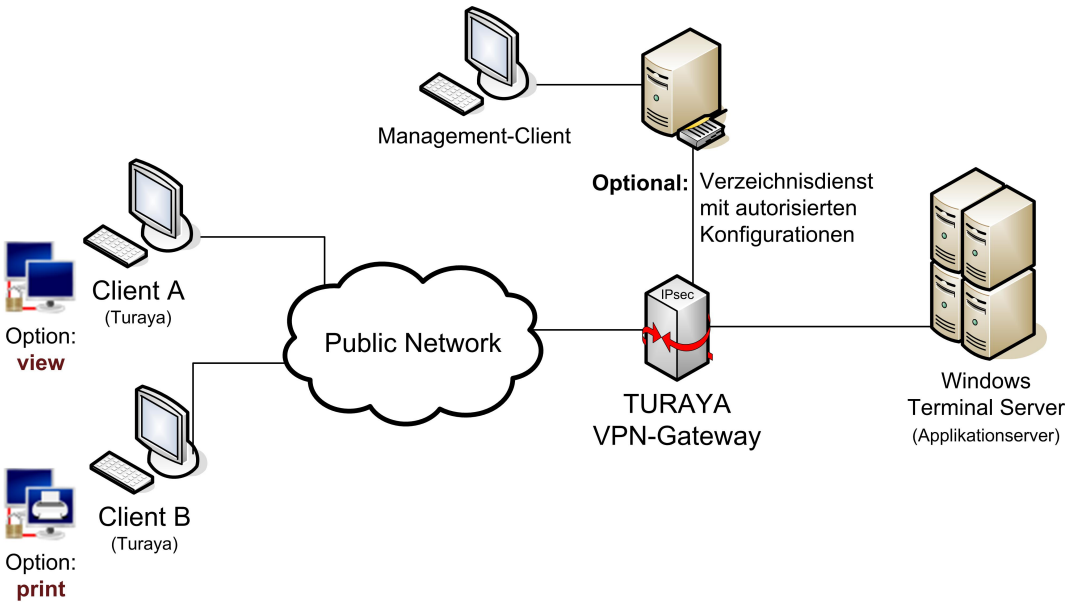

Abbildung 2: Über einen VPN Server wird bei vertrauenswürdiger Konfiguration ein Windows Terminal Server erreicht.

Im Beispiel Turaya.WTS baut der Anwender eine Verbindung zu einem entfernten Terminal-Server auf, um Dokumente zu bearbeitet. Im ersten Schritt benötigt Turaya einen Schlüssel für den Aufbau eines VPN-Tunnels zur sicheren Übertragung und Verbindung (vgl. Abb.2). Der Schlüssel ist an die Plattform gebunden. Er kann nur entschlüsselt und verwendet werden, wenn das Rechnersystem mit der korrekten Konfiguration gestartet wurde. Damit ist das System als vertrauenswürdig einzustufen. Der Schlüssel gelangt aber niemals in das herkömmliche unsichere Betriebssystem, sondern steht nur dem Compartment zur Verfügung, das die sichere VPN-Verbindung initiiert (vgl. Abb1, ERM-Compartment). Durch das etablierte VPN kann jetzt eine Verbindung zu dem Windows Terminal Server (WTS) aufgebaut werden und eine Anmeldung erfolgen.

Im Beispiel werden die Datenpakete von zwei Systemen mit zwei unterschiedlichen Policies(Optionen) versehen, die das Drucken verbieten (Option:View), bzw. zulassen (Option:Print). Der Sicherheitskern verarbeitet diese Anweisung und verweigert gegebenenfalls dem Compartment, das mit dem Terminal-Server verbunden ist (vgl. Abb.1:Trusted RDP-Client), den Zugriff auf den Drucker. Es können weitere Berechtigungen an Schlüssel und Daten gebunden werden die beispielsweise das Weiterleiten von Daten unterbinden.

