Gerd Schmidt

Automatisierte Auswertung von Protokolldateien (II)

Eine Strategie zur Verminderung von Sicherheits- und Haftungsrisiken?

Übergreifende Auswertung von Protokolldateien unterschiedlicher IT-Systeme: „Verdacht auf Passwortweitergabe“?

Mit dem Passwort authentifiziert sich ein Benutzer als der rechtmäßige Nutzer von Daten und Anwendungen. Dennoch kommt es immer wieder vor, dass Benutzer ihr Passwort an Kollegen weitergeben. Ursache sind häufig unzureichende Berechtigungen von Stellvertretern, die bei Abwesenheit des Benutzers deren Arbeiten mit erledigen sollen. Die Nachvollziehbarkeit ist jedoch bei der Weitergabe des Passworts nicht mehr gegeben und kann vor allem für den Benutzer im Einzelfall erhebliche Nachteile mit sich bringen. Aus diesen Gründen wird in vielen Unternehmen in einer Benutzerrichtlinie explizit darauf hingewiesen, dass das Passwort geheimzuhalten ist.

Eine effiziente Sensibilisierungsmaßnahme z. B. durch den Betriebsrat ist es daher, bei Verdacht auf Passwortweitergabe mit dem jeweiligen Benutzer Kontakt aufzunehmen. Ein Verdacht auf Passwortweitergabe besteht immer dann, wenn der Benutzer nicht im Unternehmen anwesend war, aber dennoch ein Login mit seiner Benutzerkennung stattgefunden hat.

Die Überprüfung, ob ein Benutzer anwesend war, ist hierbei nicht immer einfach. Ein Indiz für die quasi physische Anwesenheit von Benutzern kann der Vergleich mit den Protokolldaten aus einem elektronischen Zutrittskontrollsystem oder der Abgleich mit Urlaubslisten mit den Logins in den IT-Systemen sein. Es kann jedoch beispielsweise vorkommen, dass ein Benutzer seine Zutrittskarte vergessen und mit einer Ersatzkarte das Unternehmen betreten hat. In diesem Fall entstehen z. B. keine Zutritts-Protokolleinträge, obwohl der Benutzer anwesend war. Ferner sind bei der derartigen Prüfungen auch z. B. Telearbeiter zu beachten, die über einen Remote-Zugriff auf das Unternehmensnetz zugreifen. Die aufgezeigten und erforderlichen Ausnahmeregelungen sollten zusammen mit der Personalabteilung erarbeitet und bei den übergreifenden Auswertungen berücksichtigt werden.

Die Zutrittsprotokolldaten können dabei nicht nur mit etwaigen Windows-Anmeldungen (Logins) abgeglichen werden, sondern auch mit Anmeldungen an anderen Systemen. Auffallend kann beispielsweise auch eine Anmeldung an einem SAP R/3-System ohne ein entsprechendes Windows-Login sein.

Die Logins von Benutzern werden vom jeweiligen IT-System protokolliert. Bei den nachfolgend genannten Systemen Windows, z/OS und SAP R/3 sind die relevanten Protokolldaten wie folgt zu finden:

- Unter Windows werden erfolgreiche Netzwerk-Anmeldungen im Sicherheitsprotokoll unter der Event-ID 540 protokolliert (Abb. 2). Der Logeintrag fällt an demjenigen Domain Controller an, über den sich der Benutzer anmeldet.

- Unter z/OS in den SMF-Sätzen Record Type 80, Event Code JOBINIT (Abb. 3).

- Im SAP R/3 erkennt man im Auditlog an den Logeinträgen mit der Meldungsnummer AU1, welche Benutzer sich angemeldet haben (Abb. 4). Das Auditlog wird im SAP R/3-System mit der Transaktion SM20 aufgerufen und kann z. B. auch als Liste im Textformat gesichert werden.

