DuD
Datenschutz und Datensicherheit

Protokollierung im Windows Betriebssystem

Richard Marnau

Dieser Beitrag gibt einen knappen Einblick in die Protokollierungsmechanismen unter Windows-Systemen von Microsoft. Dabei zeigt sich, dass Protokolleinträge unter Windows leicht unterdrückbar, modifizierbar und löschbar sind. Um diese Mängel abzustellen bedarf es einer revisionssicheren Protokollierung.

Richard Marnau

Mitarbeiter beim Unabhängigen Landeszentrum für Datenschutz und zuständig für datenschutztechnische Einzelfragen

E-Mail: ld35@datenschutzzentrum.de

Einleitung

Mit der Protokollierung unter Windows 2000 oder 2003 ist es nicht möglich, die Tätigkeiten von Administratoren manipulationssicher zu überwachen oder revisionsfest zu protokollieren. Besonders problematisch wird dies, wenn mehrere Administratoren Zugriff auf kritische Systeme, Anwendungen und Daten haben.

Der Protokollierung wird meist wenig Beachtung geschenkt. Die IT-Abteilung wird als oberste Sicherheitsinstanz akzeptiert und ihr wird pauschal vertraut. Diese besondere Stellung wird durch entsprechende Dienstanweisungen untermauert, denn der Administrator ist Teil der Organisationsstruktur.

Auch im öffentlichen Bereich wird die IT immer weiter zentralisiert, indem bspw. alle Landesbehörden durch ein einzelnes Dienstleistungsunternehmen im Wege der Auftragsdatenverarbeitung administriert werden. So werden bspw. Daten aus den unterschiedlichsten Bereichen der Verwaltung auf Windows-Datei-Servern in einer großen Active Directory Domäne organisiert.

In solchen Strukturen spielt die Protokollierung eine entscheidende Rolle, denn der Domänenadministrator kann als oberste Instanz Rechte von Benutzerkonten und Dateien lesen, ändern, kopieren und löschen. Ob die Integrität und Vertraulichkeit der Daten gewährleistet ist und der Auftragnehmer seine Vertragspflichten eingehalten hat, kann nur durch Kontrollen und eine manipulationssichere Protokollierung festgestellt werden.

Im Folgenden werden die Möglichkeiten zur Protokollierung in der Microsoft Umgebungen analysiert und dargestellt.

1 Protokollierung unter Windows

Mit der Veröffentlichung von Windows 3.5 hat Microsoft begonnen, die Protokollierung durch den eventlog Dienst einzuführen und die Ereignisanzeige als zentrales Auswertungstool zu etablieren. Wie jeder andere Dienst auch läuft dieser im Hintergrund und lässt sich über gut dokumentierte API Schnittstellen[1] ansprechen. Viele Programme, die auf Microsoft Betriebsystemen laufen, schreiben ihre Protokolldaten über diese Schnittstellen unter „Anwendungen“ in die zentrale Protokollsammelstelle oder sie legen eine neue Protokolldatei an.

Microsoft teilt die Protokollierung standardmäßig in drei verschiedene Stufen und Dateien auf.[2]

- *Anwendungen* (AppEvent.Evt): In diesem Bereich legen Anwendungen ihre Protokolleinträge ab. Jedes Programm oder Tool kann hier Einträge generieren.
- *Sicherheit* (SecEvent.Evt): In diesem Bereich legen Microsoft-Betriebsysteme Protokolleinträge bezüglich Sicherheitsmeldungen ab. Dazu gehören Einträge wie „An/Abmeldung“ oder „Richtlinienänderung“. Nur das Betriebsystem kann in diese Protokolldatei schreiben.
- *System* (SysEvent.Evt): Zu den Systemereignissen gehören hauptsächlich Fehler oder Meldungen von Diensten, Programmen oder vom Betriebsystem selber. Hier werden Logeinträge geschrieben, sollte bspw. ein Dienst nicht gestartet werden können.

Auf einem Domaincontroller kommen zusätzlich folgende Logs hinzu:

[1] http://msdn.microsoft.com/library/en-us/eventlog/base/event_logging.asp

[2] http://www.microsoft.com/technet/prodtechnol/windows2000serv/maintain/monitor/03w2kadb.mspx

- *Verzeichnisdienst*: Active Directory und die dazugehörigen Dienste sammeln hier ihre Informationen
- *DNS-Server*: Wenn der DNS Server installiert ist, werden hier relevante Protokollinformationen abgelegt
- *Dateireplikationsdienst*: Dieser Eintrag sammelt Fehler und Informationen rund um die Replikationen

Gespeichert werden die Dateien unter C:\windows\system32\config mit der Endung .Evt.

