



Praktische Ausgestaltung eines Anti-Fraud-Managements unter Einsatz elektronischer Signaturen und Zeitstempel

Ambitionierte Zielvereinbarungen, missbräuchliche Ausnutzung von Handlungsspielräumen, unzureichendes Kontrollbewusstsein, blinder Gehorsam, externe Datenangriffe oder Mitarbeiter und Dritte mit krimineller Energie können in jedem Unternehmen erhebliche Schäden verursachen. Das Schlagwort „Fraud“ (engl. für Wirtschaftskriminalität) hat auch in Deutschland Einzug in die öffentliche Debatte und mediale Berichterstattung gehalten. Das Bundeskriminalamt (BKA) berichtet über Schäden durch Wirtschaftskriminalität in Höhe von 4,2 Mrd. Euro in 2005. In dieser Zahl ist die Dunkelziffer nicht enthalten, die nach Schätzungen 80-90% der Schadenssumme ausmacht. Der Beitrag soll daher die Grundzüge des Anti-Fraud-Management (AFM) darstellen. Ein wirksam implementiertes AFM stellt einen entscheidenden Baustein zur Minimierung von bestehenden Betrugs- bzw. Unterschlagungsrisiken im Unternehmen dar.

Rahmenbedingungen für die Einführung eines AFM

Der US-amerikanische Sarbanes-Oxley Act (SOA) von 2002 stellt einen der wesentlichen Auslöser für die Notwendigkeit zur Implementierung eines AFM bei in erster Linie börsennotierten Unternehmen dar. Grund für die Einführung des SOA waren die durch erhebliche Bilanzmanipulationen bedingten Zusammenbrüche US-amerikanischer Unternehmen wie z. B. Enron, Worldcom und Global Crossing. Im Rahmen des SOA wurde die Corporate Governance insoweit verändert, dass die Unternehmensleitung nunmehr regelmäßig bestätigen muss, dass sie die Jahresabschlüsse sowie die internen Kontrollen, die einen wesentlichen Einfluss auf die finanzielle Berichterstattung haben, überprüft hat und diese keine wesentlichen Fehler enthalten. Im Rahmen dieser Berichterstattung müssen auch alle Betrugsfälle genannt werden, in die das Management oder Mitarbeiter des Unternehmens involviert sind und die einen signifikanten Einfluss auf Finanzdaten oder interne Kontrollen haben.

Insgesamt wird somit ein größeres Gewicht auf die Aufdeckung von Fraud im Rahmen der Jahresabschlusserstellung und -prüfung gelegt.

Mängel im AFM können eine Kontrollschwäche darstellen, über die im Rahmen der SOA-Berichterstattung an das Audit Committee und im Falle einer wesentlichen Kontrollschwäche sogar öffentlich im 20 F Report an die SEC berichtet werden muss.

Über den SOA und damit über die Aufdeckung von fraudulent Handlungen im Rahmen der Jahresabschlusserstellung und der externen Berichterstattung hinaus werden durch Neufassungen bzw. Verlautbarungen einschlägiger Prüfungsstandards Vermögensschädigungen auf Grund von widerrechtlicher Aneignung oder Verminderung von Gesellschaftsvermögen sowie auf Erhöhung von Verpflichtungen für das Gesellschaftsvermögen gerichtete Handlungen von gesetzlichen Vertretern, Mitarbeitern oder Dritten besonders Rechnung getragen. Hierzu zählen insbesondere Unterschlagungen und

Diebstahl. Zu nennen sind in diesem Zusammenhang der US-amerikanische SAS 99, der deutsche IDW PS 210 und der bereits genannte internationale Prüfungsstandard ISA 240. Im Umkehrschluss bedeutet dies, dass auch für Aspekte außerhalb der Jahresabschlusserstellung und externen Berichterstattung die Geschäftsführung entsprechende AFM-Vorkehrungen und -Maßnahmen zu implementieren hat.

Zielsetzung und Bausteine eines AFM

Ein wirksam implementiertes und kontinuierlich durchgeführtes AFM dient der Vermeidung, Aufdeckung und Verfolgung von bewussten Verstößen gegen kapitalmarktrechtliche Vorschriften sowie sonstige Gesetzesverstößen von Organen, Mitarbeitern oder Unternehmensfremden, die eine Schädigung der Vermögensinteressen eines Unternehmens zur Folge haben.

