Analyse und Bewertung der IT-Sicherheit zukünftiger Betriebssysteme am Beispiel Microsoft Windows

Diplomarbeit

zur Erlangung des Grades eines Diplom-Ökonomen der Wirtschaftswissenschaftlichen Fakultät der Universität Hannover

vorgelegt von

Name: Grahl **Vorname: Holger**

[redacted] [redacted] [redacted]

Erstprüfer: Prof. Dr. Michael H. Breitner

Hannover, den 08.09.2005

Inhaltsverzeichnis

1. Einleitung und Begriffsklärung

Die folgende Arbeit soll den Bereich der IT-Sicherheit, bezogen auf die Betriebssystemssicherheit, behandeln. Dabei zeige ich zuerst was allgemein unter dem Begriff IT-Sicherheit verstanden wird, warum dies eines der wichtigsten Themen im IT-Bereich ist, und welche Rolle den Betriebssystemen dabei zukommt. Zu Beginn gehe ich auf die Entwicklung der Betriebssysteme ein und werde die wichtigsten aktuellen Betriebssysteme näher vorstellen. Der Hauptteil beschäftigt sich mit dem zur Zeit in der Entwicklung befindlichen Betriebssystem Windows Vista von Microsoft. Dabei sollen zuerst die neuen Elemente im Allgemeinen, und welche Anforderungen sie an die Hardware stellen, betrachtet werden. Anschließend werde ich die neuen Sicherheitselemente analysieren, welche Auswirkungen sie auf verschiedene Nutzer- und Interessengruppen haben können, wie sie konzipiert waren und wie die Umsetzung bisher erfolgt ist. Dabei soll auch gezeigt werden, welche Vorteile die neuen Elemente bringen können und mit welchen Nachteilen zu rechnen ist. Zum Abschluss gehe ich noch einmal näher auf den Einsatz von Betriebssystemen in Produktivumgebungen und den damit verbundenen speziellen Anforderungen ein. Dabei werde ich analysieren inwieweit diese bei der aktuellen Entwicklung berücksichtigt werden.

Welchen Stellenwert die IT-Sicherheit hat, lässt sich allein schon daran erkennen, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) eingerichtet wurde, welches sich mit dieser Thematik befasst und Informationen für Nutzer und Hersteller von Informationstechnik bereitstellt. Durch den verstärkten Einsatz von Informationstechnologie in Unternehmen, im öffentlichen und privaten Bereich, wächst auch die Abhängigkeit von der ordnungsgemäßen Funktion dieser Systeme. Während der Ausfall eines privaten Rechners meist nur wenig Schaden hervorruft, können beim Ausfall von Unternehmensrechnern größere Schäden entstehen.[1]

[1] Wie zum Beispiel der Ausfall des Flugverkehrs in GB http://www.heise.de/newsticker/meldung/47889 oder der große Blackout (Stromausfall) in den USA / Canada http://www.heise.de/newsticker/meldung/42234

Ein weiterer Punkt für die wachsende Bedeutung der IT-Sicherheit, liegt in der zunehmenden Vernetzung von Rechnern über immer leistungsfähigere Netze. Die Rechner sind meist permanent mit dem Internet verbunden, was neue Möglichkeiten für Angriffe auf die IT-Sicherheit bietet.

Der Begriff IT-Sicherheit wird aus den Begriffen IT und Sicherheit abgeleitet. Unter Sicherheit wird allgemein der Zustand der Freiheit vor Gefahr und Schaden verstanden.[2] Dabei wird jedoch nur von einem relativen Zustand ausgegangen, da jederzeit Änderungen auftreten können, welche diese Freiheit beeinträchtigen.
IT bezeichnet die Abkürzung für Information- und Kommunikations-technologie, wobei sie in der Literatur auch häufig als Synonym für Informationssysteme (IS) genutzt wird.[3] Ein IT-System stellt demnach „ein geschlossenes oder offenes, dynamisches technisches System mit der Fähigkeit zur Speicherung und Verarbeitung von Informationen“[4] dar.