Für das wichtige Protokoll „Sicherheit“ gilt: Der Umfang der Protokollierung wird in den Richtlinien oder Attribute festgelegt. Die Einstellungen und der Grad der Protokollierung und Überwachung können auf Objekten mit Security Access Controll List (SACL) definiert werden. Hierzu zählt typischerweise das Dateisystem NTFS mit Ordnern und Dateien. Weithin unbekannt ist, dass selbst die Registry eine solche SCAL hat. Über Richtlinien wird festgelegt, ob und wie die Protokollierung aktiviert werden soll. Es lassen sich hier erfolgreiche oder fehlgeschlagene Ereignisse einstellen. Dies gilt sowohl für Clients als auch Server.

1.1 Zentrale Dateiablagen

Die zentrale Organisation von Dateien ist heutzutage Standard in jeder größeren Organisation, um eine bessere Verfügbarkeit und Sicherung der Daten zu gewährleisten. Mit verschiedenen Berechtigungen wird verhindert, dass jeder Benutzer im Netzwerk auf jeden Ordner Zugriff hat. Administratoren können diese Berechtigungen ständig verändern, ohne dass diese Veränderung Protokolleinträge generiert.

Zwar lassen sich in den Sicherheitseinstellungen von Ordnern beliebige Überwachungen definieren, etwa wer wann die Datei aufgerufen oder verändert hat.[3] Diese Einstellungen können jedoch nach Belieben von den Administratoren verändert werden, denn das Verändern der Einstellungen wird nicht hinreichend lesbar protokolliert. Zwar wird ein Eintrag erzeugt, dieser ist aber mangels eines spezifischen Informationsgehalts nicht auswertbar.

Damit die Überwachung von Objekten überhaupt aktiv wird, muss die „Objektüberwachungsrichtlinie“ eingeschaltet werden. Für die Protokollierung der Benutzerkonten gilt ähnliches. Das Anlegen und

```
Ereignistyp:                Erfolgsüberw.
Ereignisquelle:             Security
Ereigniskategorie:          Verzeichnisdienstzugriff
Ereigniskennung:            566
Datum:                      07.03.2006
Zeit:                       13:34:00
Benutzer:                   KIEL\Administrator
Computer:                   VM-WIN2003
Beschreibung:
Objektvorgang:
Objektserver:               DS
Vorgangstyp                 Object Access
Objekttyp:                  groupPolicyContainer
Objektname:                 CN={6AC1786C-016F-11D2-945F-
                            00C04fB984F9},CN=Policies,
                            CN=System,DC=kiel,DC=de
Handlekennung:              -
Primärer Benutzername:      VM-WIN2003$
Primäre Domäne:             KIEL
Primäre Anmeldekennung:     (0x0,0x3E7)
Clientbenutzername:         Administrator
Clientdomäne:               KIEL
Clientanmeldekennung:       (0x0,0x1E6ED)
Zugriffe                    Eigenschaft schreiben

Eigenschaften:
Eigenschaft schreiben
Default property set
versionNumber
groupPolicyContainer

Weitere Info:
Weitere Info2:
Zugriffsmaske:              0x20
```

Abbildung 1

Verändern von Benutzerkonten wird nur dann protokolliert, wenn die „Benutzerkontenrichtlinie“ eingeschaltet ist. Ein Klick in diesen Richtlinien entscheidet darüber, ob die komplette Protokollierung ein- oder ausgeschaltet ist.

Um den Status der Protokollrichtlinien zu überwachen muss die so genannte „Änderungsrichtlinie“ aktiv sein.[4] Wird diese Richtlinie deaktiviert, hinterlässt sie einen letzten Eintrag. So wird verhindert, dass die wenigen Protokollrichtlinien unbemerkt verändert werden. Diese Abhängigkeit und Verschachtelung schon innerhalb der Richtlinien lässt erahnen wie komplex die Protokollierung ist. Der Ansatz, den Status der Richtlinien zu protokollieren, ist gut, jedoch fehlt jegliche Revisionsmöglichkeit.

1.2 Active Directory

In Microsoft Active Directory bieten „Gruppenrichtlinien“ eine Möglichkeit, um zentral Einstellungen und Richtlinien für Computer und Benutzer zu verteilen. Es gibt zahlreiche Gruppenrichtlinien für verschiedene Zwecke, insgesamt über 1.100 bei Windows 2003 mit Service Pack 1. Über diese Richtlinien wird auch die Protokollierung auf allen Clients und allen Servern geregelt.