Die Praxiserfahrung zeigt, dass bei einem Vorfall mit Verdacht auf Passwortweitergabe durch z. B. die unmittelbare Nachfrage des Betriebsrats beim betroffenen Benutzer mittelfristig quasi alle Benutzer im Unternehmen erheblich sensibilisiert werden. Darüber hinaus werden derartige Stichproben von den meisten Benutzern sehr positiv gesehen, da sie davon ausgehen können, dass während ihrer Abwesenheit ihr Benutzeraccount automatisiert geschützt und geprüft wird.

Protokollauswertung: Berechtigung Debuggen im Änderungsmodus im SAP-Umfeld

Gemäß § 239 Abs. 3 HGB darf in Handelsbüchern „Eine Eintragung oder eine Aufzeichnung […] nicht in einer Weise verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. Auch solche Veränderungen dürfen nicht vorgenommen werden, deren Beschaffenheit es ungewiss lässt, ob sie ursprünglich oder erst später gemacht worden sind.“

Daher ist in einem Buchhaltungssystem zu verhindern, dass nicht nachvollziehbare Änderungen am Buchungsstoff vorgenommen werden („Radieren“). In einem SAP R/3-System können ABAP-Programme zur Fehlersuche debuggt werden. Beim Debuggen ist es bei entsprechender Berechtigung

```
12/29/2005   08:58:07   8 4 576   Security   XXXXXX1   SERVERNAME   Besondere Rechte bei neuer Anmeldung:    Benutzername:   XXXXXX1
12/29/2005   08:58:07   8 2 540   Security   XXXXXX1   SERVERNAME   Erfolgreiche Netzwerkanmeldung:    Benutzername:     XXXXXX1
12/29/2005   09:03:07   8 4 576   Security   XXXXXX2   SERVERNAME   Besondere Rechte bei neuer Anmeldung:    Benutzername:   XXXXXX2
12/29/2005   09:03:07   8 2 540   Security   XXXXXX2   SERVERNAME   Erfolgreiche Netzwerkanmeldung:    Benutzername:     XXXXXX2
12/29/2005   09:04:04   8 2 538   Security   XXXXXX3   SERVERNAME   Benutzerabmeldung:     Benutzername:    XXXXXX3     Domäne:
12/29/2005   09:07:24   8 4 576   Security   XXXXXX4   SERVERNAME   Besondere Rechte bei neuer Anmeldung:    Benutzername:   XXXXXX4
12/29/2005   09:07:24   8 2 540   Security   XXXXXX4   SERVERNAME   Erfolgreiche Netzwerkanmeldung:    Benutzername:     XXXXXX4
12/29/2005   09:09:52   8 2 538   Security   XXXXXX1   SERVERNAME   Benutzerabmeldung:     Benutzername:    XXXXXX1     Domäne:
12/29/2005   09:10:17   8 4 576   Security   XXXXXX5   SERVERNAME   Besondere Rechte bei neuer Anmeldung:    Benutzername:   XXXXXX5
12/29/2005   09:10:17   8 2 540   Security   XXXXXX5   SERVERNAME   Erfolgreiche Netzwerkanmeldung:    Benutzername:     XXXXXX5
```

Abbildung 2: Auszug aus dem Security Log eines Windows-Servers. Die Event-ID 540 bedeutet eine erfolgreiche Netzwerk-Anmeldung eines Benutzers.

```
EVENT CODE                EVENT QUALIFIER      LOGIN DATUM          LOGIN ZEIT           SYSTEM               USER ID
   --------------------  -------------------- --------------------  --------------------  --------------------  --------------------
                                                                                                                -
             JOBINIT              RACINITI             2005-12-29           04:13:50             XXXX                 XXXXXX1
             JOBINIT              RACINITI             2005-12-29           06:43:40             XXXX                 XXXXXX2
             JOBINIT              RACINITI             2005-12-29           07:17:32             XXXX                 XXXXXX3
             JOBINIT              RACINITI             2005-12-29           07:23:22             XXXX                 XXXXXX4
             JOBINIT              RACINITI             2005-12-29           07:28:51             XXXX                 XXXXXX5
             JOBINIT              RACINITI             2005-12-29           07:45:18             XXXX                 XXXXXX6
             JOBINIT              RACINITI             2005-12-29           08:00:04             XXXX                 XXXXXX7
             JOBINIT              RACINITI             2005-12-29           08:03:14             XXXX                 XXXXXX8
             JOBINIT              RACINITI             2005-12-29           08:11:09             XXXX                 XXXXXX9
```

