

JOHANNES FRITSCHKE

PRO & CONTRA: DAS MEINEN EXPERTEN



Bei aller Kritik im Detail: Die Hersteller von Security-Lösungen sehen in Windows Vista deutliche sicherheitsrelevante Fortschritte. Business & IT hat die Experten verschiedener Anbieter nach ihrer Einschätzung gefragt.

Neun Experten – neun Meinungen. Das ist das wenig überraschende Ergebnis unserer Umfrage zur Sicherheit von Windows Vista. Betrachtet man die inhaltlichen Details, kann man allerdings interessante Gemeinsamkeiten und Unterschiede feststellen, die man vorab so nicht erwartet hätte. Dass Windows Vista tatsächlich das bislang sicherste Betriebssystem von Microsoft darstellt, ist unumstritten. Ob das Anwenden und Unternehmen aber weiterhilft, darüber gehen die Meinungen auseinander.

Kaum verändertes Gefährdungspotenzial



Helmut Büsker, Produktmanager der Avira GmbH:

„Microsoft hat mit den neuen Sicherheits-Features in Vista das Bewusstsein für Sicherheit

bei den Anwendern geschärft – das ist prinzipiell eine gute Sache.

Vista selbst bringt eine Reihe von Sicherheits-Features, die es in der Tat zunächst einmal schwerer machen, einen Rechner mit Malware zu infizieren. Dazu zählen unter anderem das Konzept der User Account Control (UAC) oder der Internet Explorer im Protected Mode oder die erweiterte Firewall. Gleiches gilt für eine Reihe von Sicherheitsmaßnahmen, die die Integrität des Kernels und des Systems sicherstellen oder verhindern, dass Exploits Systemschwächen ausnutzen können.

Erste unabhängige Tests haben aber schon kurz nach der Verfügbarkeit von Vista erge-

ben, dass zahlreiche Malware unter den Vista-Sicherheitskonzepten überlebensfähig ist und seine schädliche Wirkung entfalten kann. Es ist davon auszugehen, dass diese Rate drastisch ansteigen wird, sobald sich Malware-Schreiber erst mal so richtig auf Vista eingeschossen haben – oftmals bedarf es nur geringer Änderungen, um die Malware an Vista anzupassen.

Die eher ‚User-bezogenen‘ Sicherheits-Features von Vista wie UAC stellen ein besonderes Problem dar. Man muss davon ausgehen, dass die vielen Dialogfenster, die der Anwender bekommt, zu einer gewissen Abstumpfung hinsichtlich der wahren Gefahr führen werden. Im schlimmsten Fall wird ein Anwender diese Features einfach deaktivieren.

Vista kommt mit einer Reihe neuer Technologien, und die können für sich genommen ein neues Gefährdungspotenzial darstellen. Dazu gehören beispielsweise die Windows Sidebar oder verschiedene Extras wie Uhr, Kalender und RSS Reader. Diese Funktionen können von Malware-Schreibern missbraucht werden, um den Anwender zu veranlassen, Inhalte aus dem Web auf den Rechner zu laden oder darüber vertrauliche Informationen auszulesen. Denn diese Extras sind autorisiert, direkt mit dem Web zu kommunizieren.

Summa summarum wird Vista aber die IT-Infrastrukturen in einem Unternehmen nicht dramatisch verändern. Wir haben schon unter XP erlebt, dass die Malware-Szene äußerst flexibel und erfinderisch ist, wenn es darum geht, die Sicherheits-Features eines Systems auszuhebeln.

Da mittlerweile die Szene sehr stark von wirtschaftlichen Interessen getrieben wird, ist davon auszugehen, dass das Gefährdungspotenzial auf einem ähnlich hohen Niveau auch unter Vista bestehen bleiben wird. Alle IT-infrastrukturellen Sicherheitsmaßnahmen, die bislang angeraten waren, sind also nach wie vor auch unter Vista notwendig.“

Alles bleibt beim Alten



Martin Siemens, Geschäftsführer von BitDefender:

„Durch das Konzept der eingeschränkten Administratoren und der User

Account-Control-Funktion bietet Windows Vista gegenüber Windows XP ein höheres Sicherheitsniveau. Die Untersuchungen unabhängiger Testlabore und letztlich auch die Erfolge von Hackern sowie Malware-Autoren werden zeigen, wie es um die Sicherheit von Vista wirklich bestellt ist.

Für den Anwender bleibt jedoch alles beim Alten: Das Betriebssystem allein bietet keinen ausreichenden Schutz.“

Soll der Frosch den Sumpf austrocknen?



