

Brennpunkt Vista: Thomas Kuberek im Gespräch mit Michael Kalbe

21.02.2007

Michael Kalbe ist als Technologieberater Infrastruktur-Security in der Developer Platform & Strategy Group für die Microsoft Deutschland GmbH tätig.

<http://blogs.technet.com/mkalbe>



Thomas Kuberek ist Mitbegründer von MCSEboard.de, dem führenden deutschen Diskussionsforum zu den Themen Microsoft Zertifizierungen und Windows Problemlösungen.

www.mcseboard.de

Michael Kalbe ist Technologieberater bei Microsoft – speziell für den Bereich Sicherheit. Und er ist so freundlich, uns in einem Interview Fragen zu Windows Vista zu beantworten. Vista – das ist doch eine ganz neue Geschichte. Schneller, besser, sicherer und eben das neue Betriebssystem von Microsoft. Michael, kannst du uns sagen, was sich bei Windows Vista alles geändert hat? (00:00)

Zuerst einmal vielen Dank Thomas. Vollkommen richtig, Windows Vista ist ein neues Betriebssystem. Es zu entwickeln, hat einige Zeit gedauert und natürlich bietet es viel Neues. Die wesentlichen Neuheiten liegen im Bereich Sicherheit, aber auch in etlichen zusätzlichen und verbesserten Funktionen. Wenn man etwa an Unternehmensumgebungen denkt, betrifft das beispielsweise den Punkt Deployment, sprich das Verteilen vom Client-Betriebssystem im Unternehmen wird leichter.

Und was kannst du uns allgemein zu Vista sagen? Ich denke da an Themen wie verbesserte Teamarbeit. Was hat sich diesbezüglich bei Vista getan? (01:20)

Auch die Zusammenarbeit wird mit Windows Vista einfacher. Dafür gibt es sogar ein kleines Tool mit dem Namen Windows Teamarbeit. Um unter anderem eine Art Ad-hoc-Meeting einzuberufen. Das heißt, wir zwei könnten uns jetzt sofort eine Präsentation auf unseren beiden Vista-Laptops ansehen. Ohne Projektor, einfach indem wir eine Ad-hoc-Wireless-Verbindung aufbauen, um uns zusammen Dinge anzusehen oder gemeinsam Dokumente zu bearbeiten. Wenn man so will, wie eine Art Nachfolgemodell vom NetMeeting, nur wesentlich leistungsfähiger, weil hier die ganzen Mechanismen drinstecken, wie Ad-hoc-Networking und so weiter.

Was fällt dir zum Stichwort Easytransfer ein? (02:11)

Easytransfer heißt ein Tool, mit dem ich meine Einstellungen, meine eigenen Dateien, also alles, was ich „in meinem Desktop“ kreierte und konfiguriert habe, von einem Gerät auf ein anderes übertragen kann. In Windows Vista ist dieser Easytransfer Wizard integriert – beziehungsweise der Easytransfer-Agent, wie es im Deutschen heißt. Mit ihm kann ich genau diese Sachen übertragen, völlig problemlos von einem System zum anderen. Dazu gibt es mehrere Möglichkeiten: Ich kann die Daten auf ein austauschbares Medium wie eine DVD kopieren, die ich dann brenne. Ich kann sie aber auch auf einen USB Stick übertragen oder via Netzwerk auf ein anderes Gerät oder per USB-Kabel, das ich in meine zwei Systeme einstecke. Mittlerweile gibt es auch einen Download auf der Webseite von Microsoft, der das gleiche für Windows XP- und Windows 2000-Systeme ermöglicht. Das bedeutet, dass ich alles, was ich auf meinem alten Windows-System erstellt und konfiguriert habe, in eine Windows Vista-Installation übernehmen kann. Einfach Tool starten, Bereiche und Einstellungen auswählen, die übernommen werden sollen, das Ganze ins Windows Vista-System importieren und entspannt weiterarbeiten.

Das funktioniert also auch von einem bestehenden 2000- oder XP-System auf Vista? (03:34)

Genau dafür ist es ja gedacht. Soweit ich weiß, gibt es keine Möglichkeit, den Easytransfer Wizard von einem XP-System zu einem anderen XP-System anzuwenden. Es geht immer entweder um Vista zu Vista oder XP/Windows 2000 zu Vista. Das Tool, das ich gerade erwähnt habe, kann man für sein XP- oder 2000-System herunterladen, die Einstellungen dann quasi auf einem USB Stick auslagern und in die Vista-Maschine einstecken. So habe ich die Möglichkeit, die entsprechenden Konfigurationen auf dem Vista-System, also

beispielsweise POP3-Konfigurationen aus Outlook, Einstellungen zu bestimmten Symbolleisten in einer Applikation, ein Hintergrundbild vom System oder eben meine eigenen Dateien zu übernehmen.