Mit der „Default Domänencontroller Baseline Policy“ besteht eine Richtlinie, um die Protokollrichtlinien und diverse weitere Einstellungen auf dem Domaincontroller zu definieren.[5] Da auf dem Domaincontroller die Benutzer verwaltet werden, muss dieser Gruppenrichtlinie aus Gründen der Datensicherheit besondere Beachtung geschenkt werden. Jede Organisationseinheit und jede Gruppenrichtlinie hat eine eigene Security Controll Access List, womit Berechtigungen und Überwachung eingestellt werden können. Doch aus den generierten Protokolleinträgen lässt sich nicht nachvollziehen, welche Veränderungen vorgenommen wurden.

[3] http://www.microsoft.com/technet/prodtechnol/windowsserver2003/de/library/ServerHelp/ecf63dcf-17e7-4279-91ff-beb11bd0d688.mspx

[4] Unabhängiges Landeszentrum für Datenschutz (ULD), Windows2000 BackUP Magazin Nr. 5, Seite 226.

[5] http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/s3sgch05.mspx

Ein Beispielprotokolleintrag nach Veränderungen von Einstellungen innerhalb einer Gruppenrichtlinie befindet sich in Abbildung 1. Zwar lässt sich in diesem Protokolleintrag vom Objektnamen auf die Richtlinie schließen und auch der Benutzer und das Datum sind vermerkt. Doch lässt sich nicht erkennen, welche Werte verändert wurden. Das gleiche tritt bei Veränderungen von Rechten bei Ordnern und Dateien auf. Ändert ein Administrator dort die Rechte, so wird bei entsprechender Objektüberwachung zwar ein Eintrag generiert, dieser enthält jedoch nur die Nachricht, dass etwas verändert wurde. Welche Änderungen konkret vorgenommen wurden, lässt sich nicht feststellen.

2 Aufbau des Logfiles

Oftmals werden Logfiles in verschiedenen Formaten mit einem eindeutigen Textfeld (bspw. „Herr Mustermann hat auf Server ABC um 13.30 die Datei fasel.doc gelöscht“) gespeichert. Microsoft selbst verfolgt mit dem Eventdienst einen anderen Ansatz. Statt des Klartextes werden Variabeln und Fehlernummern in die Eventlogdatei geschrieben. Die Vorteile dieser Methode ist der geringe Platzverbrauch pro Logeintrag und die Übersetzungsmöglichkeit in andere Sprachen, denn um die Variablen und Fehlernummern aufzulösen, sind Meldungsschablonen in Form von Programmbibliotheken (DLL-Dateien) nötig.

Die Ereignisanzeige von Microsoft Windows findet diese Meldungsschablonen über die Windows Registry, um die Werte und Beschreibung aufzulösen. Hier liegen allerdings auch die Nachteile eines solchen Protokollierungsdesigns, denn die Schablonen können ausgetauscht, geändert oder gelöscht werden. Die Ereignisse werden dann ohne Warnung so angezeigt, wie es die Schablone vorgibt. So kann eine kritische Meldung schnell zu einer vermeintlich harmlosen umformuliert werden.

Das Arbeiten mit Schablonen für die Auflösung des Logfiles hat noch weitere Tücken. So ist nicht gewährleistet, dass Logfiles von Windows 2003 auf einem anderen Windows-Betriebsystem mit dem gleichen Inhalt angezeigt werden. Es besteht außerdem das Risiko, dass unterschiedliche Patchstände und Versionsnummern zu unterschiedlichen Log-Darstellungen führen.

2.1 Manipulierbarkeit

Wenn Protokolleinträge erzeugt werden, sollte natürlich nicht die Möglichkeit bestehen, diese ohne Spuren zu hinterlassen löschen zu können. Unter Windows 2000 und 2003 können nur ganze Spalten im Ereignisprotokoll, wie z.B. alles unter „System“, gelöscht werden. Wenn die Einträge unter „Sicherheit“ gelöscht werden, entsteht automatisch ein neuer Eintrag der anzeigt, welcher Benutzer um welche Uhrzeit das Protokoll gelöscht hat. Es ist also nicht möglich, mit Windows-Bordmitteln einen speziellen Eintrag zu löschen, ohne Spuren zu hinterlassen. Das ist sicher eine zu begrüßende Eigenschaft.