Dr. Christoph Skornia, Technical Manager Central Europe, Check Point:

„Seit dem Launch von Windows Vista und dem

von Microsoft optional angebotenen Sicherheitspaket OneCare scheint Bewegung in die Diskussion über Sicherheitsmechanismen auf dem Client gekommen zu sein. Dies ist zunächst einmal uneingeschränkt positiv zu beurteilen, da der Sicherheitszustand beim Großteil der heute auf Windows laufenden Rechner als nicht zufrieden stellend einzustufen ist. Die großen Wurm-Ausbrüche der letzten Jahre oder auch die aktuellen, durch Rootkits oder Bot-Netze verursachten Schadensfälle haben dies klar gezeigt.

Was sind jedoch die Kernaussagen, welche aus der aktuellen Diskussion hervorgehen? Wichtig scheint in jedem Fall, dass auch der Hersteller des Betriebssystems zur Absicherung nicht nur auf systemimmanente Mechanismen wie etwa professionelles Patch-Management setzt, sondern auch den Weg einer unabhängigen Instanz beschreitet, welche die Aktionen des Betriebssystems kontrolliert und schadhafte Verhalten unterbindet. Dies bestätigt die generelle sicherheitstheoretische Sicht, dass für eine verbesserte Sicherheit die Kontrollmechanismen unabhängig voneinander sein müssen – etwa so, wie es in Staatssystemen Gewaltenteilung gibt.

Ob man im konkreten Fall mit OneCare möglicherweise die Frösche beauftragt hat, den Sumpf trocken zu legen, ist noch nicht abzusehen. Die zukünftige Entwicklung der Funktionalität sowie deren Verquickung mit dem Betriebssystem werden hier Klarheit bringen. Da Microsoft aber selbst veröffentlicht, dass das jetzt laufende Windows XP länger unterstützt bleiben wird als das neu veröffentlichte Windows Vista, lohnt es sich mit Sicherheit, neugierig zu bleiben.

Bedarf für Sicherheitsmechanismen gibt es also, was den Anwender im geschäftlichen und im privaten Umfeld zu der Frage führt, welcher Weg gewählt werden sollte. Der Markt scheint komplex, und wie man sich wirklich schützt, ist augenscheinlich nicht ganz klar. Deutlich zeigt sich jedoch, dass es gerade im Firmenumfeld klare Trends auf diesem Gebiet gibt.

Hier sind vor allem zwei Entwicklungen hervorzuheben: zum einen der Einsatz von koordinierten Lösungen, welche die einzelnen Sicherheitsmechanismen abgestimmt haben. Security Suites bieten heute sehr umfangreiche Funktionalität, und die Integration dieser Systeme mit Festplatten-Verschlüsselung und Bootsicherheit ist hier der

logische nächste Schritt. Zum anderen werden Aspekte des Lösungsbetriebs immer wichtiger. Zentrales Konfigurations- sowie Informationsmanagement ist heute aus reinen Effizienz-Überlegungen heraus eine zwingende Anforderung an den Betrieb im Unternehmen. Hier gibt es noch sehr große Unterschiede bei den einzelnen Herstellern von Sicherheitslösungen, gerade auch wenn es um die Koordination zwischen Sicherheitsmechanismen auf dem Client und im Netzwerk geht.

Zusammenfassend lässt sich also sagen, dass sinnvolle Sicherheitsmechanismen unabhängig vom Betriebssystem arbeiten sollten, gleichzeitig aber ein umfangreicher Schutz des Clients mit einem effizienten Betriebskonzept verknüpft werden muss und kann. Dies bestätigt auch Microsoft mit Vista und OneCare. Dem Kunden wird es überlassen bleiben, welches Angebot ihn überzeugt. So oder so, in jedem Fall tut die neue Bewegung gut.“

Besserer Schutz für mobile Mitarbeiter



Klaus Lensert, Senior Business Development Manager Security bei Cisco Deutschland:

„Vista wird einen wesentlichen Beitrag dazu leisten, bei Sicherheitskonzepten nicht mehr in den Klassen Netzwerk- und Endgeräte-Sicherheit zu denken, sondern zu einer holistischen Infrastruktur-Sicherheitssicht zu kommen. Vista enthält die im Endgeräte-Betriebssystem notwendigen Mechanismen, die es den Kunden ermöglichen, den Endgeräte-Sicherheitszustand zu überprüfen und in Abhängigkeit davon den Netzwerk-Zugang zu steuern. Der Fokus auf einen integrierten Agent reduziert die Komplexität der Implementierung und damit die Aufwände und das Betriebsrisiko für die Kunden. Sicherheitsrichtlinien lassen sich so infrastrukturweit mit Hilfe des Netzwerks zuverlässig durchsetzen.

