

Deutschland

Microsoft TechNet

Windows Vista - Verbesserungen aus den Bereichen Sicherheit und Datenschutz

Veröffentlicht: 01. Jun 2005
Von Tony Northrup

Sicherheitsbedrohungen nehmen konstant zu. Um vor Bedrohungen aus dem Internet und über WLANs sicher zu sein, muss sich das Windows-Betriebssystem also ebenfalls weiterentwickeln. Windows Vista ist das zurzeit sicherste und vertrauenswürdigste Windows-Betriebssystem. Es wird Organisationen darin unterstützen, ihre geschäftlichen Ziele und ihre IT-Ziele sicher umzusetzen. In diesem Dokument werden die wichtigsten Sicherheitsverbesserungen, die so erzielten Vorteile und der Nutzen der neuen Features für IT-Experten vorgestellt.



Auf dieser Seite

- ↓ [Überblick](#)
- ↓ [Benutzerkontenschutz](#)
- ↓ [Authentifizierung](#)
- ↓ [Anti-Malware](#)
- ↓ [Netzwerkzugriffsschutz \(Network Access Protection\)](#)
- ↓ [Firewall](#)
- ↓ [Absicherung der Dienste \(Windows Service Hardening\)](#)
- ↓ [Internet Explorer-Erweiterungen](#)
- ↓ [Datenschutz](#)

Überblick

Microsoft nimmt grundlegende Investitionen in Technologien vor und schafft so für die Kunden mehr Sicherheit. Zu den entsprechenden Bemühungen zählen zum Beispiel ein neuer Security-Development-Lifecycle zur Entwicklung sichererer Software und Technologieinnovationen, die eine mehrschichtige Sicherheitsstrategie ermöglichen. Windows Vista umfasst eine Menge Sicherheitsfeatures und -verbesserungen, die Clientcomputer vor den neusten Bedrohungen wie Würmer, Viren und anderen schädlichen Programmen (allgemein unter dem Begriff *Malware* zusammengefasst) schützen.

- Der Benutzerkontenschutz ermöglicht es Benutzern, ohne administrative Rechte produktiv zu arbeiten und allgemeine Systemeinstellungen zu ändern. So wird verhindert, dass die Benutzer potenziell gefährliche Änderungen vornehmen. Gleichzeitig sind sie jedoch in der Lage, Anwendungen auszuführen.
- Microsoft Internet Explorer (IE), der standardmäßige Webbrowser von Windows Vista, hat viele Erweiterungen im Bereich Sicherheit erfahren. Er schützt den Benutzer vor Phishing- und Spoofing-Angriffen. Ein neues Feature ist zum Beispiel der geschützte Modus. Dieser verhindert, dass Websites oder Malware die Daten des Benutzers missbrauchen oder Konfigurationsänderungen vornehmen.
- Windows Vista erkennt viele Arten potenziell gefährlicher Software und kann den Benutzer vorab auf die entsprechenden Anwendungen hinweisen.
- Neue Filter für ausgehenden Netzwerkverkehr ermöglichen eine administrative Kontrolle über Peer-to-Peer-Filesharing-Anwendungen.
- Die Absicherung der Dienste (Windows Service Hardening) schränkt den Schaden, den Angreifer im unwahrscheinlichen Fall einer Kompromittierung eines Dienstes anrichten können, deutlich ein.
- Administratoren können den Netzwerkzugriffsschutz (Network Access Protection) nutzen, um den Zugriff auf das interne Netzwerk für die Clients zu verhindern, die nicht den Vorgaben entsprechen. So wird die

potenzielle Ausbreitung von Malware auf andere Rechner verhindert.

In Unternehmen mit entsprechender Hardware wird der sicherere Startvorgang im Fall von verlorenen oder gestohlenen Computern die Daten schützen. Bei einem Computer, der den sicheren Startvorgang nutzt, ist die gesamte Festplatte verschlüsselt.

