Gerd Schmidt

Automatisierte Auswertung von Protokolldateien (I)

Eine Strategie zur Verminderung von Sicherheits- und Haftungsrisiken?

Auf jedem IT-System fallen pro Tag eine Vielzahl von Protokollinformationen an – eine unüberschaubare Anzahl mit entsprechend unvorhersehbarem Analysepotenzial. Anhand der nachfolgenden Erläuterungen und Beispiele wird aufgezeigt, dass von einer Auswertung dieser Protokolldaten auch das Management profitieren kann.

Die Wahrung der IT-Sicherheit ist inzwischen nicht mehr alleinige Sache des IT-Verantwortlichen. Da wesentliche Prozesse in Unternehmen heute nur noch mit Hilfe der IT funktionieren, ist IT-Sicherheit zu einem wichtigen Risikofaktor geworden. Mit der zunehmenden Computerisierung und der firmeninternen und -übergreifenden Vernetzung von Informationsystemen steigt die Anzahl potenzieller Schwachstellen. Versäumnisse bei der Absicherung der IT-gestützten Geschäftsprozesse eines Unternehmens können auch für Vorstände oder Geschäftsführer haftungsrechtliche und finanzielle Folgen haben. Darüber hinaus kann der Ausfall von IT-Ressourcen dem Unternehmensimage schaden. Das Handelsblatt hat dazu in seiner Ausgabe Nr. 224 vom 18. November 2005 auf Seite 6 unter der Überschrift „Wo Vorstand draufsteht, ist Haftung drin“ eine übersichtliche Checkliste zum Thema IT-Sicherheit im Unternehmen für die Zielgruppe Vorstände und Geschäftsführer veröffentlicht. Grundlage hierfür sind gesetzliche Auflagen, wie die EU-Richtlinie zum Datenschutz oder der Sarbanes Oxley Act (SOX). Darüber hinaus bestehen nationale Gesetze, wie das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), Aktiengesetz (AktG), Handelsgesetzbuch (HGB), Strafgesetzbuch (StGB) oder das Bundesdatenschutzgesetz (BDSG). Die daraus erforderlichen Maßnahmen zur Risikobeherrschung werden mittlerweile auch bei der Bestimmung der Kreditwürdigkeit nach Basel II/ Solvency II berücksichtigt. IT-Sicherheit wird nach neuesten Pressehinweisen nun endlich Chefsache!

Die Maßnahmen, um IT-Risiken zu minimieren, reichen von der Erstellung eines IT-Sicherheitskonzeptes über regelmäßige IT-Audits bis hin zu regelmäßigen Awarenessprogrammen für Mitarbeiter, insbesondere für IT-Administratoren mit Feedbackmechanismen und effizienten Disziplinarmaßnahmen bei mangelnder Verpflichtung. Konkrete Beispiele für Maßnahmen können aus dem internationalen IT-Standard ISO17799 (neu überarbeitet in 2006: ISO27002) entnommen werden, wobei sich teilweise eine Reflexion zum BDSG, insbesondere § 9 Anlagen zeigt. Beispielsweise dient die Identifikation und Authentifikation der Zugangskontrolle (§ 9 Anlage Nr. 2 BDSG), die Rechteprüfung und -verwaltung der Zugriffskontrolle (§ 9 Anlage Nr. 3 BDSG) und die Beweissicherung und Protokollauswertung der Eingabekontrolle (§ 9 Anlage Nr. 5 BDSG).