Vista vereinfacht so wesentlich die Einführung von NAC/NAP im Unternehmen und hilft so, besonders die zunehmend mobilen Mitarbeiter besser zu schützen. Microsoft und Cisco Systems haben die NAC/NAP-Protokolle cross-lizenziert und investieren in die gemeinsame Weiterentwicklung der Lösung.“

Bewegung im Software-Markt



Karl-Heinz Warum, Area Vice President Central Europe und Geschäftsführer der Citrix Systems GmbH:

„Die Einführung von Vista ist generell als Chance zu beurteilen, denn der Software-Markt kommt dadurch in Bewegung. Viele Unternehmen stehen damit vor der Herausforderung, strategische Investitionsentscheidungen in IT-Strukturen treffen zu müssen, um in ihren Märkten weiter wettbewerbsfähig zu bleiben.

Für uns als weltweit führender Anbieter von Infrastruktur-Lösungen zur Anwendungs-Bereitstellung bietet die Vista-Migration großes Potenzial. Denn mit Citrix Presentation Server 4.5 können wir die Updates zentral und sicher durchführen und die Anwendungen virtualisiert oder gestreamt bereitstellen, ohne Hardware-Upgrades und Installationen an den Endgeräten vorzunehmen. Mit dieser Technologie verringert sich somit der Administrations-Aufwand für Unternehmen erheblich und steigert gleichzeitig deren Kosteneffizienz.“

Ein Schritt in die richtige Richtung



Matthias Rosche, Director Consulting CE und Mitglied der Geschäftsleitung von Integralis Deutschland:

„Es ist heute noch zu früh, um Praxiserfahrungen für Vista aufzuführen. Betrachtet man jedoch die Anzahl der gefundenen Schwachstellen bei Vista in den ersten drei Monaten (Stand: 21.3.2007), so sind diese mit fünf wesentlich geringer als bei XP (18 Schwachstellen) oder auch bei alternativen Betriebssystemen wie Mac OS X.10.4 (37 Schwachstellen) und Novell SUSE Linux Enterprise Desktop 10 (111 Schwachstellen) ausgefallen.

Als neue Wunderwaffe wird insbesondere die User Account Control gepriesen. Damit ist es möglich, zum Beispiel den Internet Explorer auf einer niedrigeren Berechtigungsstufe auszuführen und möglichen, virenlenten Code damit zu isolieren. Ob dem wirklich so ist, werden wir in den nächsten sechs bis zwölf Monaten sehen. Einiges

spricht jedoch schon heute dafür, dass Schwachstellen auch in diesem Konzept nicht ausbleiben werden.

Ein weiterer Fortschritt ist sicher das neue Verschlüsselungssystem Bitlocker. Hier hat Microsoft einen wesentlichen Schritt in Richtung mehr Sicherheit getan. Allerdings gibt es im Unternehmenseinsatz einige Anforderungen, die Bitlocker nicht abdeckt. Dies wären zum Beispiel vollständig integrierte Administrationswerkzeuge, Verschlüsselung aller Partitionen inklusive Wechselmedien sowie der Support von Nicht-Windows-Umgebungen. Hier werden die bekannten Anbieter von Verschlüsselungs-Tools auch 2007 noch einiges umsetzen können. Alles in allem ist aber das Bemühen von Microsoft zu erkennen, im Sicherheitsbereich voranzugehen.“

Deutlich sicherer als XP



Simon Azzopardi, Vice President EMEA Sales bei GFI Software:

„Vista bietet im Vergleich zu früheren Versionen von Windows ein erheb-

lich höheres Maß an Sicherheit. Technologien wie Bitlocker, die verstärkte Absicherung von Windows Services sowie eine zusätzliche granulare Zugriffssteuerung von Nutzern und Geräten werben wir ganz klar als Schritte in die richtige Richtung.

Trotz allem ist Vista noch immer kein vollkommen sicheres System, denn es gibt Unternehmen nicht den Einblick und die Kontrolle, die für einen umfassenden Schutz von Netzwerken und Systemen nötig sind.“

Ein Betriebssystem ist keine Sicherheitslösung



Alexander Peters, Global Client & Partner Services Manager bei MessageLabs:

„Microsofts Schritt, das Betriebssystem sicherer zu machen, geht auf alle Fälle in die richtige Richtung. Microsofts Engagement im Security-Umfeld und die damit zusammenhängenden Diskussionen leisten auch einen Beitrag dazu, die Security-Problematik einer breiteren Zielgruppe bewusst zu machen und ihr die notwendige Aufmerksamkeit zu verschaffen. Allerdings sollte

man ein Betriebssystem nicht mit einer Security-Lösung verwechseln; für wirklich umfassenden Schutz sind nach wie vor Sicherheitslösungen notwendig, die sämtliche möglichen Einfallstore für Malware überwachen können.

