

Milliardenschäden durch Wirtschaftskriminalität

Praktische Ausgestaltung eines Anti-Fraud-Managements unter Einsatz digitaler Signaturen

Die Komplexität von Prozessen in Unternehmen nimmt von Tag zu Tag zu. Ein wesentlicher Grund dafür, dass Schutz und Nachvollziehbarkeit von immer größerer Bedeutung sind. Vor allem Führungskräfte benötigen daher einfach anwendbare und gleichzeitig verlässliche Tools, um Prozesse zu überwachen, Risiken, Betrugsfälle und Fehler zu identifizieren und Gegenmaßnahmen einzuleiten – das Anti-Fraud-Management. Vor dem Hintergrund evtl. persönlicher Haftungsrisiken von Organträgern sowie des US-amerikanischen Sarbanes-Oxley Acts werden in dem Aufsatz die Notwendigkeiten und Rahmenbedingungen für die Implementierung eines Anti-Fraud-Managements dargestellt. Hierbei wird erläutert, wie digitale Signaturen und Zeitstempel zur Implementierung automatisierter Anti-Fraud-Management-Prozesse genutzt werden können.

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 berichtet über Schäden durch Wirtschaftskriminalität in Höhe von 4,2 Mrd. € im Jahr 2005. In dieser Zahl ist die Dunkelziffer nicht enthalten, die nach Schätzungen 80 bis 90% der Schadenssumme ausmacht.

Im Folgenden werden die Grundzüge des Anti-Fraud-Managements (AFM) dargestellt. Ein wirksam implementiertes AFM stellt einen entscheidenden Baustein zur Minimierung von bestehenden Betrugs- bzw. Unterschlagungsrisiken im Unternehmen dar.

Rahmenbedingungen für die Einführung eines Anti-Fraud-Managements

Motivation zur Einrichtung eines AFM liefern u. a. persönliche Haftungsrisiken für Organmitglieder sowie Führungskräfte mit Personalverantwortung, die sich allein aufgrund ihrer Stellung ergeben können, wenn strafbare Handlungen im Unternehmen begangen werden, selbst wenn sie davon keine konkrete Kenntnis hatten. Wer sich von der Haftung befreien will, muss nachweisen können, dass ihn kein Organisationsverschulden trifft. Dies setzt voraus, dass der Verantwortungsbereich ordnungsgemäß orga-

nisiert ist, Mitarbeiter ordnungsgemäß und sorgfältig ausgesucht und regelmäßig in angemessener Weise überwacht werden. Die Implementierung eines AFM enthält wesentliche Merkmale, die zur Schuldbefreiung eines Verantwortlichen führen können.

Nach den Bestimmungen des US-amerikanischen Sarbanes-Oxley Acts (SOX) ist das AFM eine Komponente des Kontrollumfelds eines Unternehmens. Mängel im AFM können eine Kontrollschwäche darstellen, über die bei der SOX-Berichterstattung an das Audit Committee und im Fall einer wesentlichen Kontrollschwäche sogar öffentlich im 20F-Report an die Börsenaufsichtsbehörde (Securities and Exchange Commission – SEC) berichtet werden muss. Über den SOX hinaus sind als Grundlage für die Einführung eines AFM auch die Prüfungsstandards IDW PS 210 und der internationale Prüfungsstandard ISA 240 zu nennen.

Zielsetzung und Bausteine eines Anti-Fraud-Managements

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

Ein AFM-Projekt enthält die Komponenten Risiko- und Kontrollkultur (Control Environment), Risikofassung und -beurteilung (Fraud Risk Assessment), Prävention- und Aufklärungsmaßnahmen (Prevention und Detection), Implementierung eines Berichtswesens (Reporting) und 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 Fraud Circle (Bild 1). Das Fraud Risk Assessment ist die Basis für die daran anschließend durchgeführten Maßnahmen, die fortlaufend umgesetzt werden müssen. Wie der Fraud Circle sym-

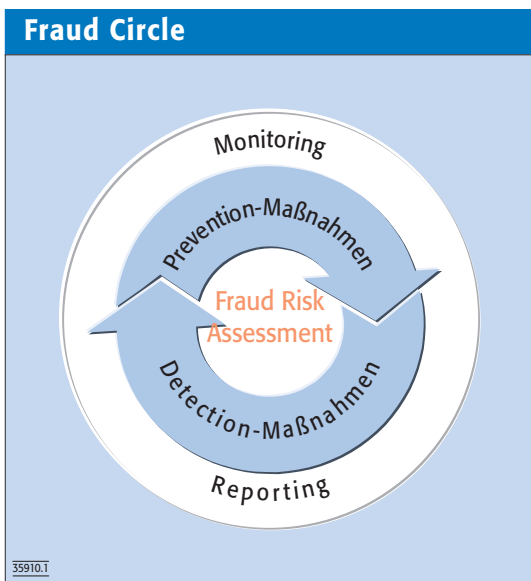


Bild 1. Mit dem Fraud Risk Assessment werden unternehmensweit potenzielle Fraud-Risiken identifiziert

bolisch darstellt, kann keine Maßnahme isoliert betrachtet werden. Wesentlicher Bestandteil des Fraud Circles sind die Prevention- und Detection-Maßnahmen.