Sowohl versehentliche als auch absichtliche IT-Sicherheitsvorfälle durch eigene Mitarbeiter werden immer noch unterschätzt. Für manche Bereiche sind rein präventive Maßnahmen, z. B. eingeschränkte Berechtigungen oder eine entsprechend „sichere“ Konfiguration, zielführend und ausreichend. An anderer Stelle hilft dagegen nur eine entsprechende Nachweisführung, um Angriffe oder Verstöße zumindest im Nachhinein nachvollziehen und damit evtl. ahnden zu können. Eine manuelle IT-Auditierung z. B. von Änderungs- und Zugriffsprotokollen allein genügt jedoch nicht und ist in der Regel in der Praxis mangels Personalressourcen nicht durchführbar. Nur wenn eine regelmäßige, möglichst automatisierte Auswertung der Protokolle stattfindet, wird einer missbräuchlichen Verwendung tatsächlich vorgebeugt, weil keiner darauf vertrauen kann, dass Verstöße unentdeckt bleiben. Da Protokolle häufig personenbezogen sind, ist bei einem derartigen Vorgehen immer der Betriebsrat/Personalrat und der Datenschutzbeauftragte zu beteiligen. Der Betriebsrat hat gemäß § 87 Abs.1 Betriebsverfassungsgesetz ein Mitbestimmungsrecht bei Maßnahmen zur Leistungs- und Verhaltenskontrolle. Der Datenschutzbeauftragte prüft die Einhaltung des BDSG z. B. hinsichtlich der Zugriffsberechtigungen (§ 9 Anlage Nr.3 BDSG) auf die Protokolldaten, der besonderen Zweckbindung der Protokollierung (§31 BDSG) und darauf, ob nicht mehr Daten als unbedingt notwendig genutzt werden (§ 3a BDSG). Eine Auswertung von Protokolldaten z. B. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen ist datenschutzrechtlich grundsätzlich zulässig. Sie sollte aber konkret sein und in jeder Hinsicht in einer Betriebsvereinbarung festgeschrieben werden.

Weitere Informationen zur IT-Sicherheit und speziell zur Protokollierung und Protokollauswertung finden Sie beispielsweise beim BSI (Bundesamt für Sicherheit in der Informationstechnik) unter anderem im IT-Grundschutzhand-

buch (http://www.bsi.de/gshb/deutsch/index.htm), z. B. in den Maßnahmen M 2.64 (Kontrolle der Protokolldateien), M 2.110 (Datenschutzaspekte bei der Protokollierung) oder M 5.9 (Protokollierung am Server), oder in der „Orientierungshilfe und Checkliste zur Protokollierung“ vom 18.08.2000 des Landesbeauftragten für den Datenschutz Niedersachsen (http://www.lfd.niedersachsen.de -> Service-Angebote -> Checklisten -> Protokollierung).

Viele Unternehmen haben eine sehr heterogene IT-Landschaft mit einer Vielzahl von sicherheitsrelevanten Informationen, die sowohl die Konfiguration des IT-Systems (z.B. Paßwortrichtlinien) als auch das Benutzerverhalten (z.B. Zugriffsversuche auf sensible Daten) betreffen können. Diese sicherheitsrelevanten Informationen erhalten Sie aus den verschiedensten Quellen. Bei Windows stehen z. B. sehr viele Informationen in 3 unterschiedlichen Protokolldateien, Hier wird nach System-, Sicherheits- und Anwendungsprotokoll unterschieden. Bei SAP R/3 sind z. B. Syslog, AuditLog oder auch einzelne Tabellen zu nennen. Bei z/OS sind insbesondere die SMF-Sätze und die RACF-Datenbank interessant. Diese Protokolldaten liegen in den unterschiedlichsten Formaten vor. Es kann sich z. B. um einfache ASCII-Textdateien handeln, um Drucklisten, Tabellen oder bei IBM-Großrechnern der zSeries mit z/OS um Daten im EBCDIC- oder binären Format, die noch dazu mehrzeilig sind.

Ein Lösungsansatz für diese komplexe Problemstellung dieser vielzähligen sicherheitsrelevanten Informationen auf den unterschiedlichen IT-Systemen in den Unternehmen ist die automatisierte Auswertung von relevanten Protokolldaten. Sie spart vor allem Kosten und Zeit! Nach der einmaligen, etwas aufwändigeren Erstellung der Auswertungsroutinen kann anschließend zeitnah und effizient quasi auf „Knopfdruck“ eine Aussage über eventuelle Sicherheitsvorfälle getroffen werden. Bei gleichzeitig erhöhter Sicherheit kann dann möglicherweise auf eine mit geschätzten 50.000 € pro IT-System kostenintensive Ausbildung z. B. von IT-Revisoren verzichtet werden, oder zumindest zusätzlicher Personalbedarf in diesem Bereich vermieden werden. Nachfolgend dazu 3 Beispiele aus der Praxis.