Die vermeintliche Absicherung eines Betriebssystems macht es in der Tat schwieriger für die Malware-Entwickler, jedoch hat sich in der Vergangenheit gezeigt, dass es bei diesem Wettrüsten den so genannten Black-Hats (also Hackern, die Schwachstellen ausfindig machen und diese zu ihrem Vorteil ausbeuten) immer wieder gelingt, die Nase vorn zu haben.

Microsofts Einstieg in das Security-Segment setzt die etablierten Anbieter natürlich unter Druck. Wir persönlich glauben jedoch daran, dass das die Entwicklung hin zu Managed Services eher noch beschleunigen wird.

Anwendern wird immer bewusster, dass die Komplexität des Problems nicht allein über einzelne Desktop- oder Server-Tools gelöst werden kann, der hierzu nötige Aufwand wird immer unüberschaubarer. Deshalb wird sich IT-Sicherheit vermehrt zu einer Dienstleistung entwickeln, die man wie Wasser oder Strom bezieht.“

Viel Licht und Schatten



Dietmar Schettgen, Leiter Systemberatung bei der RDS Consulting GmbH:

„Windows Vista ist in der Enterprise Edition das bislang sicherste Windows.

Besonders für Unternehmen, die viele Außendienst-Mitarbeiter mit Notebooks beschäftigen, bringt Vista einen Sicherheitsgewinn. Dazu zählt die Verschlüsselung der Daten, die bereits vor dem Booten geschützt sind. Zudem waren unter Windows XP häufig Außendienst-Mitarbeiter mit Administratorrechten auf ihren Notebooks unterwegs. Mit der Benutzerkonten-Steuerung unter Vista können nun auch die meisten Anwendungen mit eingeschränkten Berechtigungen ausgeführt werden.

Mit Blick auf unterschiedliche Einsatzorte erlaubt die überarbeitete Firewall unterschiedliche und profilbasierende Konfigurationen, die auf die jeweilige Umgebung zugeschnitten sind. Mit der Blockade ausgehender Verbindungen, um zum Beispiel Trojanern die Kommunikation nach außen zu verwehren,

wird eine längst überfällige Funktion erfüllt. Nach wie vor sind aber die bislang eingesetzten Firewalls anderer Hersteller einfacher zu konfigurieren.

Zusätzlichen Schutz bietet auch der in Vista eingebundene Internet Explorer mit eingebautem Phishing-Filter und Protected Mode. Hilfen bei der Entscheidung, ob ein Zugriff erlaubt oder verhindert werden soll, fehlen allerdings. Ein durchschnittlicher Anwender ohne das nötige Know-how ist hier überfordert und trifft mit einer fünfzigprozentigen Wahrscheinlichkeit eine falsche Entscheidung. Firmennetzwerken und Mobil Computing bietet Vista also mehr Schutz und Sicherheit. Auch wenn dem Außendienst-Mitarbeiter das Notebook abhanden kommt, bleibt das Tor zu Netzwerken und Daten weitgehend verschlossen.

Das Patch-Management unter Vista kommt internationalen Unternehmen zugute: Nun können einzelne Module des Betriebssystems geändert werden, ohne andere Komponenten zu beeinflussen. Dadurch müssen bei einem Update von Windows-Komponenten – zum Beispiel Sicherheits-Patches – nicht mehr alle Sprachversionen getestet werden. Positiv ist auch die Möglichkeit, bereits erstellte Images nachträglich mit Updates zu bestücken.

Unbefriedigend bleibt dagegen auch unter Vista der Schutz vor Viren, Würmern und Trojanern. Unseren Kunden empfehlen wir dringend nach wie vor den Einsatz einer professionellen Virenschutz-Software. Der in Vista integrierte Windows Defender bietet keinen ausreichenden Schutz gegen die heute im Internet kursierenden Bedrohungen.

Zu den neuen, positiven Eigenschaften gehört ein komplettes Sicherungsverfahren auf Basis von Images, die auch über das Netzwerk erstellt werden können. 3rd-Party-Tools werden damit überflüssig. Hervorzuheben ist auch eine neue Gerätesicherheit: Unter Vista können mobile Speicher (USB-Sticks oder auch iPods) verwaltet werden; über Gruppenrichtlinien lässt sich der Zugriff steuern und gegebenenfalls unterbinden.

Negativ ist die Benutzerkontenführung, die auf den ersten Blick sehr nützlich scheint und endlich die riskante Generalvergabe von Administratorrechten beendet. Die Häufung von Sicherheitsabfragen und das Bestätigen von Dialogboxen führt jedoch schnell zum ‚blinden Klicken‘ oder gar zum Abschalten der Abfragen. Dies macht dann einen Teil des Sicherheitsgewinns wieder zunichte.“

JFM