Fraud Risk Assessment

Mit dem Fraud Risk Assessment werden unternehmensweite potenzielle Fraud-Risiken identifiziert, z. B. im Wege einer Checklistenbefragung oder auf Basis von Ergebnissen aus Workshops in einzelnen Fachbereichen des Unternehmens. Gegenstand der Analyse ist die gesamte Aufbau- und Ablauforganisation, vor allem unter Berücksichtigung der Möglichkeiten, existierende Kontrollen zu umgehen. 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 werden korrespondierende Fraud-Prevention- und Detection-Maßnahmen implementiert, um die identifizierten, wesentlichen Fraud-Risiken zu beherrschen.

Zielsetzung hierbei ist es, von einem zufallsgesteuerten, ungeplanten Bekanntwerden von Betrugs- bzw. Unterschlagungsfällen zu ei-

ner proaktiven Vermeidung und Aufklärung durch geplante und zielgerichtete Maßnahmen überzugehen. Hierzu bedarf es der Implementierung von Verhaltensrichtlinien und Kontrollmechanismen, der Entwicklung von Aufklärungstests und von in den Unternehmensprozess integrierten Prüfkriterien, die verdächtige Transaktionen und Unregelmäßigkeiten kennzeichnen und offen legen.

Die Nutzung quantitativer Methoden, wie spezieller Prüfsoftware oder mathematisch-statistischer Analysemodelle, und 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 »Ws« müssen mit 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 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 zugehörigen Maßnahmen (Prevention und Detection) systematisch aufgeführt werden.

Im Rahmen des AFM-Monitorings findet eine regelmäßige Überprüfung und Dokumentation der Vorgaben des AFM statt. 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.

Es empfiehlt sich, das Management des AFM an eine unabhängige

Stelle 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 Fällen von Wirtschaftskriminalität sollte aber nicht beim AFM-Management angesiedelt werden, sondern bei einer unabhängigen Stelle, z. B. der internen Revision. Wichtig ist, dass die Unternehmensführung sich rechtzeitig mit einem Notfallplan für wirtschaftskriminelle Fälle auseinandersetzen sollte. Der Notfallplan und dessen Übung sind ebenfalls ein wichtiger Bestandteil des AFM. Denn eine unsystematische Bearbeitung dieser Fälle kann zu Beweisverlusten sowie zur Fehlkommunikation 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 i. d. R. besser ausgebildet sind und über die entsprechenden Systeme und Programme verfügen.

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 (Bild 2). 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.

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

Die im Rahmen eines AFM eingeführten elektronischen Signaturen bzw. digitalen Zeitstempel dienen u. a. aufgrund ihrer Charakteristik als wirksame Abschreckungsmaßnahme gegenüber wirtschaftskriminellen 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 Tatbestände unter Berücksichtigung des involvierten Personenkreises. Dies führt zu einer fast lückenlosen Beweiskette, die in den sich möglicherweise anschließenden gerichtlichen Auseinandersetzungen die Beweisführung erleichtert. Denn nichts ist im Anschluss an die Aufdeckung von wirtschaftskriminellen Handlungen unbefriedigender, als die Täter nicht zur Verantwortung ziehen zu können.

Was ist eine digitale Signatur?

Mit einer digitalen Signatur ist im Allgemeinen eine »personenbezogene Signatur« gemeint. Sie stellt eine elektronische Unterschrift dar. Signaturen und auch Zeitstempel werden u. a. durch komplexe mathematische Operationen erstellt, die wiederum mit 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 ein Vertrag elektronisch unterzeichnet und per E-Mail 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 Dokumentation wurde eine weitere Form der digitalen Signatur definiert – der digitale Zeitstempel.