Das gefällt mir, zumal ich ja auch mein bestehendes und gewachsenes XP-System auf ein Vista-System übertragen muss, das erleichtert mir die Arbeit mit der Sicherheit. Und wie sieht es für Administratoren eines Unternehmensnetzwerkes aus? Verbessert und erleichtert Vista auch deren Arbeit? (04:30)

Schön, dass du diesen Punkt ansprichst. Die meisten Neuheiten von Windows Vista sieht man nämlich tatsächlich, wenn man das System in einem Unternehmensnetzwerk einsetzt. Die ganze Bandbreite der einzelnen Werkzeuge, wie zum Beispiel das Protokollieren von Ereignissen, hat man als Endanwender nicht so unmittelbar im Blick, weil man anders mit dem Gerät arbeitet. Aber im Unternehmensnetzwerk steht man vor ganz anderen Herausforderungen. Da muss der Administrator die Systeme verwalten. Vielleicht braucht er einen Zustandsbericht über die einzelnen Geräte. Oder er muss Fehler frühzeitig erkennen und kann nicht warten, bis ein Anwender beim Helpdesk anruft. An genau diesen Punkten setzt Windows Vista an. Damit sehe ich quasi schon im Vorwege, dass vielleicht ein Problem auf mich zusteuert, dass die Platte kurz davor ist, den Geist aufzugeben, um es mal salopp auszudrücken, oder dass andere Applikationen Probleme machen. So kann ich mich als Administrator schon proaktiv an die Fehlersuche machen und Fehler vermeiden, damit der Anwender immer ein Windows Vista-System besitzt, das funktioniert und mit dem er arbeiten kann, und er im Prinzip gar nichts von dieser Tätigkeit im Hintergrund mitbekommt.

Wenn ich das richtig verstanden habe, ist das ein bisschen wie mit der berühmten Glaskugel. Ich sehe, was in der Zukunft passieren kann, basierend auf Informationen, die mir das System liefert. Und zwar ausgehend von einer Ansicht auf die gesammelten Daten, die mir nicht nur einzelne Teile eines Ereignisprotokolls anzeigt, sondern sie im Kontext betrachtet. So erkenne ich Tendenzen und Entwicklungen, die möglicherweise bald auf mich zukommen und die ich aus der einzelnen Meldung nicht ersehen könnte. Stimmt das so? (06:11)

Prinzipiell ja. Es existiert zwar leider kein MMC Snapp-In, das sich Glaskugel nennt, aber es gibt die Zuverlässigkeitsüberwachung. Diese bezeichnet eine Stelle, an der viele Informationen zusammenlaufen. Mit Windows Vista haben wir das Ereignisprotokoll umgestellt, das bedeutet, im Ereignisprotokoll findest du relativ aufgeräumte Informationen. Eine tabellarische Ansicht, die auch addiert, zeigt zum Beispiel an, dass ein bestimmter Fehler schon 47-mal aufgetreten ist. Wenn du diese Fehlermeldung anklickst, bekommst du nur Teilinformationen zu genau diesem Fehler und wirst nicht gleichzeitig mit anderen Fehlermeldungen überfordert. So erhältst du sehr spezifische Informationen. Besagte System-Zuverlässigkeitsüberwachung kombiniert viele Ereignisse miteinander. Wenn ich also einen Fehler auf dem System habe, kann ich in der Überwachung sehen, dass die Maschine etwa unmittelbar aus dem Ruhezustand zurückgekommen ist, ein Treiber aktualisiert wurde, was entsprechend zum Absturz einer Applikation geführt hat. Also finde ich schon hier die Information, dass bestimmte Ereignisse zusammentreffen und diesen Fehler erzeugen. Wer meine Vorträge kennt, der weiß, dass mir letztes Jahr auf der ICE (Intelligent Communities for Europe) genau das passiert ist. Damals ist mir mein Rechner vom Tisch gefallen und die Zuverlässigkeitsüberwachung hat mir umgehend sinngemäß folgendes gemeldet: Pass auf, du solltest schleunigst eine Datensicherung machen, denn die Festplatte wird nicht mehr lange mitmachen. Und nach dem Vortag hat die Festplatte sich

tatsächlich verabschiedet. Hier hat mich also das Programm alarmiert, indem es vorzeitig gemeldet hat, dass ein Problem auf mich zukommt. Wegen verschiedener Fehler oder entsprechender Programmabstürze sank die Leistung des Geräts immer weiter. Mit dieser Kontrollmeldung habe ich einfach mehr Möglichkeiten, zu dem Fehler vorzudringen und ihn schneller zu finden. Ich muss nicht lange überlegen und in verschiedenen Logdateien suchen, sondern sehe alles in einer zentralen Ansicht.