Um sicherzustellen, dass eine große Menge an unterschiedlichen Authentifizierungsmechanismen zur Auswahl steht, nutzt Windows Vista eine neue Authentifizierungsarchitektur. Diese macht es Drittanbietern einfacher, neue Mechanismen zu integrieren.

[↑ Zum Seitenanfang](#)

Benutzerkontenschutz

Beschreibung des Features

Im Moment arbeiten viele Windows-Benutzer mit administrativen Rechten - und zwar sowohl im Unternehmen als auch zu Hause. Dies führt dazu, dass die Arbeitsstationen schwer zu verwalten sind und das die Supportkosten potenziell sehr hoch sind. Die Arbeitsstationen so einzurichten, dass die Benutzer nicht mit administrativen Rechten arbeiten, kann Kosten sparen. Die Benutzer haben so nicht die Möglichkeit, fehlerhafte oder versehentliche Konfigurationen vorzunehmen oder Anwendungen zu installieren, die die Systemstabilität beeinflussen. Leider ist die Arbeit ohne administrative Berechtigungen im Moment problematisch. Viele Anwendungen werden nicht korrekt ausgeführt, und die Benutzer sind nicht in der Lage, häufig auftretende Aufgaben, wie zum Beispiel das Hinzufügen von Druckern, auszuführen. Der Benutzerkontenschutz von Windows Vista stellt eine grundlegende Änderung des Betriebssystems dar und vereinfacht das Arbeiten für nicht-administrative Benutzer. Ein mobiler Benutzer ist zum Beispiel in der Lage, einen WEP-Schlüssel einzurichten und so einem WLAN beizutreten, einen Drucker einzurichten, Anwendungsupdates herunterzuladen und zu installieren, eine VPN-Verbindung einzurichten und zu konfigurieren und viele andere häufig auftretende Aufgaben auszuführen - und das alles ohne administrative Rechte.

Standardmäßig werden die meisten Anwendungen unter Windows Vista mit eingeschränkten Rechten ausgeführt. Dies gilt sogar dann, wenn der Benutzer mit administrativen Rechten angemeldet ist. Dieses Feature wird jedoch nicht verhindern, dass Benutzer die gewollten administrativen Aufgaben ausführen. Wenn eine solche Aufgabe ausgeführt werden soll, dann fragt Windows Vista explizit nach einer Bestätigung oder fordert administrative Anmeldeinformationen an. Dieses Feature kann außerdem über Gruppenrichtlinien gesteuert werden.

Wenn sich Benutzer anmelden, die nicht Mitglieder der lokalen Gruppe Administratoren sind, dann können diese trotzdem die meisten Windows Vista-Anwendungen ausführen - ohne dass weitere Rechte erforderlich sind.

Wenn dennoch administrative Rechte erforderlich sein sollten, dann müssen Sie nicht das **Ausführen als**-Feature bemühen. Windows Vista fordert die entsprechenden Anmeldeinformationen automatisch an.

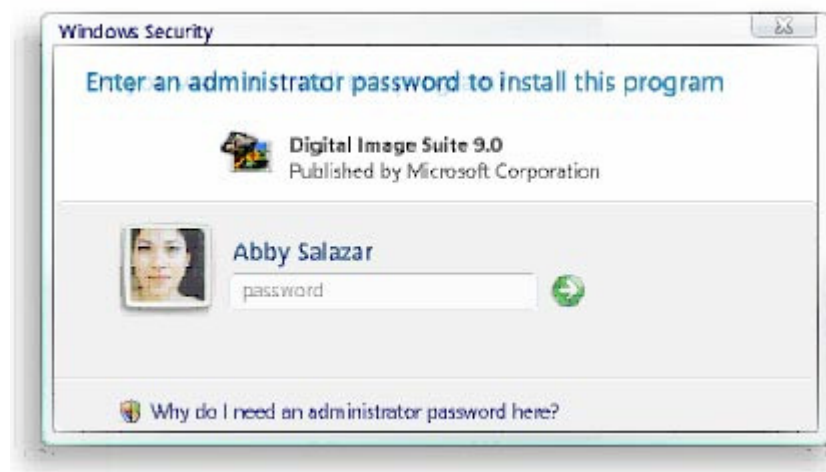


Abbildung 1: Windows Vista fordert bei Bedarf automatisch administrative Anmeldeinformationen an.