Abbildung 3: SMF-Sätze ausgewertet mit dem Standardwerkzeug ICETOOL unter z/OS. Anhand des Event Codes "JOBINIT" und des Event Qualifiers "RACINITI" , kann das Login eines Benutzers zu einem bestimmten Datum und einer bestimmter Uhrzeit nachgewiesen werden.

```
-------------------------------------------------------------------------------------------------------------------------------
|Zeit        |Instanz             |Typ|Nr|Man|Benutzer   |Transaktionscode    |Terminal|MNr|Text                        Datum: 29.12.05
-------------------------------------------------------------------------------------------------------------------------------
|09:02:24    |sap-instanzname1    |DIA| 0|100|XXXXXX1    |SESSION_MANAGER     |YYYYYYY1|AU1|Login erfolgreich (Typ=A)
|09:04:59    |sap-instanzname2    |DIA| 0|100|XXXXXX2    |SESSION_MANAGER     |YYYYYYY2|AU1|Login erfolgreich (Typ=A)
|09:06:29    |sap-instanzname1    |DIA| 0|100|XXXXXX3    |SESSION_MANAGER     |YYYYYYY3|AU1|Login erfolgreich (Typ=A)
|09:06:46    |sap-instanzname1    |DIA| 0|100|XXXXXX3    |                    |YYYYYYY3|AUC|Logoff Benutzer
|09:07:03    |sap-instanzname1    |DIA| 0|100|XXXXXX4    |SESSION_MANAGER     |YYYYYYY4|AU1|Login erfolgreich (Typ=A)
|09:07:30    |sap-instanzname1    |DIA| 0|100|XXXXXX5    |SESSION_MANAGER     |YYYYYYY5|AU1|Login erfolgreich (Typ=A)
|09:07:43    |sap-instanzname1    |DIA| 0|100|XXXXXX6    |                    |YYYYYYY8|AU1|Login erfolgreich (Typ=A)
|09:09:04    |sap-instanzname2    |DIA| 0|100|XXXXXX7    |SESSION_MANAGER     |YYYYYYY7|AU2|Login gescheitert (Grund=1, Typ=A)
|09:09:10    |sap-instanzname2    |DIA| 0|100|XXXXXX7    |SESSION_MANAGER     |YYYYYYY7|AU2|Login gescheitert (Grund=1, Typ=A)
|09:09:24    |sap-instanzname2    |DIA| 0|100|XXXXXX7    |SESSION_MANAGER     |YYYYYYY7|AU1|Login erfolgreich (Typ=A)
|09:10:10    |sap-instanzname2    |DIA| 1|100|XXXXXX2    |                    |YYYYYYY2|AUC|Logoff Benutzer
```

Abbildung 4: Das Auditlog unter SAP R/3. Anhand der Meldungsnummer (MNr) kann das jeweilige Ereignis zugeordnet werden. Die Meldungnummer AU1 bedeutet beispielsweise eine erfolgreiche Benutzeranmeldung.

auch möglich, Werte von Variablen zu verändern. Sofern diese Berechtigung in einem Produktivsystem bestehen, können also auf nicht nachvollziehbare Weise Buchungsdaten geändert werden. Abbildung 5 zeigt, wie in einem SAP R/3-System mit Hilfe des Reports RSUSR002 überprüft werden kann, wer über die Berechtigung verfügt, ABAP-Programme im Änderungsmodus zu debuggen.