Protokollauswertung: „Zugriff auf sensible Daten unter Windows“

Elektronische Informationen von z. B. Vorständen oder Geschäftsführern enthalten oft sensible Informationen und Geschäftsgeheimnisse. Gelangen diese Daten z. B. in die Hände von Konkurrenten oder auch der Medien, kann beträchtlicher Schaden entstehen. Eine Einschränkung von Zugriffsberechtigungen ist deshalb oft eine notwendige Voraussetzung für die Vertraulichkeit der Daten. Jedoch kann ein Zugriff für manche Personengruppen, z. B. Windows-Administratoren, technisch nicht ausgeschlossen werden. Um unberechtigte Zugriffsversuche zu erkennen oder ggf. erfolgte Zugriffe nachvollziehen zu können, kann es sinnvoll sein, die betroffenen Informationen/Daten zu überwachen. Dies erfolgt unter Windows durch Aktivierung der Datei- und Objektüberwachung in den Überwachungsrichtlinien des jeweiligen File-Servers. Hier können sowohl erfolgreiche als auch abgewiesene Zugriffe interessant sein.

Zusätzlich muss für die zu überwachenden Objekte (z.B. Verzeichnisse oder Dateien) das Protokollieren der Zugriffe aktiviert werden. Dies erfolgt im Windows-Umfeld unter den Sicherheitseinstellungen des jeweiligen Objektes über die Option „Erweitert“ auf der Registerkarte Überwachung. Da erfahrungsgemäß sehr viele Protokolleinträge bei Datei- und Objektzugriffen erzeugt werden, ist selektiv zu entscheiden, für welche Verzeichnisse eine Überwachung tatsächlich erforderlich ist. Dabei kann auch eine Einschränkung auf einzelne Zugriffsarten und Benutzer oder Gruppen erfolgen.

Die Protokolldaten z. B. von erfolgreichen und abgewiesenen Zugriffen werden im Sicherheitsprotokoll Security-Log) unter den Event-IDs 560-565 abgebildet (Abb.1). Auch die Zugriffsart wird mitprotokolliert. Beispielsweise bedeutet der Eintrag „%%4417“ den Zugriff „Daten schreiben oder Datei hinzufügen“. Eine Extraktion des Security-Logs nach dieser Event-ID ist beispielsweise mit dem Windows-Tool „dumpel“ aus dem Windows Ressource Kit möglich.

In der Abbildung 1, könnten z. B. die Zugriffe des Benutzers XXXXXX2 am späten Abend eventuell ein Hinweis auf unzulässige Benutzeraktivitäten sein.

```
12/29/2005 14:34:51 8 3 560 Security  Domäne\XXXXXX1 Server  Security File E:\Vorstand\Planung 2006\Strategie\Gesch ...
12/29/2005 14:37:45 8 3 560 Security  Domäne\XXXXXX1 Server  Security File E:\Vorstand\Planung 2006\Personal 5752 0...
12/29/2005 14:45:55 8 3 560 Security  Domäne\XXXXXX1 Server  Security File E:\Vorstand\Planung 2006\Personal\Neuein ...
12/29/2005 21:59:59 8 3 560 Security  Domäne\XXXXXX2 Server  Security File E:\Vorstand\Planung 2006\ 1684 0 4999757 ...
12/29/2005 21:59:59 8 3 560 Security  Domäne\XXXXXX2 Server  Security File E:\Vorstand\Planung 2006\Strategie 1708 ...
12/29/2005 22:00:00 8 3 560 Security  Domäne\XXXXXX2 Server  Security File E:\Vorstand\Planung 2006\Strategie\Gesch ...
12/29/2005 22:00:08 8 3 560 Security  Domäne\XXXXXX2 Server  Security File E:\Vorstand\Planung 2006\Strategie\Market...
12/29/2005 22:00:10 8 3 560 Security  Domäne\XXXXXX2 Server  Security File E:\Vorstand\Planung 2006\Strategie\Konkur...
12/29/2005 22:00:15 8 3 560 Security  Domäne\XXXXXX2 Server  Security File E:\Vorstand\Planung 2006\Strategie\Finan ...
```

Abbildung 1: Das Windows-Security-Log binhaltet eine Vielzahl von Ereignissen.

Weitere Praxisbeispiele für übergreifende Auswertung von Protokolldateien unterschiedlicher IT-Systeme folgen in Teil II in der nächsten Ausgabe der AWV-Informationen.

Gerd Schmidt, ab 1991 Datenschutzbeauftragter Konzern und 15 Jahre Leiter der IT-Revision, NÜRNBERGER Versicherungsgruppe. G.Schmidt ist interner Unternehmensberater (GDV), Autor, Referent und Mitglied in diversen Arbeitskreisen in den Bereichen IT-Revision und Datenschutz. Er gründete 1997 den GDD-Erfakreis „Datenschutz und Informationssicherung“ bei der IHK Nürnberg. E-Mail: gerd.schmidt@nuernberger.de