Unter Windows XP können einige Anwendungen nicht ohne administrative Rechte ausgeführt werden. Dies liegt daran, dass diese Anwendungen versuchen, Änderungen an Dateien oder an der Registrierung vorzunehmen, die sich auf den gesamten Computer auswirken (zum Beispiel C:\Programm, C:\Windows, oder HKEY_LOCAL_MACHINE. Die Virtualisierung der *Registrierung und des Dateisystems* von Windows Vista leitet diese Schreibzugriffe um (wenn der Benutzer nicht über administrative Rechte verfügt).

Vorteile

Der Benutzerkontenschutz ermöglicht es Organisationen, zu einer besser verwaltbaren Umgebung zu wechseln und so die Supportkosten zu senken. Er führt dazu, dass weniger Arbeitsstationen neu aufgesetzt werden müssen und dass die Systeme weniger von Malware-Angriffen betroffen sind.

Auswirkungen

Unter Windows XP hatten die Administratoren zwei Alternativen:

- Den Benutzern administrative Rechte zu geben und mit den so häufiger auftretenden Supportfällen durch fehlerhafte Installationen oder Konfigurationen zu leben.
- Den Benutzern eingeschränkte Rechte zu geben und mit den Supportfällen durch nicht korrekt funktionierende Anwendungen zu leben.

Unter Windows Vista müssen Sie keine Kompromisse mehr eingehen. Die Benutzer können produktiv arbeiten, sind durch die fehlenden administrativen Rechte vor Malware geschützt und können weiterhin fast jede Anwendung ausführen. Wenn der Benutzer tatsächlich administrative Aufgaben ausführen muss, dann fordert Windows Vista eine Bestätigung an. Dies wird zu weniger Supportfällen führen. Außerdem wird weniger Zeitaufwand dafür erforderlich sein, Anwendungen so einzurichten, dass sie mit fehlenden administrativen Rechten ausgeführt werden können.

[↑ Zum Seitenanfang](#)

Authentifizierung

Beschreibung des Features

Windows Vista unterstützt auch weiterhin standardmäßig Kennwörter und Smart Cards. Da jedoch viele Kunden nach Alternativen zu diesen beiden Authentifizierungsverfahren suchen, vereinfacht Windows Vista die Implementierung von eigenen Authentifizierungsmöglichkeiten durch externe Entwickler (zum Beispiel Biometrieverfahren). Windows Vista erweitert außerdem das Kerberos-Authentifizierungsprotokoll und Anmeldungen über Smart Cards. Tools zur Bereitstellung und Verwaltung von Smart Cards (zum Beispiel PIN-Reset-Tools) vereinfachen die Handhabung von Smart Cards. Ein API-Modell vereinfacht die Entwicklung.

Vorteile

Die Verbesserungen bezüglich der Smart Cards machen es Organisationen einfacher, eine entsprechende Authentifizierung bereitzustellen und zu supporten. Entwickler profitieren durch die einfachere Implementierung neuer Authentifizierungsmöglichkeiten. Es stehen mehr Möglichkeiten zur Verfügung, auf Lösungen von Drittanbietern zurückzugreifen.

Auswirkungen

In vielen Organisationen ist eine Single-Factor-Authentifizierung nicht ausreichend. Wenn eine hohe Sicherheit erforderlich ist, muss eine Multi-Factor-Authentifizierung eingesetzt werden. Durch die einfacheren Möglichkeiten für Entwickler, eigene Lösungen zu integrieren, stehen den Unternehmen mehr Authentifizierungsmöglichkeiten zur Verfügung.