Im laufenden Betrieb sichert sich der „Ereignisprotokolldienst“ den exklusiven Zugriff auf die Eventlogdateien und lässt sich nicht ohne weiteres beenden. Da der Dienst nicht beendet werden kann, muss der Starttyp auf „manuell“ geändert und der Server neu gestartet werden, um ihn endgültig zu stoppen. Aus diesem Grund ist es auch nicht möglich, auf die Datei im laufenden Betrieb zuzugreifen. Keine Kunst ist es hingegen, die Dateien zu manipulieren, wenn das System bspw. mit einer Knoppix CD gestartet wird.

2.2 Manipulation des Eventlog Dienst

Arne Vidstorm hat ein Tool namens WinZapper[6] für Windows NT und Windows 2000 geschrieben. Dieses Programm macht es möglich, die Protokolldateien zu bearbeiten, obwohl der Dienst weiterhin scheinbar gestartet ist. Es lassen sich einzelne Einträge löschen, ohne Spuren zu hinterlassen, obwohl das Betriebsystem weiterhin in Betrieb ist.

Für einen effektiven Angriff ist WinZapper nur eingeschränkt geeignet. Denn es lassen sich ausschließlich die Sicherheitseinträge bearbeiten und der Computer muss neu gestartet werden, um die Veränderungen durchzuführen. Erschwerend kommt hinzu, dass Administratorrechte erforderlich sind, um dieses Tool auszuführen und es zur Beschädigung des Systemprotokolls kommen kann. Leider ist keine Dokumentation zu diesem Tool erhältlich, so kann man nur vermuten, dass der Dienst zum Absturz gebracht wird, wenn ein Angreifer an die Protokolldatei kommen will.

WinZapper ist ein „Proof of Concept“-Tool. Weiterentwickelte Programme und Scripte können unter Windows 2000 und NT im Ereignisprotokoll unter Umständen Einträge hinzufügen, verändern oder löschen. Unter Windows 2003 lässt sich Winzapper nicht starten.

2.3 Manipulation der Schablonendateien

Für die Auflösung der Variablen eines Logfiles ist unter Windows 2000 und Windows 2003 hauptsächlich die Datei „msaudite.dll“ zuständig. Zwar lassen sich mit einem Hexeditor die Dateien editieren und somit falsche Aussagen zu den Werten eingeben, jedoch bemerkt die Windows eigene Schutzfunktion SFP (System File Protection) WFP (Windows File Protection) innerhalb weniger Sekunden Veränderungen und stellt diese Datei wieder her.

Dieser vermeintliche Schutz lässt sich aber leicht umgehen. Löscht oder verändert man die Sicherheitskopie[7] der „msaudite.dll“, kann Windows die Datei nicht wiederherstellen und verlangt die Windows 2003 CD. Alternativ kann die veränderte Datei auch übernommen werden. Über diesen Weg konnte der Autor die Schablone so manipulieren, dass die Ereignisanzeige falsche Protokolleinträge darstellt.

2.4 Manipulation der Registry

Um die eigentliche Schablone in Form der DLL-Datei zu verändern, müssen die Windows-Schutzfunktionen umgangen werden. Es gibt aber noch einen einfacheren Weg, um gefälschte Aussagen im Ereignisprotokoll herzustellen. So sind in der Registry

```
\HKEY_LOCAL\MACHINE\System\
ControlSet001\Services\Eventlog\
Security\Security\
```

mit den Werten „EventMessageFile“, „Guid MessageFile“ und „ParameterMessageFile“ die Schablonendateien angegeben.

Die größten Auswirkungen im Sicherheitspotokoll hat der Eintrag EventMessageFile. Wenn dieser gelöscht wird, läßt sich keine Beschreibung eines Logeintrag auflösen. Angreifer können jetzt in diesen Registry-Einträgen beliebig andere Schablonen angeben, ohne dass Windows dadurch im Ablauf gestört wird. Die

[6] http://www.ntsecurity.nu/toolbox/winzapper/

[7] http://support.microsoft.com/kb/555486/en-us

Ereignisanzeige wird die Protokolldateien mit den manipulierten Schablonen anzeigen.

2.5 Übername von Verzeichnissen

Wenn ein Benutzer einen Ordner erstellt, gehört ihm dieser automatisch. Das heißt, er kann ihn löschen, umbenennen, die Sicherheitseinstellungen bearbeiten und den Administratoren die Rechte entziehen. Dies könnte jemand mit der Absicht tun, um Dateien auch vor Administratoren schützen. Da der Administrator aber dennoch Zugriff auf den Ordner benötigt, um bspw. einen Missbrauch nachzuweisen, kann er den Besitz von Ordnern übernehmen.