Die IT-Sicherheit umfasst die Bereiche Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit.[5] Alle diese Bereiche können für die Nutzer von IT-Systemen sicherheitsrelevant sein. In der Literatur finden sich neben den vier genannten Schutzzielen teilweiße noch weitere, wie zum Beispiel Authentizität, Anonymisierung und Pseudomisierung[6], jedoch können diese nach meiner Ansicht auch zu den vier erstgenannten gezählt werden. So würde ich die Authentizität dem Bereich Verbindlichkeit und die Anonymisierung sowie Pseudomisierung dem Bereich Vertraulichkeit zuordnen.
Bei der Begriffsklärung möchte ich der Arbeit von Hoppe / Prieß folgen. Danach ist Vertraulichkeit, der ausschließliche Zugriff bzw. Zugang von autorisierten Personen auf Daten oder Systeme. Unter Verfügbarkeit wird verstanden, dass das System bzw. die Daten von den berechtigten Nutzern ohne Einschränkungen verwendet werden können. Damit die Integrität von

[2] Vgl. Hoppe, G. / Breitner, M.H.: IT-Sicherheit.
[3] Vgl. Hoppe, G. / Breitner, M.H.: IT-Sicherheit
[4] Vgl. Eckert [2005, S. 1].
[5] Vgl. Hoppe [2003, S. 24/25].
[6] Vgl. Eckert [2005, S. 6-12].

System und Daten nicht verletzt ist, müssen diese korrekt, vollständig, widerspruchsfrei und aktuell sein. Die Verbindlichkeit von System und Daten ist gegeben, wenn Änderungen bzw. Nutzung von diesen, einem Nutzer direkt zugeordnet werden kann.[7]

Nachdem ich kurz aufgeführt habe was unter IT-Sicherheit verstanden wird, möchte ich jetzt darauf eingehen welche Bedrohungen es für diese gibt. Bedrohungen für die IT-Sicherheit können von direkten Angriffen oder unbeabsichtigten Störungen ausgehen.[8] In meiner Arbeit möchte ich mich hauptsächlich mit dem Schutz vor Angriffen befassen. Schutz vor Störungen kann das Betriebssystem nur bedingt bieten, da diese meist auf Höhere Gewalt oder Fahrlässigkeit beruhen.

Die Arten der Bedrohungen hat sich in den letzten Jahren stark gewandelt. Während bis in die 90er Jahre die größte Gefahr für Rechner von unerfahrenen bzw. böswilligen Nutzern oder sich langsam mit Hilfe von Disketten verbreitenden Computerviren ausging, bietet die zunehmende Verbindung der Rechner über das Internet bzw. andere Netzwerke, eine Vielzahl neuer möglicher Angriffsformen.

Angriffe auf die IT-Sicherheit lassen sich unterteilen in aktive (Sabotage) und passive (Spionage) Angriffe.[9] Bei Letzterem erfolgt der Angriff ohne Änderungen der Daten. Dazu zählt zum Beispiel das unautorisierte Abhören oder Mitlesen von wichtigen Daten. Eine weit verbreitete Form dieser Art stellt der Sniffer-Angriff dar, bei dem Datenpakete in Netzwerken vor allem nach Passwörtern durchsucht werden.
Eine umfangreichere Bedrohung stellen aktive Angriffe dar. Dabei werden zum Beispiel durch passive Angriffe, Brute-Force-Angriffe oder Social Engineering erlangte Passwörter genutzt, um in Rechner oder Netzwerke einzubrechen und Daten zu manipulieren oder zu löschen.[10] Beim Spoofing einer weiteren weitverbreiteten Art von Angriffen im Internet, wird versucht

[7] Vgl. Hoppe [2003, S. 24/25].
[8] Vgl. Hoppe [2003, S. 33].
[9] Vgl. Eckert [2005, S. 14/15].
[10] Vgl. Hoppe [2003, S. 77-79].

eine andere Identität vorzutäuschen, um so an vertrauliche Informationen zu gelangen. Es werden beim Spoofing verschiedene Varianten unterschieden, je nachdem was gefälscht wird. Eine Variante, das URL-Spoofing wird oft in Verbindung mit Phishing verwendet. Dabei werden e-Mail Empfängern, durch das Vortäuschen falscher Absender, vertrauliche Informationen entweder direkt, oder über den Link zu einer gefälschten Website, entlockt. Zu den aktiven Angriffe zähle ich weiterhin das Benutzen von Malware[11]. Diese kann verschiedene Schäden verursachen. Eine Variante davon, das Backdoor ermöglicht beispielsweise den Zugang zum betroffenen Rechner. Diese werden dann oft für DDoS-Angriffe genutzt, bei welchen die Verfügbarkeit des Zielrechners durch sehr viele Anfragen eingeschränkt wird.
Dies waren einige häufig anzutreffende Angriffsformen. Diese und eine Übersicht von weiteren Angriffsformen und Erläuterungen dazu findet man bei Hoppe [2003, S. 37ff.].