Eine prima Sache, um proaktiv nach Fehlern zu suchen, und vielleicht auch, um Gegenmaßnahmen für Fehler zu ergreifen, bevor sie überhaupt auftreten. Das Beispiel von der ICE belegt das wunderbar: Das System sagt, sichere die Daten, die Platte macht es vielleicht nicht mehr lange. Das hättest du sonst erst gemerkt, wenn es zu spät gewesen wäre und die Platte sich schon verabschiedet hätte. Wie ist es mit Gruppenrichtlinien? Ich habe gehört, dass sich ihre Zahl nahezu verdoppelt hat und es daher auch deutlich größere Möglichkeiten gibt, um alles administrativ über ein Netzwerk zu verwalten. (08:46)

Gruppenrichtlinien zur zentralen Verwaltung – auch ein sehr schöner Punkt, weil man hier sehr einfach Dinge ändern und konfigurieren kann. Du hast es angesprochen, die Zahl der Richtlinien hat sich mehr als verdoppelt, ich glaube bei XP waren es knapp 700 Gruppenrichtlinien, die auf dem System mitgekommen sind. Bei Windows Vista sind wir jetzt ungefähr bei 3200 Gruppenrichtlinien. Diese im Einzelnen durchzugehen, halte ich für müßig. Und genauso lautet auch mein Rat an Unternehmen: Macht nicht den Fehler und setzt euch hin, um zu sehen, was es für neue Konfigurationsmöglichkeiten gibt, sondern geht den umgekehrten Weg. Überlegt, was will ich mit dem Desktop haben, welche Konfiguration möchte ich mit dem Desktop haben? Dann prüft ihr, wie ihr dieses Ziel über die Gruppenrichtlinien erreicht. Bei den Gruppenrichtlinien gibt es zum Teil große Änderungen. Sehen wir uns ein Beispiel mal genauer an: Internet Explorer 7, der zu Windows Vista gehört, kann komplett über die Gruppenrichtlinien administriert werden. Das ging in der Vergangenheit nicht ganz so einfach. Da musste man diese Konfigurationseinstellungen über andere Mechanismen anwenden. Wenn wir uns die Firewall-Konfiguration über die Gruppenrichtlinien ansehen, erkennen wir, dass die grafische Oberfläche zum Konfigurieren der Gruppenrichtlinien identisch mit der grafischen Oberfläche zum Konfigurieren der Firewall per System ist. Für mich als Administrator bedeutet das kein Umdenken à la „war das jetzt eine doppelte Verneinung?“ oder „welche Haken muss ich setzen?“, sondern ich benutze einfach die gleiche Oberfläche, die ich auch vom Klient kenne. Es gibt Gruppenrichtlinienvorlagen und ein neues Format. Das neue ADMX löst das alte Template-Format ADM ab. Das bietet natürlich ein XML-Format, womit ich auch andere Managementsysteme ansprechen oder Gruppenrichtlinien von anderen Quellen steuern oder generieren kann. Warum ausgerechnet ADMX? Ganz einfach, weil in Unternehmen, die global agieren, oft ein Problem auftritt: die Sprachkonfiguration oder sprachunabhängige Konfiguration. Wenn ich eine Gruppenrichtlinienvorlage für ein deutsches System einrichte, wird sie im Zweifelsfall nicht für die englischen Systeme in meinem Unternehmen angewandt. Je mehr Sprachen ich habe, umso mehr Vorlagen müsste ich also generieren. Mit dem ADMX-Format kann ich die Einstellungen für alle Sprachversionen in einer Vorlage definieren und das verschlankt natürlich die Verwaltung.