Ein AFM-Projekt beinhaltet die Komponenten Risiko- und Kontrollkultur (Con-

trol Environment), Risikoerfassung und -beurteilung (Fraud Risk Assessment), Prävention- und Aufklärungsmaßnahmen (Prevention und Detection), Implementierung eines Berichtswesens (Reporting) sowie eines Monitoring-Systems. Dabei müssen die Organmitglieder und die Beschäftigten eines Unternehmens für Fraud-Risiken und Compliance-Anforderungen im täglichen Geschäft sensibilisiert und ein sachgerechter Umgang mit diesen Risiken und Anforderungen sichergestellt werden.

Grundlage für den Aufbau eines AFM Systems ist der sog. Fraud Circle



Das Fraud Risk Assessment ist die Basis für die daran anschließend durchgeführten Maßnahmen, welche fortlaufend umgesetzt werden müssen. Wie der Fraud Circle symbolisch darstellt, kann keine Maßnahme isoliert betrachtet werden. Wesentlicher Bestandteil des Fraud Circle sind die Prevention- und Detection-Maßnahmen.

Fraud Risk Assessment

Im Rahmen des Fraud Risk Assessments werden unternehmensweite potentielle Fraud-Risiken identifiziert, z. B. im Wege einer Checklistenbefragung oder auf Basis von Ergebnissen aus durchgeführten Workshops in einzelnen Fachbereichen des Unternehmens. Gegenstand der Analyse ist die gesamte Aufbau- und Ablauforganisation, insbesondere unter Berücksichtigung der Möglichkeiten der Umgehung existierender Kontrollen. Nach einer anschließenden Priorisierung dieser Risiken wird ermittelt, inwieweit die bestehenden Kontrollen die Fraud-Risiken effektiv mindern und das Interne Kontrollsystem als funktionsfähig betrachtet werden kann.

Fraud Prevention und Detection

Aufbauend auf den Ergebnissen des Fraud Risk Assessments erfolgt die Implementierung von korrespondierenden Fraud Prevention und Detection Maßnahmen, um die identifizierten wesentlichen Fraud-Risiken zu beherrschen.

Zielsetzung hierbei ist es, von einem zufallsgesteuerten, ungeplanten Bekanntwerden von Betrugs- bzw. Unterschlagungsfällen zu einer proaktiven Vermeidung und Aufklärung durch geplante und zielgerichtete Maßnahmen überzugehen. Hierzu bedarf es der Implementierung von Verhaltensrichtlinien und Kontrollmechanismen, der Entwicklung von Aufklärungstests sowie von in einem Unternehmensprozess integrierten Prüfkriterien, die verdächtige Transaktionen und Unregelmäßigkeiten kennzeichnen und offen legen.

Die Nutzung quantitativer Methoden, wie spezieller Prüfsoftware oder mathematisch-statistischer Analysemodelle, sowie qualitativer Methoden wie Frühwarnindikatoren, Informationen aus öffentlich zugänglichen Quellen und Erfahrungen aus Fällen der Vergangenheit bzw. denkbaren Handlungsmustern, ist hierbei unerlässlich.

Die Einrichtung von wirksamen Detection-Maßnahmen dient im Wesentlichen der umfassenden Beantwortung von sieben „W“-Fragen:

Wer hat wann was wo mit wem wie und warum gemacht?

Diese sieben „W's“ müssen mit Hilfe einer nachweisbaren und gerichtsverwertbaren Dokumentation aufgeklärt werden. In diesem Zusammenhang ist an den Einsatz von Digitalen Signaturen und Zeitstempeln zu denken.

Reporting/Monitoring

Das AFM Reporting sollte in einer AFM spezifischen Reporting-Struktur festgehalten werden. Diese Reporting-Struktur muss Informationen über die Erst- und Folgeaufnahme der Fraud Risiken

und Maßnahmen, sowie eine Darstellung der Veränderungen und von Restrisiken enthalten. Die Basis für die Reporting Struktur kann somit ein Fraud Risk Reduction-Report bilden. In diesem Report müssen alle wesentlichen Fraud Risiken sowie die dazugehörigen Maßnahmen (Prevention und Detection) systematisch aufgeführt werden.