[↑ Zum Seitenanfang](#)

Anti-Malware

Beschreibung des Features

Der weiter oben besprochene Benutzerkontenschutz und die Sicherheitsverbesserung des Internet Explorers (inklusive des weiter unten diskutierten geschützten Modus) können die Risiken durch Malware reduzieren.

Zusätzlich kann Windows Vista viele Würmer, Viren, Rootkits oder Spyware-Programme beseitigen, und es stellt so die Integrität des Betriebssystems und den Schutz der persönlichen Dateien der Benutzer sicher.

Anmerkung: Die standardmäßige Anti-Spyware-Funktionalität richtet sich an Endbenutzer. Sie unterstützt keine Verwaltung für Unternehmensumgebung.

Vorteile

Malware führt oft zu einer Verschlechterung der Systemperformance. Dies führt dann oft dazu, dass die Benutzer ihre Computer als zu langsam oder zu unzuverlässig empfinden und die Computer neu aufgesetzt werden. Die größte Bedrohung durch Malware betrifft jedoch die Sicherheit. Malware kann zum Beispiel vertrauliche Daten kompromittieren oder zu neuen Sicherheitslücken führen. Daher verbessert der Schutz vor Malware die Leistung und die Sicherheit des Computers.

Auswirkungen

IT-Abteilungen wenden viel Zeit dafür auf, Probleme durch Malware zu beseitigen (langsame Computer, schlechte Zuverlässigkeit und Sicherheitsprobleme). Die Anti-Malware-Features von Windows Vista beseitigen schädliche Software und ermöglichen den Benutzern mehr Kontrolle darüber, welche Programme auf ihren Computern installiert werden.

[↕ Zum Seitenanfang](#)

Netzwerkzugriffsschutz (Network Access Protection)

Beschreibung des Features

Windows Vista nutzt einen Agenten, der einen Client daran hindert, auf Ihr privates Netzwerk zuzugreifen, wenn dieses nicht über die aktuellsten Sicherheitsupdates, Virensignaturen oder andere zwingende Voraussetzungen verfügt. Der Netzwerkzugriffsschutz kann Ihr Netzwerk vor RAS-Clients und vor LAN-Clients schützen. Der Agent übermittelt den Status des Clients an einen serverbasierten Dienst. Dann legt eine von Windows Server "Longhorn" zur Verfügung gestellte entsprechende Infrastruktur fest, ob der Client einen Zugriff auf das private Netzwerk oder auf ein eingeschränktes Netzwerk erhält.

Vorteile

Der Netzwerkzugriffsschutz kann Statusanforderungen für mobile Computer, Remotecomputer und LAN-Clients durchsetzen. Benutzer, die ihre Computer mit sich führen, sind oftmals nur einmal pro Woche oder seltener in der Lage, sich mit dem privaten Netzwerk zu verbinden. Wenn sie denn eine Verbindung aufbauen, reicht die Zeit oftmals nicht aus, um die aktuellsten Updates, Konfigurationseinstellungen oder Virensignaturen herunterzuladen. Daher entspricht der Status mobiler Computer oftmals nicht den Unternehmensanforderungen. Der Netzwerkzugriffsschutz verbessert die Sicherheit dieser Computer und sorgt dafür, dass diese vor einer Verbindung mit dem privaten Netzwerk über die erforderlichen Updates verfügen.

Auswirkungen

Viren und Würmer werden oftmals durch mobile Computer oder Remotecomputer in private Netzwerke eingeschleust. Der Netzwerkzugriffsschutz von Windows Vista ermöglicht es Ihnen, Anforderungen für solche Computer durchzusetzen. Wenn ein Client diesen Anforderungen nicht entspricht, haben Sie die folgenden Möglichkeiten:

- Verhindern, dass der Computer sich mit dem privaten Netzwerk verbindet und möglicherweise Viren und Würmer verbreitet.
- Dem Benutzer Anweisungen zur Verfügung stellen, mit denen dieser seinen Computer aktualisieren kann, oder die Aktualisierung automatisch durchzuführen.
- Dem Benutzer einen Zugriff auf eine beschränkte Anzahl von Servern im privaten Netzwerk ermöglichen und diesen so die erforderlichen Updates herunterladen zu lassen.