Die gestellten Anforderungen an ein ERM-System sind damit erfüllt. Nur ein vorher definiertes und als vertrauenswürdig eingestuftes Rechnersystem erhält Zugang zu einem Dokumentenmanagementsystem, das in diesem Beispiel durch den WTS dargestellt wird. Außerdem können Berechtigungen (Optionen/Policies) für den gesamten Lebenszyklus an Dokumente gebunden werden (Objektsicherheit). Festgelegte Berechtigungen zu dem jeweiligen Vorgang werden vertrauensvoll durchgesetzt und können nur äußerst schwer manipuliert werden. Alle sicherheitskritischen Informationen, wie Schlüssel und Zugangsdaten sind vor dem unsicheren Benutzerbetriebssystem durch Isolation geschützt. Die Weitergabe von Zugangsdaten oder Schlüsseln ist zwecklos, da diese Informationen nur mit dem autorisierten Rechnersystem entschlüsselt werden können.

7 Fazit

ERM-Systeme sind ein hervorragendes Mittel für ein vertrauenswürdiges und sicheres Dokumentenmanagement. Sie vermögen das Know How und wichtige Informationen von Firmen in heterogenen Netzen zu schützen und verhindern sowohl den vorsätzlichen Angriff von Kriminellen, als auch viele Nachlässigkeiten von Mitarbeitern.

Bereits in aktuellen Systemen bietet ERM einen Mehrwert, wird aber durch unsichere korrumpierte Betriebssysteme ausgehebelt. Aus der Forschung kommt die entscheidende Ergänzung für diese Systeme in Form von Sicherheitsplattformen, wie Turaya, die Trusted Computing Technologien nutzen, um die Vertrauenswürdigkeit von Rechnersystemen zu beweisen.

Erstaunlich ist in diesem Zusammenhang die Tatsache, dass ERM-Systeme bisher vergleichsweise selten eingesetzt werden und Firmen nach wie vor auf globale reaktionäre Sicherheitsmechanismen für Ihre IT vertrauen. Firmen sollten darüber aufgeklärt werden, dass der Schutz der Unternehmensdaten mit ERM Systemen auf Basis einer Sicherheitsplattform stark verbessert werden kann und die Vorteile einer Sicherheitsplattform wie Turaya einen Quantensprung in der Absicherung von IT-Systemen und Anwendungen, wie ERM bedeuten.

www.internet-sicherheit.de

Literaturbox

[1] A.Alkassas, M.Hartmann, M.Linnemann, C.Stüble: „Rechte auf Reisen – Sicheres ERM mit Trusted Computing, in <kes>, 1/2008

[2] N.Heibel, M.Linnemann, N.Pohlmann: „Dokumente sicher im Griff – Sicheres Enterprise Rights Management mit Trusted Computing“, in IT SECURITY, 2/2008

[3] Lagebericht zur Informationssicherheit: <kes> Microsoft Sicherheitsstudie 2006, in <kes>, 4,6/2006

[4] M.Linnemann, N.Pohlmann: „Die vertrauenswürdige Sicherheitsplattform Turaya", in "DACH Security 2006", Hrsg.: Patrick Horster, syssec Verlag, 2006

[5] M.Linnemann, N.Pohlmann: „Schöne neue Welt – Die vertrauenswürdige Sicherheitsplattform Turaya“, in IT-Sicherheit 3-4/2006

[6] N.Pohlmann, M.Linnemann: Turaya – Die offene Trusted-Computing-Sicherheitsplattform; Open Source Jahrbuch 2007, Lehmann Media, S. 299 - 314

[7] A.Sadeghi, C. Stüble, N. Pohlmann: “European Multilateral Secure Computing Base - Open Trusted Computing for You and Me”, in Datenschutz und Datensicherheit (DUD) 9/2004, Vieweg Verlag (2004), pp. 548-554

[8] J.Wagley, “Sizing up Enterprise Rights Management”, in Security Management, September 2007