Welche Aufgabe kommt nun dem Betriebssystem zur Verbesserung der IT-Sicherheit zu?
Das Betriebssystem ist zusammen mit der Hardware das Basissystem eines IT-Systems.[12] Weitere Komponenten sind Manware, Orgware Anwendungssoftware und Daten. Außer den Daten, welche einen rein passiven Charakter haben, können alle anderen Komponenten Schwachstellen aufweisen und somit zum Angriffspunkt auf die IT-Sicherheit werden.[13] Das Betriebssystem alleine kann zwar keinen vollkommenen[14] Schutz gewähren, jedoch hat es als Schnittstelle zwischen Umwelt und Computer einen großen Einfluss auf die Sicherheit des Computers. Je nach Konzeption kann es in Verbindung mit der Hardware und den anderen Komponenten die IT-Sicherheit positiv, aber auch negativ beeinflussen.

[11] Vgl. http://de.wikipedia.org/wiki/Malware.
[12] Vgl. Baldi [1999, S. 58].
[13] Vgl. Hoppe [2003, S. 20].
[14] soweit überhaupt von vollkommenen Schutz gesprochen werden kann, da dieser Zustand relativ ist.

7 Fazit und Ausblick

Die Relevanz von IT-Sicherheit hat in den letzten Jahren stetig zugenommen. Die steigende Verbreitung von IT-Systemen und ihre Nutzung in immer mehr Bereichen, hat zu einer Veränderung der Motivation der Angreifer geführt. Ging es früher hauptsächlich um Aufmerksamkeit, so zählen heute vor allem finanzielle Interessen. Bei Unternehmen sind dies zum Beispiel Angriffe auf die Verfügbarkeit der Rechner, mit finanziellen Nachteilen für das Unternehmen, sowie Angriffe auf die Vertraulichkeit von Informationen, mit finanziellen Vorteilen für die Angreifer. Bei Privatanwendern wird vermehrt auf vertrauliche Informationen zum Beispiel PIN und TAN Nummern abgezielt, durch die sich die Angreifer geldwerte Vorteile verschaffen können.
Vor allem die zunehmende Vernetzung über immer schnellere Leitungen, lässt das Bedrohungspotential weiter steigen. Die Anwendungssoftware ebenso wie die Betriebssysteme werden dabei immer komplexer und damit auch fehleranfälliger. Die Zeiten zwischen Bekanntmachung und Ausnutzung von Schwachstellen werden immer kleiner, so dass für die Hersteller kaum Zeit bleibt diese Lücken durch Sicherheitsupdates rechtzeitig zu schließen. Selbst wenn diese rechtzeitig verfügbar sind, so werden sie doch oft nicht rechtzeitig installiert. Bei den Privatanwendern geschieht dies oft aus Unerfahrenheit und bei Unternehmen müssen Sicherheitsupdates erst auf unerwünschte Nebenwirkungen getestet werden, bevor sie in der Produktivumgebung eingesetzt werden können. Bei kleinen und mittleren Unternehmen kommt meist noch hinzu, dass sie finanziell bzw. personell mit dem Thema IT-Sicherheit überfordert sind.

Es müssen daher neue Wege gefunden werden um die Sicherheit der IT-Systeme zu erhöhen. Microsoft hat deshalb für sein nächstes Betriebssystem neben einigen optischen Neuerungen[86] auch ein neues Sicherheitskonzept Namens Palladium, später dann Next Generation Secure Computing Base (NGSCB) genannt, angekündigt. Aber auch für das

[86] z.B. das Grafiksubsystem Avalon

aktuelle Betriebssystem Windows XP wurde mit dem Servicepack 2, durch eine leichtere Konfiguration der Windows-Firewall und einer besseren Überwachung der Aktualität von Betriebssystem und Anti-Virenprogrammen, eine bessere Sicherheit ermöglicht. So sank die Größe der Bot-Netze, welche aus unter fremder Kontrolle stehenden Rechnern bestehen, nach Veröffentlichung des Servicepack 2.
Auch der Einsatz von Linux wird oft empfohlen um die Sicherheit des Rechners zu erhöhen. Aber mit zunehmender Verbreitung von Linux auch bei unerfahrenen Anwendern, steigt auch hier das Sicherheitsrisiko, wie die zunehmende Anzahl von Linux Viren zeigt. Es lässt sich befürchten, dass mit wachsender Nutzerzahl auch Linux stärker als bisher in den Blickpunkt von Angreifern gerät.