Der Besitzer eines Ordners hat immer die Möglichkeit, die Zugriffsrechte zu verändern, auch wenn er selber vorher überhaupt keinen Zugriff hatte. Wenn der Administrator den Besitz eines Ordners übernimmt, kann er sich die Rechte selbst geben, um auf den Ordner zuzugreifen.

Unter Windows 2000 war dies scheinbar nachweisbar, da der Besitzer des Ordners nun der Administrator war, und nicht mehr der ehemalige Benutzer. Doch diese Nachweisbarkeit besteht nur deshalb scheinbar, weil Arne Vidstorm mit dem Tool „Setowner“ nachweist, dass es einem Administrator möglich ist, den Besitzer eines Ordners auf jeden beliebigen Benutzer zu ändern[8].

Wenn die Überwachung aktiviert war, wird ein Log erstellt. Dort ist vermerkt, dass der Administrator, der das Tool ausgeführt hat, den Besitzer verändert hat. Auf welchen Besitzer der Ordner übergegangen ist, lässt sich daraus jedoch nicht entnehmen.

Unter Windows 2003 wurde das Konzept überarbeitet. Der Administrator kann nun Verzeichnisse übernehmen und den neuen Besitzer frei wählen. Das heißt, er kann den Besitzer von „Max“ auf „Administrator“ ändern, um sich Zugriff zu verschaffen und den Besitzer danach wieder auf „Max“ zurücksetzen.

Dass der Administrator somit Zugang zu allen Verzeichnissen auf einem Windows 2003 Server hat, muss jedem klar sein, der dort seine Daten speichert. Dieses Problem läst sich nur durch eine Verschlüsselung umgehen. Diese muss jedoch so implementiert sein, dass der Administrator keinen Zugriff auf die Schlüssel hat. Die Administration und Konfiguration der Verschlüsselungssoftware sollte in diesem Fall nicht in den Händen der Administratoren liegen.

3 Was kann man tun?

Administratoren sollten immer über personalisierte Konten verfügen. So lassen sich die wenigen Informationen in den Protokolldateien auf eine reale Person beziehen und diese kann ihre Tätigkeiten verantworten.

Bei Analysen und Unstimmigkeiten im Logfile sollte nicht nur das Logfile selbst gesichert werden, sondern auch die dazugehörigen Schablonen und die Einstellungen der Registry. Dies gilt besonders für forensische Untersuchungen.[9] Es ist außerdem zu empfehlen, alle Protokolleinträge auf einem zentralen Protokollserver zu sammeln. Hierzu werden kostenlose Tools angeboten[10], um alle Ereignisprotokolle auf einen Syslog-Server umzuleiten.

Auf jeder Workstation und auf jedem Server in Netzwerken werden Protokolldateien erzeugt, die unter Umständen für die Administration wichtige Informationen enthalten können. Kaum ein Administrator schaut jedoch in den Ereignismanager, um die zum Teil unüberschaubare Anzahl der Einträge auszuwerten. Hier können gesonderte Tools Abhilfe schaffen, welche die Protokolldateien auslesen und alle Ereignisse an zentraler Stelle sammeln.

4 Fazit

Jeder Benutzer sollte sich dessen bewusst sein, dass Daten auf Windows Servern nicht vor der Administration geschützt sind. Während ein unbefugter Zugriff auf den Inhalt einer E-Mail noch bemerkt werden kann, weil bspw. eine neue E-Mail als gelesen markiert oder Empfangsbestätigungen versendet wurden, so ist es für den Nutzer weitaus schwieriger, einen Zugriff auf seine Verzeichnisse und Dateien festzustellen und seine Berechtigung zu prüfen.

Die unzureichende und leicht manipulierbare Protokollierung wird gerade bei der Administration größerer Netzwerke zu einem gravierenden Problem. Es ist angekündigt, dass sich mit Microsoft Vista bei der Protokollfunktion einiges ändern soll. Zu hoffen bleibt außerdem, dass das Konzept so überarbeitet wird, dass Schablonen nicht zu manipulieren werden können.

[8] http://www.ntsecurity.nu/toolbox/setowner/

[9] Schuster, A. (2005). Windows Eventlogs in der forensischen Analyse. In: M. Thorbrügge (Hrsg.), Tagungsband des 12. DFN-CERT Workshops Sicherheit in vernetzten Systemen, Hamburg, März 2005, S. D1-D16; Fox/Kelm, DuD 2004, 491.

[10] http://www.loganalysis.org/sections/syslog/windows-to-syslog/