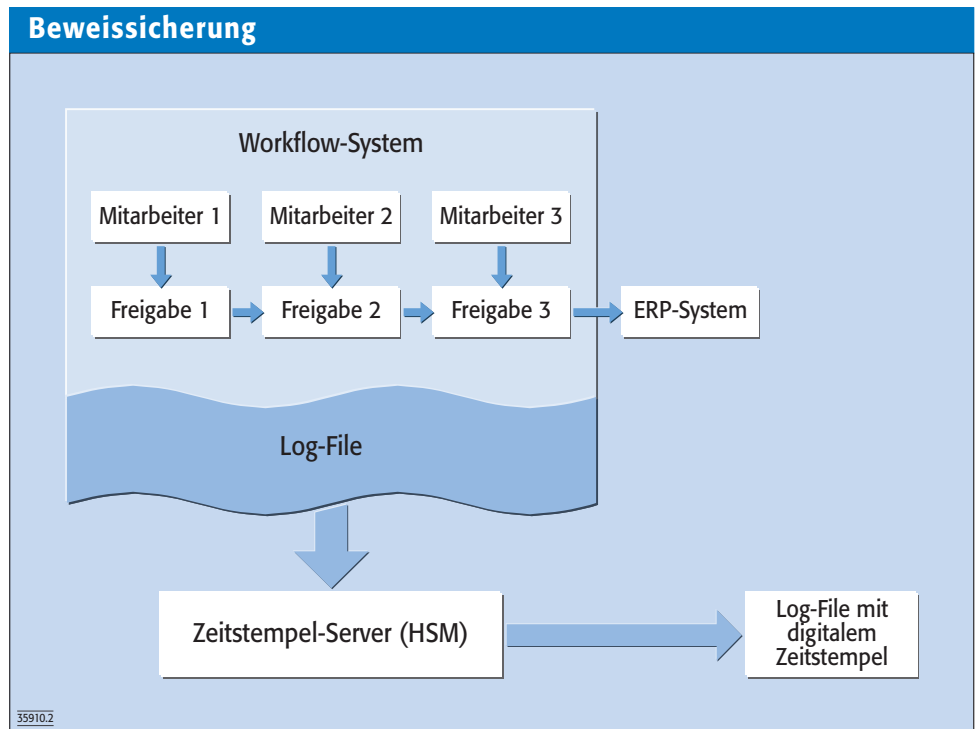


Bild 2. Eine Zeitstempelsoftware erstellt automatisch digitale Zeitstempel für alle mit der Software verarbeiteten Daten, z. B. Log-Files, einzelne Prozess-Schritte oder Dokumente

Zeitstempel bieten die Möglichkeit, eine unabhängige, verlässliche Zeitangabe für Signaturen und signierte Daten zu erhalten. Elektronische Daten werden durch einen Zeitstempel quasi »eingefroren«.

Bei der Einrichtung von Prozesskontrollmaßnahmen können digitale Zeitstempel daher mehrere Funktionen übernehmen. Eine Funktion ist 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 Systemadministratoren, gesteuert werden.

Im Rahmen der Corporate Governance muss versichert werden, dass Abschlüsse und interne Kontrollen geprüft wurden und keine wesentlichen Fehler vorhanden sind. Das Management benötigt daher ein verlässliches Instrument, das ihm ermöglicht, eine Aussage über die Unternehmensprozesse abzugeben.

Aufgrund der stetig steigenden Komplexität von Unternehmens-

prozessen, ist eine derartige Aussage von den Verantwortlichen häufig nur schwer zu machen, ohne sich auf die Aussagen Dritter (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 zu zeigen, wenn ein Prozess von der Norm abweicht. Ein solches autark arbeitendes Monitoring-Instrument ermöglicht zum einen die sofortige Aufdeckung von Wirtschaftskriminalität und die Einleitung von Gegenmaßnahmen und bietet zum anderen ein Abschreckungsmittel, wirtschaftskriminelle Handlungen zu begehen.

Praktische Umsetzung

Um Prozesse durch Zeitstempel zu sichern, werden hauptsächlich zwei Komponenten benötigt, eine entsprechende Zeitstempelsoftware und eine geeignete Hardware auf der die Software betrieben wird, z. B. einen Server.

Grundsätzlich kann die Erstellung von digitalen Zeitstempeln vereinfacht wie folgt beschrieben

werden: Eine Zeitstempelsoftware erstellt automatisch digitale Zeitstempel für alle mit der Software verarbeiteten Daten. Dies können z. B. Log-Files, einzelne Prozess-Schritte oder 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 im Unternehmen bestehenden Prozesse.

Technische Sicherheit

Die Zeitstempelösung im AFM-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 Hardware Security Module (HSM). Sie werden seit Jahren in kritischen Geschäftsprozessen, u. a. im militärischen Bereich, eingesetzt. Diese HSM können einfach und schnell mit spezieller Zeitstempelsoftware ausgestattet und somit die Zeitstempel in der sicheren Umgebung des »Zeitstempel-Servers (HSM)« erzeugt werden.

Die Zeitstempelsoftware sollte so beschaffen sein, dass sie eine möglichst hohe Zahl von Zeitstempeln innerhalb kürzester Zeit erzeugen kann (Performance). So ist sichergestellt, dass auch hochvolumige Prozesse wie im AFM 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 Prozess- und Bewegungsdaten in jedem beliebigen Format erzeugt und dem »Zeitstempel-Server (HSM)« zugeführt werden können.

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 in Verbindung mit Zeitstempelsoftware kann dieser Nachweis schnell und einfach erbracht werden. Am Markt sind bereits HSM verfügbar, die nach weltweit gültigen IT-Sicherheitsstandards geprüft wurden. Hierzu zählen CC (Common Criteria), FIPS 140-2 (Federal Information Processing Standard) u. a.

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 Prozessdokumentationen in elektronischer Form. Das Management kann somit effizient und von jedem Standort interne Kontrollen durchführen.

Zur Prüfung der digitalen Zeitstempel stehen bereits verschiedene Tools zur Verfügung. Hierunter auch Softwaremodule, mit denen automatisiert und schnell auch hohe Volumina, also eine Vielzahl an digitalen Zeitstempeln, geprüft werden können.

(35910)

judith.balfanz@authentidate.de

cparsow@deloitte.de