Im Rahmen des AFM-Monitorings erfolgt eine regelmäßige Überprüfung und Dokumentation der Vorgaben des AFM. Basis für das Monitoring kann der Fraud Risk Reduction-Report bilden. Die Ergebnisse dieses regelmäßigen Monitorings sollten über definierte Berichtswege an die Aufsichtsgremien

(Aufsichtsrat, Audit Comitee) gemeldet werden.

Nach unserer Erfahrung empfiehlt es sich, das Management des AFM an eine unabhängige Stelle, wie z. B. den Chief Compliance Officer, zu vergeben. Nur so können Informations- und Reibungsverluste im Unternehmen bezüglich der systematischen Erhebung von Fraud-Risiken und der hierauf aufzusetzenden Maßnahmen vermieden werden.

Die Sachverhaltsaufklärung bei eingetretenen Fraud Fällen sollte aber nicht im Bereich des AFM-Managements angesiedelt werden, sondern bei einer davon unabhängigen Stelle wie z. B. die Interne Revision. Wichtig ist hier zu erwähnen, dass die Unternehmensführung sich rechtzeitig mit einem Notfallplan für Fraud-Fälle auseinandersetzen sollte. Der Notfallplan und dessen Übung sind ebenfalls ein wichtiger Bestandteil des AFM. Denn eine unsystematische Bearbeitung von Fraud-Fällen kann zu Beweisverlusten sowie Fehlkommunikationen führen, die den eingetretenen Schaden noch erhöhen können. In den meisten Fällen empfiehlt sich daher die Übertragung dieser Aufgabe an externe Forensiker, da diese über die gesetzlichen Bestimmungen der gerichtssicheren Datenerhebung in der Regel besser ausgebildet sind und über die entsprechenden Systeme und Programme verfügen.

Wer hat wann was wo mit wem wie und warum gemacht?

Digitale Signaturen und Zeitstempel als Prevention / Detection-Maßnahmen im Anti-Fraud-Management

Digitale¹ Signaturen und Zeitstempel bieten die Möglichkeit elektronische Prozesse sicher abzubilden und langfristig, nachweisbar zu dokumentieren. Sie sind das IT-Werkzeug, um kostenintensive Papierprozesse durch elektronische abzulösen. Der Gesetzgeber hat Signaturen und Zeitstempel in verschiedenen Ausprägungen (Sicherheitsstufen) vorgesehen, die es ermöglichen, signierten Daten unterschiedliche rechtliche Relevanz zu geben. Dies geht soweit, dass signierten elektronischen Daten (Dokumente) vor Gericht dieselbe rechtliche Bedeutung zukommt, wie Papierdokumenten.

Die im Rahmen eines AFM eingeführten elektronischen Signaturen bzw. digitalen Zeitstempel dienen unter anderem aufgrund ihrer Charakteristik als wirksame Abschreckungsmaßnahme gegenüber fraudulenter Handlungen, da nunmehr jede mögliche Manipulation von Dokumenten oder Vorgängen personen- und zeitbezogen nachvollziehbar ist.

Daneben entfalten sie zusätzlich eine Beweissicherungsfunktion. Denn sie erleichtern die detaillierte Darstellung der einzelnen Tathandlungen unter Berücksichtigung bzw. Einbeziehung des involvierten Personenkreises. Dies führt letztendlich zu einer fast lückenlosen Beweiskette, die in den sich möglicherweise anschließenden gerichtlichen Auseinandersetzungen die Beweisführung erheblich erleichtert. Denn nichts ist im Anschluss an die Aufdeckung von wirtschaftskriminellen Handlungen unbefriedigender, als die Täter letztendlich nicht zur Verantwortung ziehen zu können.

Was ist eine digitale Signatur?

Spricht man von einer digitalen Signatur, meint man im Allgemeinen eine so genannte „personenbezogene Signatur“. Sie stellt eine elektronische Unterschrift dar. Signaturen und auch Zeitstempel werden unter anderem durch komplexe mathematische Operationen erstellt, die wiederum durch entsprechende Softwarelösungen durchgeführt werden.