Sprich eine erheblich einfachere Verwaltung und ein geringerer administrativer Aufwand. Kommen wir zum Thema Deployment. Wie sieht es denn mit dem Deployment von Vista aus? In der Vergangenheit gab es verschiedene Möglichkeiten,

um größere Systemumgebungen zu verteilen. Ist das mit Vista auch einfacher und besser? (11:46)

Auch da haben wir eine dramatische Änderung innerhalb der Szenarien. Wenn ich Windows Vista als Endanwender im Elektronikfachhandel oder über sonst einen Kanal erwerbe, also die Box quasi kaufe und in mein System einlege, dann ist das kein Setup wie bei Windows XP oder Windows 2000. Stattdessen erwirbt man eine CD/DVD mit einem Image und genau darin liegt die Philosophie, die wir mit Windows Vista stärker verfolgen, das es immer nur um eine Imageverteilung geht. Für Unternehmensnetzwerke bedeutet das: Was auf meinem Datenträger liegt, ist schon mein fertiges Image, das ich entsprechend in meinem Unternehmensnetzwerk verteile. Ich kann unattended Parameter setzen – so wie unattended XML –, diese lösen also quasi TXT ab. Damit bieten sich mir auch hier mehr Möglichkeiten, Vorgaben bezüglich der Konfiguration zu geben. Mit dem Business-Desktop-Deployment (kurz BDD) haben wir ein Tool-Set generiert, mit dem man das auch einfach anpassen kann. Im Klartext heißt das, ich habe eine Oberfläche, mit der ich beispielsweise einstellen kann, dass mein Desktop nach dem Deployment über eine Bildschirmauflösung von 1024 X 768 verfügt, das Hintergrundbild identisch mit dem meines Unternehmens ist und der Bildschirmschoner so und so aussieht. Und das kann ich alles über dieses Tool konfigurieren. Imagebasierend bedeutet also auch die Möglichkeit unterschiedlicher Wege. Entweder erledige ich das über die grafische Oberfläche oder ich installiere mir einfach eine Windows Vista-Maschine, ändere dann alles, was ich haben möchte, und erstelle mir davon wiederum ein Image. Dazu gibt es ein entsprechendes Tool mit dem Namen Image X, das ich quasi starte, von diesem System mein Image ziehe, das dann eine Vorlage für das Deployment im Unternehmen bildet. Auch hier verlangt die Sprachenunabhängigkeit besondere Berücksichtigung, weshalb wir die Verteilung im Unternehmensnetzwerk stark reduziert haben. In der Vergangenheit gab es unterschiedliche Images, wenn ein Unternehmen XP genutzt hat. Beispielsweise ein deutsches für die Kollegen in Deutschland, ein englisches für die entsprechenden Kollegen in den USA oder Großbritannien und vielleicht noch ein französisches für die französischen Kollegen. Das macht schon drei unterschiedliche Images. Dazu kamen vielleicht fünf, sechs oder noch mehr unterschiedliche Hardwaretypen wie Laptops, Desktop PCs und andere, die auch alle entsprechende Anpassungen und neue Images erforderten. Das hieß, viele Images vorbereiten und auch pflegen zu müssen. Bei jedem Aktualisieren des Systems musste man alle Images einzeln berücksichtigen. Windows Vista liefert ein Image für alle Sprachversionen und alle Hardwareversionen. Beim Aktualisieren kann ich dieses Image einspielen und muss nur noch ein Image-Set pflegen. Auch hier kann ich wohlweislich unterschiedliche Konfigurationen walten lassen. Wenn ich einen Desktop für eine Sekretärin einrichte, mit wenig Anwendungen und einer restriktiven Konfiguration und daneben aber für meine Entwickler eine offenere, freizügigere Umgebung konfigurieren möchte, habe ich immer noch ein Image, allerdings mit unterschiedlichen Beschreibungsdateien und Unterkapiteln in meiner attended AMX-Datei. Vor dem Installieren lege ich fest, welche Editionen ich wählen will – die und die Version, mit unterschiedlichen Berechtigungen für die verschiedenen Anwender – und dann kann ich entsprechend installieren. Ein weiterer Vorteil der imagebasierten Verteilung liegt in der immensen Zeitersparnis. Eine reine Vista-Installation ohne weitere Applikationen dauert im Schnitt je nach Netzwerk- oder Festplattenperformance im System 20 Minuten. Wenn noch weitere Dinge, wie beispielsweise Office dazukommen, dauert es natürlich länger. Aber in 20 Minuten hat man ein entsprechendes Betriebssystem installiert, egal ob das Image von der DVD stammt oder vom Netzwerk installiert wird.