[↕ Zum Seitenanfang](#)

Firewall

Beschreibung des Features

Die Firewall von Windows Vista baut auf der Funktionalität von Microsoft Windows XP Service Pack 2 auf. Sie führt Filter für ausgehenden Netzwerkverkehr auf Anwendungsbasis ein. Die Windows Firewall ermöglicht es Administratoren beispielsweise, Anwendungen zu blockieren (zum Beispiel File-Sharing-Clients oder Instant-Messaging-Anwendungen). Außerdem sind alle Windows Vista-Firewalleinstellungen über Gruppenrichtlinieneinstellungen konfigurierbar.

Vorteile

Viele potenziell gefährliche Anwendungen, wie zum Beispiel File-Sharing-Anwendungen, umgehen Firewalls, die eingehende Verbindungen blockieren. Die Firewall von Windows Vista gibt Administratoren nun die Möglichkeit, zugelassene oder blockierte Anwendungen über Gruppenrichtlinien festzulegen.

Auswirkungen

Einer der wichtigsten Wege, über die Administratoren Sicherheitsrisiken minimieren können, ist, den Netzwerkzugriff für Anwendungen einzuschränken. Die Firewall von Windows Vista ist Teil einer solchen Strategie. Mit ihr können Administratoren das Ausführen einer Anwendung genehmigen, ihren Netzwerkzugriff jedoch gleichzeitig einschränken.

[↑ Zum Seitenanfang](#)

Absicherung der Dienste (Windows Service Hardening)

Beschreibung des Features

Die Absicherung der Dienste schränkt die Möglichkeit von kritischen Windows-Diensten ein, unerwünschte Aktionen bezüglich des Dateisystems, der Registrierung, im Netzwerk oder anderer Ressourcen durchzuführen. Der RPC-Dienst kann zum Beispiel so eingeschränkt werden, dass er keine Systemdateien ersetzen oder die Registrierung verändern kann.

Windows-Dienste stellen einen großen Teil der Angriffsfläche eines Systems dar. Windows Vista schränkt die Anzahl der ausgeführten Dienste ein. Viele Systemdienste und Dienste von Drittanbietern werden im Moment unter dem lokalen Systemkonto ausgeführt. Bei diesen Diensten kann ein Sicherheitsproblem zu einem enormen Schaden für den betreffenden Computer führen (inklusive einer Formatierung der Festplatte, einem Zugriff auf die Benutzerdaten oder der Installation von Treibern).

Die Absicherung der Dienste reduziert den möglichen Schaden durch kompromittierte Dienste durch neue Konzepte bezüglich der Windows-Dienste:

- Es wird ein Service Security Identifier (SID) für jeden Dienst eingeführt. Dieser führt dazu, dass jeder Dienst über eine Identität verfügt, was wiederum eine Steuerung über ACLs über das bestehende Zugriffsmodell von Windows ermöglicht. Sie können nun explizit ACLs auf Ressourcen anwenden, die nur einem bestimmten Dienst zur Verfügung stehen. So können Sie verhindern, dass andere Dienste oder Benutzer auf diese Ressourcen zugreifen.
- Dienste werden unter Konten mit weniger Rechten ausgeführt (zum Beispiel LocalService oder NetworkService).
- Nicht benötigte Windows-Berechtigungen werden für jeden Dienst einzeln beseitigt (zum Beispiel das Debugging-Recht).
- Es wird ein Token auf den Dienst-Prozess angewandt, das keine Schreibberechtigung hat. Schreibversuche auf Ressourcen, die einer Dienst-SID nicht explizit genehmigen wurden, schlagen fehl.
- Diensten werden Netzwerk-Firewallrichtlinien zugewiesen. Diese verhindern einen Netzwerkzugriff außerhalb der normalen Grenzen des Dienstes. Die Firewallrichtlinie ist direkt mit der SID verknüpft.