Ein Anwender kann, soweit er über die notwendige Hard- und Software verfügt, elektronische Daten personenbezogen signieren. Die Signatur stellt damit eine elektronische Unterschrift der Daten dar. Übertragen auf das allgemeine Geschäftsleben ermöglicht dies die Beschleunigung von Bearbeitungsprozessen und somit Kostenreduktionen. So kann z. B. ein Vertrag elektronisch unterzeichnet und per Email an einen Geschäftspartner übermittelt werden. Dieser kann durch entsprechende Prüfung der Signatur eindeutig feststellen, welche Person das Dokument unterzeichnet hat. Die personenbezogene Signatur dokumentiert somit das „Wer“ und „Was“.

Der digitale Zeitstempel

Vielfach ist jedoch ein weiterer Sachverhalt von Bedeutung. Das „Wann“ und „Was“. Für diese Art der Doku-

mentation wurde eine weitere Form der digitalen Signatur definiert – der digitale Zeitstempel. Zeitstempel bieten die Möglichkeit, eine unabhängige, verlässliche Zeitangabe für Signaturen bzw. signierte Daten zu erhalten. Elektronische Daten werden durch einen Zeitstempel quasi „eingefroren“.

Im Rahmen der Einrichtung von Prozess-Kontrollmaßnahmen können digitale Zeitstempel daher mehrere Funktionen übernehmen. Eine Funktion ist dabei von besonderer Bedeutung. Zeitstempel können, entsprechende Hard- und Software vorausgesetzt, nicht nachträglich erstellt, gelöscht oder ausgesetzt werden. Dies ist unabhängig von der Mitwirkung der am Prozess beteiligten Mitarbeiter. Die Prozessdokumentation kann daher auch nicht von Personen, die für die Prozessaufzeichnung verantwortlich sind, wie z. B. Systemadministratoren, gesteuert werden.

Wie bereits erläutert, muss im Rahmen der Corporate Governance versichert werden, dass Abschlüsse und interne Kontrollen geprüft wurden und keine wesentlichen Fehler vorhanden sind. Management und Unternehmensführung benötigen daher ein verlässliches Instrument, welches ihnen die Möglichkeit gibt, ein Statement über die Unternehmensprozesse abzugeben.

Aufgrund der stetig steigenden Komplexität von Unternehmensprozessen, ist eine derartige Aussage von den Verantwortlichen häufig nur schwer zu machen, ohne sich auf die Aussagen Dritter (z. B. Systemadministratoren) zu verlassen. Aus den genannten Gründen eignen sich Zeitstempel zur Implementierung übergeordneter Kontrollmechanismen.

Sie bieten ein IT-Werkzeug und Hilfsmittel, um Prozesse automatisch und transparent zu dokumentieren und gleichzeitig den Verantwortlichen aufzuzeigen, wenn ein Prozess von der Norm abweicht. Ein solches autark arbeitendes Monitoring-Instrument ermöglicht zum einen die sofortige Aufdeckung von Fraud und Einleitung von Gegenmaßnahmen und bietet zum anderen ein Abschreckungsmittel, Fraud überhaupt zu begehen.

¹Korrekterweise müsste die Bezeichnung „elektronische Signatur“ verwendet werden. Da sich die Bezeichnung „digitale Signatur“ im allgemeinen Sprachgebrauch jedoch stark verankert hat, werden hier und im Folgenden die Begriffe „digital“ und „elektronisch“ synonym verwendet.

Signaturen & Zeitstempel als Monitoring Instrument

Praktische Umsetzung

Um Prozesse durch Zeitstempel abzusichern, benötigt man im Wesentlichen zwei Komponenten. Eine entsprechende Zeitstempelsoftware und eine geeignete Hardware, auf der die Software betrieben wird (z. B. einen Server).

Grundsätzlich kann man die Erstellung von digitalen Zeitstempeln vereinfacht wie folgt beschreiben: Eine Zeitstempelsoftware erstellt automatisch digitale Zeitstempel für alle mit Hilfe der Software verarbeiteten Daten. Dies können z. B. LogFiles, einzelne Prozessschritte oder einzelne Dokumente sein.

Bei Auswahl und Einsatz von Hard- und Software sollten zwei Kriterien im Vordergrund stehen. Die technische Sicherheit, sowie die Anwenderfreundlichkeit und Integrationsfähigkeit in die bereits im Unternehmen bestehenden Prozesse.