Der Deployment-Prozess ist also erheblich einfacher geworden. Und ich kann trotzdem weiterhin verschiedene Systeme adressieren, was unterschiedliche Hardware angeht, verschiedene Nutzergruppen adressieren, was die Nutzung angeht, und verschiedene Sprachvarianten, verschiedene Nutzungsbedingungen sowie restriktivere Desktops umsetzen. Du hast gesagt, dass man Software mit installieren und verteilen kann. Wie ist das bei Vista? Ich gehe natürlich davon aus, dass ich alle Microsoft-Software einbauen kann, aber wie sieht das bei Non-Microsoft-Software aus, kann ich die auch mit einem Vista-Image ausrollen? (16:13)

Natürlich kannst du auch andere Applikationen, Nicht-Microsoft-Applikationen über diesen Mechanismus verteilen. Auch da gibt es unterschiedliche Mechanismen. Entweder machst du, wie gesagt, einen Schnappschuss vom Rechner, ziehst also quasi ein Image von einem installierten Rechner. In dem Fall ist alles, was du an Tools oder anderen Applikationen möchtest, schon installiert. Damit kannst du das Image zusammenbauen. Der andere Weg liefe über die Workbench, die im BDD integriert ist. Damit kannst du auch eigene Applikationen hinzufügen und andere Applikationen von Fremdherstellern, um sie dann in diesem Image oder über diesen Mechanismus zu verteilen.

Also auch hier erheblich weniger Aufwand, alles ist einfacher zu administrieren und ich habe trotzdem alle Möglichkeiten, die ich vorher auch hatte, und sogar noch einige mehr. Kommen wir zum ganz großen Thema – zur Sicherheit. Microsoft sagt, Vista sei das sicherste System, das es bisher gab. Und da fällt mir gleich das Thema überhaupt ein, wenn es um Vista geht: User Account Control. Was kannst du uns darüber sagen? (17:23)

User Account Control adressiert einfach einen Zustand, der über die Jahre gewachsen ist. Wenn man mit administrativen Rechten auf einem Rechner unterwegs ist, wirkt sich alles, was man tut, jede Aktion, die man ausführt, vielleicht auf das System aus. Denn wenn ich mit den höchsten Privilegien Aktionen vornehme, werden diese einfach erledigt und es gibt oft gar keine große Nachfrage. Viele Applikationshersteller gehen davon aus, dass der Anwender auch der Administrator ist und sie daher in den Systembereich schreiben können. Oder es wird von den Herstellern in Bereiche der Registry geschrieben, die normalerweise für das Betriebssystem wichtig sind, einfach eine Konfiguration geändert, DLLs werden mit denen des Applikationsherstellers ausgetauscht, die für das Betriebssystem wichtig sind. Das alles führt natürlich dazu, dass das System nicht mehr so stabil arbeitet. User Account Control schützt vor der wahllosen Vergabe administrativer Privilegien und sorgt dafür, dass man sie erst dann einholt beziehungsweise bekommt, wenn man sie braucht. Sprich, bei bestimmten administrativen Tätigkeiten gibt es noch eine Instanz, die nachfragt: „Hey willst du das jetzt wirklich? Bist du dir da auch ganz sicher?“ oder „Du bist momentan in einem Bereich, in dem du die Konfigurationseinstellungen ändern willst“, was man einfach noch einmal bestätigt. Dabei gibt es zwei unterschiedliche Ansätze. Zum einen, ich bin Mitglied der lokalen Administratorgruppe und bekomme nur so einen Bestätigungsdialog oder ich bin eben kein Mitglied der Administratorgruppe. Für den zweiten Fall gibt es ein entsprechendes Account Login, das heißt, jemand der lokale Administratorrechte besitzt, kann dort Benutzernamen und Kennwort eingeben. Ein paar Dinge sollten dabei beachtet werden. Dieser Dialog, der einfach nur eine Bestätigung liefert, informiert natürlich auch darüber, ob die Applikation, die diesen Dialog verursacht hat, eine von Windows kompilierte Komponente oder eine Nicht-Microsoft-Komponente ist, die diese Berechtigung anfordert. Innerhalb des Dialogs gibt es schon einmal farbliche Unterscheidungen, sowohl bei der Eingabe von Benutzername und Kennwort als auch beim Bestätigen. Zum anderen gibt es das Ausgrauen