Vorteile

Die Absicherung der Dienste stellt eine zusätzliche Schutzzebene für Dienste zur Verfügung. Sie kann einen gefährdeten Dienst nicht davor schützen, kompromittiert zu werden - hierfür sind andere Windows Vista-Komponenten und -Strategien wie die Windows-Firewall und ein vernünftiger Prozess zur Patchverwaltung zuständig. Die Absicherung der Dienste kann jedoch beeinflussen, wie viel Schaden ein Angreifer anrichten kann. Die Absicherung steht auch Drittanbietern zur Verfügung, so dass auch diese von ihr profitieren

können.

Auswirkungen

Die Kosten bezüglich einer Sicherheitskompromittierung können sehr hoch sein. Vertrauliche Daten könnten kompromittiert sein, Benutzer könnten Daten verlieren, und die Produktivität kann beeinträchtigt werden. Es kann sein, dass eine IT-Abteilung mehrere Wochen damit verbringt, den Schaden durch eine schwerwiegende Kompromittierung zu beseitigen. Die Absicherung der Dienste kann diesen Schaden stark reduzieren.

[↑ Zum Seitenanfang](#)

Internet Explorer-Erweiterungen

Beschreibung des Features

Mit dem Benutzerkontenschutz wird der Internet Explorer auf gerade so viele Berechtigungen eingeschränkt, wie er zum Browsen im Web benötigt. Er ist nicht in der Lage, Dateien des Benutzers oder Einstellungen zu verändern. Dieses Feature nennt sich geschützter Modus und wird mit Beta 2 zur Verfügung stehen. Es führt dazu, dass auch im Fall eines Angriffes durch eine schädliche Website keine ausreichenden Rechte bestehen Software zu installieren, Dateien in den Autostart-Ordner zu kopieren oder die Startseiten- oder Suchanbieter-Einstellungen zu verändern.

Der Internet Explorer geht folgendermaßen vor:

- Er markiert die neue Sicherheits-Statusleiste, wenn eine Site besucht wird, die mit SSL (Secure Sockets Layer) geschützt ist. Der Benutzer kann über die Statusleiste sehr einfach die Gültigkeit des Zertifikats der Site prüfen.
- Er verwendet einen Phishing-Filter, der das Browsen des Benutzers sicherer macht. Er informiert den Benutzer, wenn eine Website versucht, vertrauliche Informationen zu stehlen. Um dies zu erreichen, analysiert der Filter die Inhalte der Site und sucht nach charakteristischen Merkmalen für Phishing-Techniken. Zusätzlich nimmt er ein globales Netzwerk in Anspruch, über das er feststellen kann, ob eine Website vertrauenswürdig ist. Der Filter wird mehrmals pro Stunde aktualisiert, was bei der Geschwindigkeit mit der neue Phishing-Sites auftauchen, sehr wichtig ist.
- Er löscht alle zwischengespeicherten Daten mit einem Mausklick.

Vorteil

Die neuen Features des Internet Explorer unterstützen den Zugriff des Benutzers auf Internetressourcen und minimieren gleichzeitig die Sicherheitsbedrohungen. Somit werden auch die potenziellen Kosten bezüglich der Sicherheit reduziert.

Auswirkungen

Schädliche Websites können den Computer des Benutzers kompromittieren - sogar dann, wenn dieser nur offensichtlich harmlose Sites besucht. Die Verbesserungen des Internet Explorer reduzieren das Risiko einer Kompromittierung erheblich. Mit der Kombination von Benutzerkontenschutz und dem neuen geschützten Modus kommt es zu weniger Supportfällen.