Abbildung 5: Benötigte Berechtigung zum Debuggen im Änderungsmodus.

Das Berechtigungsobjekt S_DEVELOP wird für Berechtigungen für Objekte der ABAP/4 Development Workbench benötigt. Die Berechtigung erlaubt „Ändern“ (Aktivität 02) von „Programmen und dazugehörigen Objekten“ (Objekttyp PROG) und ist somit für die REPLACE-Funktion im Debugging erforderlich.

Diese Berechtigung sollte im Produktivsystem nur ein Notfallbenutzer bzw. nur ein nach dem Vier-Augen-Prinzip eingesetzter Benutzer besitzen.

Lösungsansatz in der Nürnberger Versicherungsgruppe mit CrossAudit

In der NÜRNBERGER Versicherungsgruppe wurde im Jahr 2001 entschieden, für die dynamische Prüfung der komplexen IT-Infrastruktur durch die IT-Revision eine plattformübergreifende, automatisierte IT-Prüfung einzuführen. Im Rahmen des Projekts „CrossAudit“ wurden bis Ende 2005 9 IT-Systeme, z. B. z/OS, SAP R/3 und die Oracle-Datenbanken, an ein plattformübergreifendes Informationssystem angebunden. Die Auswahl der IT-Systeme erfolgte in Absprache mit dem Vorstand im Hinblick auf die Kernprozesse und deren IT-Plattformen. Vor der Anbindung wurden die IT-Systeme mit Unterstützung von externen Sicherheitsberatern analysiert. Darauf aufbauend wurden in enger Zusammenarbeit mit den jeweiligen IT-Systemverantwortlichen und dem Betriebsrat relevante Policies (=Prüfungsrichtlinien) erarbeitet, die teilweise systemspezifisch (z. B. kritische SAP R/3-Berechtigungen), teilweise systemübergreifend (z. B. unternehmensweite Passwortrichtlinien) gelten.

Inzwischen werden täglich mehrere hundert Megabyte Protokoll-

daten mit ca. 100 Policies sowohl bezüglich Konfiguration der IT-Systeme (=ConfigAudit) als auch bezüglich des Benutzerverhaltens (=EventAudit) verarbeitet. Die automatisierte Auswertung erfolgt mit Hilfe des Revisionstools IDEA. Mittlerweile bietet der Markt für diese Aufgabenstellung leistungsfähige Alternativ-Softwareprodukte. Das Ergebnis wird auf einer zentralen Informationsplattform bereitgestellt und stichprobenartig geprüft (Abb. 6).

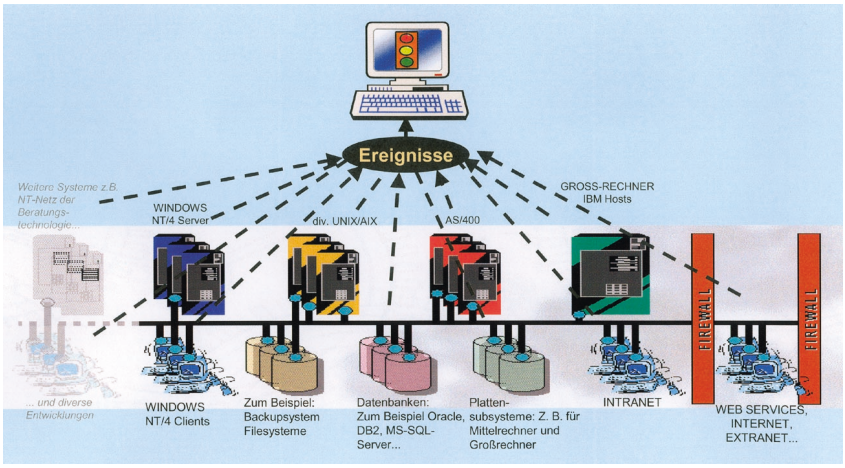

Abbildung 6: Schematische Darstellung von Cross Audit

Policies mit personenbezogenen Auswertungen (z. B. der oben dargestellte Verdacht auf Passwortweitergabe) erhält der Betriebsrat zur weiteren Bearbeitung. Auswertungen mit it-systembezogenen Policies (z. B. mögliche Sicherheitslücken in der Konfiguration) erhalten die jeweiligen IT-Systemverantwortlichen. Auf diese Weise wird die komplette Belegschaft wiederkehrend sensibilisiert. CrossAudit hat sich damit als fester Bestandteil der Unternehmenssicherheit und des Internen Kontrollsystems etabliert.