des Bildschirms, der dieses Fenster fokussiert. Windows Vista funktioniert so, dass jedes einzelne Fenster auf einer eigenen virtuellen Ebene transparent ist. Ich habe also mehrere Fenster, in unterschiedlichen Schichten übereinander, und jedes Fenster kann mit den anderen kommunizieren. So kann ich durchaus von einem Fenster ein Kommando zum anderen Fenster schicken, mit der Botschaft: „Hey klick mir bitte mal auf okay“. Um genau das zu verhindern, gibt es dieses Ausgrauen, als virtuelle Security Ebene, den Secure-Desktop. Dort kann ich keine Kommandos zum Fenster schicken, weil das User-Account Control schließlich sofort ab absurdum führte. Das heißt also, diese Dialogbox, die mir die Möglichkeit gibt, auf okay oder abbrechen zu klicken, ist eigentlich die sicherste Form des URC-Dialogs. Wenn wir uns das einmal ansehen: Benutzerkennwort-Eingabe, den Bildschirmhintergrund abdimmern – wo immer ich als Anwender Kennwortinformationen oder meinen Account preisgebe, birgt das potenzielle Möglichkeiten für Angreifer, quasi Fälschungen dieses Dialogs zu veröffentlichen. Nehmen wir ein ganz normales Bankterminalprogramm – wie kann ich da sicher sein, dass es auch wirklich die PIN-/TAN-Abfrage meiner Bank ist und mir nicht vielleicht jemand dieses Fenster einfach untergeschoben hat. Genauso gäbe es vielleicht eine Möglichkeit, das bei Vista zu tun. User-Account Control garantiert mir, dass der Dialog auch tatsächlich vom Betriebssystem kommt. User-Account Control kann deaktiviert werden. Wer das also nicht möchte oder vielleicht im Unternehmensbereich eine administrative Konsole hat und häufig administrative Dinge erledigt, für den macht es natürlich keinen Sinn, dass er sich hundert Mal am Tag sicher ist. In dem Fall würde ich raten, User-Account Control abzuschalten. Ansonsten kann ich nur sagen, wenn ich ganz normal mit meinem System arbeite, also nicht gerade auf der Bühne stehe und dieses Feature demonstriere, taucht der Dialog bei mir eigentlich nicht auf, weil ich meine Mails abarbeite, vielleicht mal eine virtuelle Maschine starte, um ein paar Sachen auszuprobieren, ansonsten aber keine administrativen Dinge auf meinem System ändere, höchstens einmal in der Woche, und dann kommt man schon ganz gut damit zurecht.

Also kann der Administrator weiter mit seinem administrativen Account arbeiten, aber dazwischen liegt jetzt User Account Control. Und wenn er Tätigkeiten ausführt, die systemrelevant sind oder administrative Rechte benötigen, werden diese nicht einfach ausgeführt, sondern das System stellt eine Frage und sagt sinngemäß: „Pass auf, da will jemand, wer auch immer das ist, etwas ändern, bist du damit einverstanden oder nicht?“. Und dieser Dialog liegt über dem eigentlichen System. Wenn nun ein Virus oder Wurm das System infiziert und das System diesen Dialog startet, kommen Virus oder Wurm dann gar nicht an den Dialog ran? Weil signalisiert wird, dass irgendjemand zugreifen will. Dann startet automatisch der Dialog und unten drunter ist alles still gelegt, so dass nichts ausgeführt werden kann – außer wenn ich sage: Mach das. Habe ich das richtig verstanden? (22:30)

Exakt richtig. Vielleicht sollte ich noch erklären, wie das technisch funktioniert. Also, ich habe vielleicht fünf, sechs Applikationen offen und lade dann die MMC-Konsole, weil ich etwas administrieren will. Im nächsten Moment erscheint der Dialog, weil MMC die Möglichkeit bietet, administrative Dinge zu beeinflussen. Beim Starten von MMC werden administrative Privilegien ausgeführt und alles andere bleibt wie es ist. Sobald ich die Applikation schliesse, wird diese Ansicht quasi rückgängig gemacht, und ich kann ganz normal weiterarbeiten.

Aus meiner Sicht eine tolle Sache, da die meisten Probleme bisher doch daraus entstanden sind, dass Leute einfach aus Bequemlichkeit – und da nehme ich mich selbst nicht aus – gern als Administrator angemeldet waren und dadurch natürlich auch für alles, was im Hintergrund lief, die gleichen administrativen Rechte hatten.

User Account Control wird vielleicht noch eine Zeit lang heiß diskutiert werden, aber ich finde, das ist ein großer Schritt in die richtige Richtung. (24:12)

Selbst wenn das nur dazu führt, dass die Anwendungsentwickler endlich in die richtigen Bereiche schreiben und nicht in systemrelevante Zweige, haben wir unser Ziel erreicht.