Technische Sicherheit

Die Zeitstempelösung im Anti-Fraud-Kontext sollte auf weltweit gebräuchlichen Standards aufsetzen und gewährleisten, dass die Sicherheitsanforderungen möglichst hoch und allgemein anerkannt angesetzt sind.

Aus diesem Grund ist es sinnvoll, Zeitstempel im AFM-Kontext in einer besonders sicheren und nachweisbar nicht manipulierbaren Form zu erzeugen und mit den bereits bestehenden Geschäftsprozessen zu verknüpfen. Diese Sicherheit bei der Erzeugung von digitalen Zeitstempeln kann z. B. durch spezielle Hardware gewährleistet werden. Besonders geeignet sind hierzu Hardware Security Module (HSM's). Sie werden seit Jahren in kritischen Geschäftsprozessen, u. a. im Militärischen Bereich, eingesetzt. Diese HSM's können einfach und schnell mit spezieller Zeitstempelsoftware ausgestattet und somit die Zeitstempel in der sicheren Umgebung des HSM's („Zeitstempel-Server (HSM)“) erzeugt werden.

Die Zeitstempelsoftware sollte so beschaffen sein, dass sie eine möglichst hohe Anzahl von Zeitstempeln innerhalb kürzester Zeit erzeugen kann (Performanz). So ist sichergestellt, dass auch hochvolumige Prozesse, wie gerade im Anti-Fraud-Management, ohne Zeitverzug signiert und dokumentiert werden können.

Anwenderfreundlichkeit und Integration in Bestandsprozesse

Der Einsatz eines „Zeitstempel-Servers (HSM)“ ist auch aus Sicht der Anwenderfreundlichkeit und Integrationsfähigkeit positiv zu bewerten. So ist der Eingriff in bestehende IT-Infrastrukturen zur Implementierung minimal. Vorteilhaft wirkt sich vor allem aus, dass digitale Zeitstempel grundsätzlich für jedes Datenformat erstellt werden können. Das bedeutet, dass man Prozess- und Bewegungsdaten in jedem beliebigen Format erzeugen und dem „Zeitstempel-Server (HSM)“ zuführen kann.

Die Bedeutung von digitalen Zeitstempeln für die Prüfung

Wie erwähnt, muss eine IT-Lösung nicht nur sicherstellen, dass elektronische Daten nicht unbemerkt manipuliert werden können. Eine ebenso wichtige Anforderung ist die Nachweisbarkeit. Ein Zeitstempelverfahren ist nur dann sinnvoll für die Dokumentation, wenn bei späteren Prüfungen einfach, schnell, über lange Zeiträume hinweg und überzeugend nachgewiesen werden kann, dass die signierten Daten dem tatsächlichen Stand der Prozesse zum fraglichen Zeitpunkt entsprechen.

Durch Einsatz von hochsicheren HSM's in Verbindung mit Zeitstempelsoftware kann dieser Nachweis schnell und einfach erbracht werden. Am Markt sind bereits HSM's verfügbar, die nach weltweit gültigen IT-Sicherheitsstandards geprüft wurden. Hierzu zählen CC², FIPS 140-2³ und andere, die hier nicht näher erläutert werden sollen.

Entscheidend ist, dass der Anwender bereits auf eine von unabhängigen Dritten geprüfte Hardware zugreifen kann (und dies auch zwingend beim Anbieter einfordern sollte), innerhalb derer die digitalen Zeitstempel erstellt werden.

Ein weiterer positiver Aspekt beim Einsatz von Zeitstempeln ist die Verfügbarkeit der Prozess-Dokumentationen in elektronischer Form. Das Management kann somit effizient und von jedem Standort aus interne Kontrollen durchführen bzw. überprüfen.

Zur Prüfung der digitalen Zeitstempel stehen bereits verschiedene Tools zur Verfügung. Hierunter auch Softwaremodule, mit deren Hilfe man automatisiert und schnell auch hohe Volumen, also eine Vielzahl an digitalen Zeitstempeln, prüfen kann.

²CC – Common Criteria

³FIPS – Federal Information Processing Standard

.....
Judith Balfanz
SIGNAMIC

Christian Parsow
Senior Manager, Wirtschaftsprüfer & Steuerberater
Deloitte & Touche GmbH
cparsow@deloitte.de