[↑ Zum Seitenanfang](#)

Datenschutz

Beschreibung des Features

Der Verlust oder Diebstahl des intellektuellen Eigentums eines Unternehmens ist eine immer stärkere Bedrohung. Mit Windows Vista sind Daten auf Dokument-, Verzeichnis- und Computerebene besser geschützt. Der integrierte Rights Management-Client ermöglicht es Organisationen, Richtlinien bezüglich der Nutzung von Dokumenten durchzusetzen. Das verschlüsselnde Dateisystem bietet eine bessere Verschlüsselung und wurde so erweitert, dass Verschlüsselungsschlüssel nun auf Smart Cards gespeichert werden können. Einen zusätzlichen Schutz bietet der gesicherte Systemstart. Auf einem Computer mit entsprechender Hardware ist der gesamte Festplatteninhalt verschlüsselt - inklusive der Windows-Systemdateien und der Datei für den Ruhezustand. Um eine einfach bereitzustellende und zu verwaltende Lösung zu ermöglichen, wird ein TPM 1.2-Chip (Trusted Platform Module) zur Speicherung der Schlüssel

verwendet. Damit das Feature möglichst einfach zu verwenden ist, sind ein TPM und eine entsprechende Infrastruktur notwendig.

Ein TPM-Chip ist eine Hardwarekomponente, die nur auf neueren Computern zur Verfügung steht.

Zusätzlich werden bestimmte Informationen über das Betriebssystem auf dem TPM-Chip gespeichert. Jedes Mal, wenn der Computer gestartet wird, überprüft Windows Vista, ob die Betriebssystemdateien bei einem Offline-Angriff verändert wurden. Ein Offline-Angriff ist ein Szenario, in dem ein Angreifer mit einem anderen Betriebssystem startet. Wenn die Dateien verändert wurden, dann benachrichtigt Windows Vista den Benutzer und gibt den Zugriff auf Windows nicht frei. Das System wechselt in einen Wiederherstellungsmodus und fordert den Benutzer zur Eingabe eines Wiederherstellungsschlüssels auf.

Auch wenn die Festplatte in ein anderes System verschoben wurde, wird der Wiederherstellungsmodus verwendet. Dies liegt daran, dass der Wiederherstellungsschlüssel immer nur für einen bestimmten Computer gültig ist.

Vorteile

Windows XP und seine Vorgänger waren für Offline-Angriffe verwundbar. Zu den häufigsten Arten von Offline-Angriffen gehören:

- Starten eines Computers mit einer Bootdiskette und Zurücksetzen des Administrator Kennwortes.
- Zugriff auf die Festplatte über ein anderes Betriebssystem und somit Umgehen der Dateisystemberechtigungen.

Der sichere Systemstart kann Sie vor beiden Angriffstypen schützen. Er ist besonders für mobile Computer von großem Nutzen, da diese leicht gestohlen werden können.

Auswirkungen

Verlorene oder gestohlene Computer enthalten oftmals vertrauliche Informationen. Die Kompromittierung dieser Daten kann zu großen Problemen führen.

Mit der vollständigen Volumenverschlüsselung von Windows Vista kann das Risiko einer Kompromittierung durch Offline-Angriffe drastisch verringert werden. Sie stellt sicher, dass der Angreifer auch bei verlorenen oder gestohlenen Computern nicht auf vertrauliche Dateien zugreifen kann.

Anmerkung: Die hier besprochenen Features können sich ändern. Einige Features können aufgrund von Marketinggründen, technischen Gründen oder anderen Ursachen möglicherweise nicht im fertigen Produkt enthalten sein.

[↑ Zum Seitenanfang](#)

[Verwalten Sie Ihr Profil](#)

©2005 Microsoft Corporation. Alle Rechte vorbehalten. [Nutzungsbedingungen](#) | [Markenzeichen](#) | [Informationen zur Datensicherheit](#) | [Impressum](#)

Microsoft