Weitere Sicherheitsfeatures wären zum Beispiel Windows Defender. Was kannst du uns zu Windows Defender erzählen? (24:45)

Viele Anwender wünschen sich ja immer die totale Kontrolle über das System, weil sie wissen wollen, was momentan auf ihrem System geändert wird und was überhaupt an Kommunikation abläuft. Windows Defender ist so ein Tool und dient als zweite oder dritte Sicherheitsinstanz neben den anderen integrierten Merkmalen, wie beispielsweise User Account Control, oder Internet Explorer 7 in Protected Mode. Defender analysiert und erkennt Änderungen am System. Wenn ich beispielsweise ganz normal eine Software installiere, etwa eine Shareware, und mir die Lizenzbedingungen nicht durchgelesen habe. Das sollte man spaßeshalber mal machen, weil ganz unten häufig so etwas steht wie, „ach übrigens, wenn ich installiert werde, dann installiere ich noch ein bisschen Ad-Ware und sonstige Programme mit“. Das würde Defender erkennen und mir sagen: „Pass auf, du installierst gerade eine Software, die übrigens noch weitere Software installiert. Willst du das haben oder nicht?“. Dann kann ich als Anwender sagen: „Nein, die Ad-Ware will ich nicht“ und kann sie explizit blocken. Defender geht noch einen Schritt weiter. Wann immer ich einen anderen Fehler gemacht habe, vielleicht bei einem Download aus dem Internet oder mit dem Anklicken einer Datei, die wiederum andere Dinge ausführt wie Änderungen am System vorzunehmen oder Registry-Einstellungen und sogar die Hostdatei ändert, um IP Zuordnungen zu manipulieren, wird Defender aktiv und sagt: „Hier pass auf, gerade wird eine Änderung in deiner Hostdatei ausgeführt, da nimmt einer eine Zuordnung von einer IP Adresse zu einer entsprechenden Website vor, willst du das, ja oder nein?“ Und auch in dem Fall kann ich noch entsprechend eingreifen. Im Unternehmensbereich ist es vermutlich nicht so sinnvoll, die Kontrolle über Defender dem Endanwender zu überlassen. Dafür haben wir entsprechendes Werkzeug, Forefront Client Security, mit dem man genau diese Meldungen an einer zentralen Administratorkonsole auflaufen lassen kann und dann als Admin entscheidet, was auf dem System passiert – will ich, dass die Komponente installiert wird oder nicht. Das ist jetzt immer noch ein Unterschied zum Unternehmensnetzwerk, aber Defender ist quasi der stille Wächter im Hintergrund, der überprüft, dass nichts schief geht.

Ein großes Sicherheitsproblem für viele Unternehmen liegt meiner Ansicht nach in den mobilen Arbeitsplätzen der Mitarbeiter, sprich den Notebooks. Schon mit Windows XP gab es ja die Möglichkeit, die Festplatte entsprechend zu verschlüsseln. Aber wenn jemand physikalisch an das Notebook gekommen ist, es beispielsweise auf dem Flughafen geklaut hat, dann konnte diese Person sich mit entsprechenden Werkzeugen durchaus administrativen Zugang verschaffen und so auch die Verschlüsselung wieder aufheben. Bei Windows Vista gibt es nun BitLocker. BitLocker kann das erheblich restriktiver handhaben als XP mit der Festplattenverschlüsselung. Was genau ist mit BitLocker sicherer geworden? (26:54)

Die Antwort liegt ja schon fast in deiner Frage, denn viele verstehen BitLocker in der Tat falsch und sagen: „Hey, BitLocker ist die Festplattenverschlüsselung, meine Daten sind sicher“. Das stimmt nur begrenzt. Wir werden alle immer mobiler. Fast jeder besitzt ein Laptop. Auf dem Flughafen sieht man es ganz häufig, das ist besonders interessant. Aber

was ist nun der Zweck von BitLocker? Ganz einfach: zu verhindern, dass jemand, wenn er mein System in die Hände bekommt, den entsprechenden Zugriff auf das System erhält, mit der Absicht, meine Daten zu lesen. BitLocker adressiert quasi diesen Secure StartUp, wenn man so will, denn ich kann nicht mehr von einer fremden Betriebssystem-CD booten, das Admin-Kennwort zurücksetzen und mich dann auf dieser Maschine einloggen. Vielmehr habe ich einen Schutz, so dass mein „Kontroll-Alt-Benutzername-Kennwort“ eben wirklich das entscheidende Sicherheitsmerkmal ist. Denn nur mit gültigen Anmeldeinformationen erhalte ich Zugriff zum System. Das schafft schon einmal eine entsprechend sichere Basis. Man könnte sich jetzt umgekehrt fragen, ob eine Smartcard-Implementierung oder andere Sicherheitstechnologien denn überhaupt Sinn machen, wenn ich ein System habe, das nicht einmal über BitLocker verfügt? Schließlich muss ich ja nur das System kompromittieren und schon habe ich diese ganzen Sicherheitsvorkehrungen unterwandert. Darum ist BitLocker ein sehr wichtiges Tool, das einen Angriff von außen nicht mehr ermöglicht. Was passiert genau? Die Systempartition unter Windows Vista wird verschlüsselt und damit automatisch alle Daten, die auf dieser Partition liegen, also auch das Windows-Verzeichnis, Cachefile und Registry. All diese Dateien sind dann verschlüsselt und ohne den entsprechenden Key kann das Betriebssystem die Informationen auf der Platte nicht lesen. Für den Einsatz des Keys gibt es unterschiedliche Szenarien, ich kann ihn auf einem USB-Stick speichern oder beispielsweise ein eingebautes Trusted Plattform Modul (kurz TPM) nutzen, um Schlüsselinformationen abzuspeichern und dann den „Secure Start Up“ zu nutzen.