Das von Microsoft für Windows Vista ursprünglich vorgesehene NGSCB, zur Erhöhung der Betriebssystemsicherheit wurde durch verschiedene Gruppen abgelehnt. Um dennoch die Sicherheit zu verbessern, wurden einige neue Konzepte entwickelt. Zur NGSCB zählt zur Zeit nur das Secure Startup mit Full Volume Encryption. Andere Elemente wie die gesicherten Umgebungen auf Basis der hardwareunterstützten Virtualisierung sollen eventuell später noch nachgereicht werden. Das Secure Startup verspricht einen gesicherten Systemstart in Verbindung mit der Verschlüsselung der Systempartition. Einen wesentlich besseren Schutz auch im laufenden System könnten die sicheren Umgebungen in virtuellen Rechnern, durch einen Parallelbetrieb von sicherheitskritischen Anwendungen ermöglichen.
Eine gute Möglichkeit um die Folgen von verschiedenen Angriffen zu reduzieren, ist eine sinnvoll konfigurierte Zugriffsrechteverwaltung. Zwar besitzt auch Windows XP, wie alle aktuellen Betriebssysteme eine solche, jedoch wird sie aus verschiedenen Gründen viel zu selten genutzt. In Windows Vista wird deshalb eine Funktion mit dem Namen „User Account Protection“ eingeführt. Durch diese können auch weniger versierte Anwender mit eingeschränkten Zugriffsrechten arbeiten und so die Sicherheit ihres Rechners erhöhen.
Beim NGSCB war bisher immer auch die Rede von sicheren Umgebungen, sicherer Eingaben bzw. sicherer Ausgaben, welche spezielle sichere

Hardware erfordern, zum Beispiel das TPM. Speziell für diese sicheren Umgebungen programmierte Software und Daten sollten so besonders geschützt werden können. Findet die Software nicht sichere Hardware im Rechner, kann ihre Ausführung verhindert werden. Auch wenn diese sicheren Umgebungen, bedingt durch die noch nicht verfügbaren hardwareunterstützten Virtualisierungsfunktionen, erst später eingeführt werden sollen, so gibt der Protected Media Path einen Einblick wie diese aussehen könnten. Dieser stellt eine sichere Umgebung inklusive sicherer Eingabe und sicherer Ausgabe dar und dient der Umsetzung des DRM. Eine der Kritiken am NGSCB war die mögliche Nutzung für das DRM und nun wird bei Windows Vista der Protected Media Path erst einmal die einzige sichere Umgebung sein, während das NGSCB Konzept durch Secure Startup vorerst nur ansatzweise umgesetzt wurde.

Windows Vista enthält einige gute Ansätze, die geeignet sind die Sicherheit des Betriebssystems zu erhöhen. Diese setzen jedoch zum Teil neue Hardware voraus, so dass sich Windows Vista als Betriebssystem nur langsam durchsetzen dürfte. Speziell die sicheren Umgebungen stellen besondere Anforderungen an die Hardware, auch wenn diese vorerst auf Multimediasoftware und -inhalte beschränkt bleiben.
Von dem grundlegend neuen Sicherheitskonzept, welches Windows Vista zu einem der sichersten Betriebssysteme machen sollte, ist in Windows Vista noch nicht viel zu sehen. Die Elemente Secure Startup, Full Volume Encryption und User Account Protection, stellen vielmehr Erweiterungen und Verbesserungen der bisher schon vorhandenen Elemente Verschlüsselung und Zugriffsrechteverwaltung dar. Die einzigen wirklichen Neuerungen sind die Einbindung des TPM in das Betriebssystem sowie der Protected Media Path.
Größtes Potential für die Zukunft sehe ich in den virtuellen Rechnern, basierend auf der hardwareunterstützten Virtualisierung. Allerdings sollte dazu die Lizenzpolitik vieler Softwarehersteller überarbeitet werden, da sonst für jeden virtuellen Rechner extra Lizenzen notwendig werden könnten.