Fazit

Der mittlerweile vier-jährige Praxiseinsatz der automatisierten Auswertung von Protokolldateien zeigt, daß damit Sicherheits- und Haftungsrisiken präventiv verringert werden können. Mit der wirtschaftlichen und permanenten Analyse der in der Regel standardmäßig vorhandenen IT-Protokolldateien, werden frühzeitig Schwachstellen erkannt und Sicherheitslücken geschlossen. Darüber hinaus ist die automatisierte Auswertung unter Kosten-/Nutzenaspekten ein erfolgreiches und leistungsfähiges Awarenessprogramm für alle Mitarbeiter. Ein weiterer positiver Nebeneffekt ist, daß auf die bereits genannte kostenintensive Qualifizierung von IT-Revisoren verzichtet werden kann. Mit der Vorgehensweise entsteht ein Know-how-Speicher mit Wiederverwendbarkeit von Prüfungswissen. Der normalerweise zusätzlich erforderliche Bedarf an Personalkapaziäten für derartige IT-Prüfungsarbeiten kann entfallen.

Das Bewußtsein, dass IT-Sicherheit und Datenschutz wichtige Fundamente für die Erhaltung der Wettbewerbsfähigkeit darstellen, setzt sich dabei immer mehr durch.

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

Teil I dieses Artikels finden Sie in den AWV-Informationen 1/06.

VERWALTUNG & MANAGEMENT
Zeitschrift für allgemeine Verwaltung

Zahlungsmoral: Vorbild öffentliche Hand?

Seit Jahren signalisieren Umfragen zum Zahlungsverzug privater, gewerblicher oder öffentlicher Auftraggeber eine sinkende Bereitschaft bzw. Fähigkeit der Schuldner zur Begleichung ihrer Rechnungen. Das Thema Zahlungsmoral ist somit zum Dauerbrenner geworden und droht damit in der schnelllebigen Medienwelt das Interesse der Öffentlichkeit zu verlieren. Zwar hatten frühere Untersuchungen zu diesem Thema bereits die Politik zum Handeln veranlasst, doch hat sich an der steten Zunahme von Zahlungsverzögerungen bis hin zu Forderungsausfällen bislang nichts Entscheidendes geändert.

Erik Ruh legt dazu in einem Aufsatz für die Fachzeitschrift „Verwaltung & Management“ neues empirisches Material vor, anhand dessen die Ursachen von Zahlungsverzug und deren Konsequenzen für die Auftragnehmer besser beleuchtet und der Blick auf die Maßnahmen gelenkt wird, mit denen die Wahrscheinlichkeit des Auftretens von Zahlungsverzug spürbar verringert werden kann. Dabei zeigt sich, dass gerade den Unternehmen selbst vielfältige Möglichkeiten zur Verfügung stehen, deren Nutzung aber an eine bessere Kenntnis verwaltungsrechtlicher Strukturen und der einschlägigen gesetzlichen Vorschriften gekoppelt ist. Der Leser erhält somit einen Überblick über die für ein professionelles Forderungsmanagement in Behörden und Unternehmen zur Verfügung stehenden Instrumente.

Der ausführliche Beitrag kann in „Verwaltung & Management – Zeitschrift für allgemeine Verwaltung“ (Nomos Verlagsgesellschaft, Baden-Baden) auf den Seiten 105 bis 110 von Heft 2/2006 nachgelesen werden.