Danke, auch in meinen Augen ist das ein sehr wichtiger Punkt, denn ich möchte nicht wissen, wie viele Tausende Notebooks jeden Monat auf Flughäfen und in Cafés verschwinden. Die Kosten für die Hardware sind dabei sicher der geringste Verlust, viel schlimmer ist, dass viele Daten in die falschen Hände gelangen. Durch BitLocker ist das jetzt besser zu handhaben und erheblich sicherer. Vorhin hast du erzählt, dass dein Notebook auf der letzten ICE zum Glück erst nach deinem Vortrag den Geist aufgegeben hat. Was hat sich in Sachen Backup und Restore-Mechanismen denn Neues mit Vista getan? (29:56)

Backup und Restore – auch da gehen die Meinungen weit auseinander. Wir haben die Backup- und Restore-Funktionen, die im Betriebssystem mit integriert ist, sehr stark vereinfacht. Unter XP konnte ich noch sehr granular wählen, was ich sichern will, über bestimmte Verzeichnisse und Ähnliches. Das kann ich unter Vista so jetzt nicht mehr. Diesen „Marktplatz“ haben wir früher all den kleinen Tool-Herstellern überlassen, die Backup-Tools auf den Markt bringen. Mit Windows Vista habe ich zwei Möglichkeiten oder sagen wir lieber drei: Erstens, ich sage, ich will alle meine Daten sichern. Dann wird alles, was in meinem User-Bereich gehört, gesichert, natürlich auch die Einstellungen der eigenen Applikationen. Das ist die eine Art des Backups. Als zweites kann ich ein komplettes System-Backup machen und drittens ein System-Backup, das ich später wieder als komplette Installation benutzen kann. Also zwei unterschiedliche Herangehensweisen, bei der ersten sage ich: „Okay, ich starte mein Vista und spiele mein komplettes Backup wieder ein.“ Und bei der zweiten installiere ich quasi mein Backup, habe also ein Image meines Systems, so wie wir das vorhin schon einmal besprochen haben. Dieses Image spiele ich einfach komplett wieder zurück und kann so natürlich auch wieder sehr einfach meine Maschine sichern. Unser Ziel war es, auch dem Heimanwender die Möglichkeit zu geben, ein komplettes Abbild seines Rechners, so wie er jetzt ist, einfach wegzuschreiben und, wann immer etwas kaputt geht, alles wieder einzuspielen und genau an den Punkt zu kommen, den er festgehalten hat.

Also einerseits die Möglichkeit, meine persönlichen Einstellungen zu sichern, um nach einem Systemcrash erst Vista zu installieren und dann meine persönlichen Einstellungen und Installationen darauf zu schreiben oder auch ein komplettes Image zu ziehen. Was ja auch mit Drittanbieter-Tools geht und somit quasi mein eigenes, persönliches Deployment auf meinem eigenen System ermöglicht. Klasse Sache. (32:07)

Michael, ich danke dir, dass du dir Zeit für uns genommen hast, uns ein paar Fragen beantwortet und uns geholfen hast, besser zu verstehen, was hinter Vista steht und was für neue Möglichkeiten wir damit haben.

Auch von meiner Seite herzlichen Dank für die Möglichkeit, mit dir in lockerer Atmosphäre ein wenig zu fachsimpeln. Ich hoffe, es hat ein paar Informationen gegeben, die so vielleicht noch nicht bekannt waren. Ansonsten gilt natürlich immer die Einladung, auf Blogs: <http://blogs.technet.com/mkalbe> vorbeizuschauen.

Danke, dass ihr euch die Zeit genommen habt, uns zuzuhören und etwas Neues über Vista zu erfahren. Wenn ihr noch Fragen habt, stellt sie bitte – und zwar alle – in www.mcseboard.de, dem entsprechenden Vista-Unterforum. Wir werden alle noch offenen Fragen beantworten und sollte sich herausstellen, dass wir noch mehr Zeit brauchen, wird Michael Kalbe sich hoffentlich bereit erklären, weitere Fragen zu beantworten. Vielen Dank.