

## Organisations-Sicherheit IT-Sicherheit und Compliance

### Inhalt:

→ Kein Spiel ohne Grenzen Seite 2

→ Revisionsssicheres Auditing:  
Kontrollmechanismen und  
Instrumente für das IT-Management Seite 8

→ Impressum

# Kein Spiel ohne Grenzen

IT-Security und Compliance sind eng miteinander verknüpft und beide für Unternehmen von existenzieller Bedeutung.

❖ Text: Dr. Volker Scheidemann

Die postmoderne Welt ist pluralistisch, zufällig, chaotisch – so behauptet es jedenfalls die Internet-Enzyklopädie Wikipedia. Ein Zustand, der die Sehnsucht nach Ordnung weckt. Denn selbst Kinderspiele machen nur mit guten Regeln Spaß. Und wer mogelt, darf nicht mehr mitspielen. Auf Unternehmen übertragen heißt das: Durcheinander und Strukturlosigkeit sind so gut wie immer existenzbedrohend. Um allen Beteiligten größere Sicherheit zu geben, prägen neben Managementanstrengungen vor allem gesetzliche Anforderungen und Branchenregeln das Streben nach Ordnung. »Compliance« – also die Einhaltung all dieser Vorschriften – heißt der zugehörige Fachbegriff. Ein Anspruch, den Unternehmen routinemäßig erfüllen müssen.

Je feingliedriger und differenzierter Produktion und Dienstleistungen werden, um so stärker wächst die damit verbundene Informationsfülle an. Seit der sogenannten »digitalen Revolution« ist damit ein



weltweiter Datenaustausch verbunden, der über Internet oder E-Mail in Sekundenschnelle erfolgt. Dieser bedeutet eine drastische Beschleunigung der Lebensverhältnisse, die insbesondere den Wirtschaftsunternehmen riesige Wachstumspotenziale erschlossen hat.

## 3

### Compliance

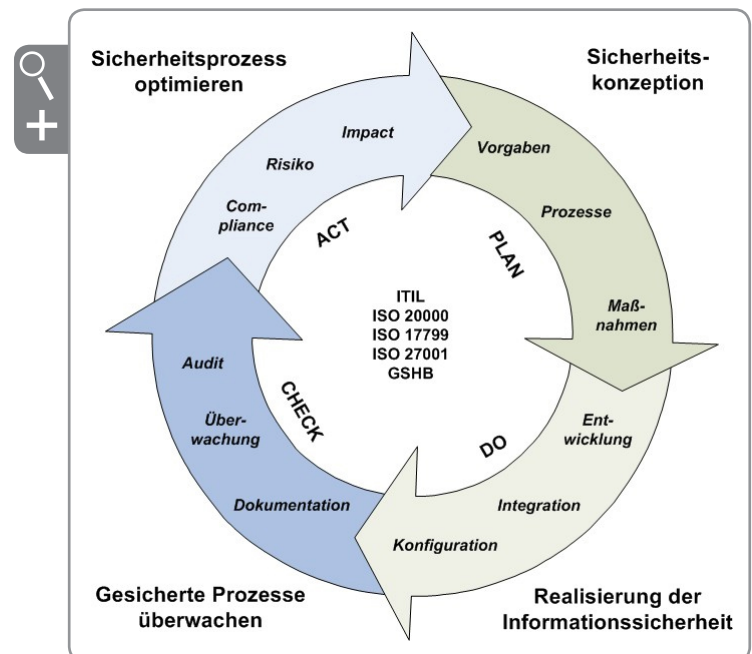
Mit dem Begriff »Compliance« wird die Einhaltung von und Übereinstimmung mit verpflichtenden Vorgaben bezeichnet. Diese Regeln können sowohl gesetzlich vorgeschrieben sein als auch aus den organisatorischen Bedürfnissen einer Branche oder Industrie resultieren.

Doch wo so viel Licht ist, fällt immer auch ein Schatten. Denn der schnelle und unmittelbare Datenaustausch mit nahezu jedem Ort auf der Welt birgt auch eine Reihe von Risiken. Die entgrenzte Kommunikation macht es kaum noch möglich, den Rahmen des eigenen Unternehmens wahren zu können. Kundendaten oder firmeneigene Forschungsergebnisse können heute leichter denn je in unbefugte Hände gelangen – sei es versehentlich, sei es in krimineller Absicht. Und konsequenter Weise finden die rasend schnellen digitalen Medien auch beinahe täglich einen spektakulären Fall, in dem einer Firma irgendwo in Deutschland Daten abhanden gekommen sind.

### Risiko Datenverlust

Gerade in Zeiten, in denen der Datenschutz und die informationelle Selbstbestimmung als Werte deutlich an Bedeutung gewonnen haben, werden solche Pannen von der Bevölkerung zu recht kaum noch

toleriert. Auch der Gesetzgeber sieht sich in der Pflicht, für mehr Sicherheit und sorgfältige Datenhaltung zu sorgen. Das Bundesdatenschutzgesetz BDSG belegt beispielsweise Schutzverletzungen personenbezogener Daten inzwischen mit erheblich höheren Geldbußen. Wer den Verlust solcher Daten zu verantworten hat, muss ihn außerdem öffentlich machen. Und wo aus Datenverlusten unmittelbar ein finanzieller Schaden droht, wie etwa in der Kredit-



IT-Sicherheit ist ein zyklischer Prozess

## 4

kartenindustrie, sind die brancheninternen Standards für IT-Sicherheit – wie etwa der PCI-DSS »Payment Card Industry Data Security Standard« – seit jeher besonders hoch. Anforderungen, die alle Unternehmen zum Handeln zwingen. Denn wenn diese die Vorschriften nicht erfüllen, verschwinden sie im ungünstigsten Fall vom Markt.

Beispiel: Ein Onlineshop ohne Zahlungsmöglichkeit per Kreditkarte ist heutzutage kaum vorstellbar. Und mit Branchenriesen wie Visa oder Mastercard ist nicht zu spaßen. Sie bestimmen, wer mitspielen darf.

So ist Compliance längst zu einem Begriff geworden, der die Unternehmenswelt wie kaum ein zweiter prägt. Wer sich »compliant« – so das Adjektiv – verhalten möchte, greift vor allem auf Maßnahmen aus dem Bereich der IT-Security zurück. Dabei empfiehlt es sich, derartige Compliance-Anforderungen nicht ausschließlich als unübersichtliches Regelungs-dickicht wahrzunehmen. Denn viele dieser Vorgaben dienen auch dem Zweck, einer Reihe unternehmerischer Risiken wirkungsvoll begegnen zu können. Wer sich konsequent an sie hält, für den können sie auch eine Vielzahl von Chancen bedeuten. Anders gesagt: Da die Einhaltung von Regeln ohnehin sichergestellt werden muss, sollte man bei der Gelegenheit auch die Arbeitsprozesse gründlich unter die Lupe nehmen und sorgfältig analysieren, um sie anschließend auch verbindlich steuern zu können – ein Vorgang, der wegen seiner Komplexität heute oft IT-gestützt erfolgt.

### Digitalisierte Abläufe helfen

Auch für diesen Bereich der IT-gestützten Steuerung von Arbeitsprozessen hat sich mit dem Begriff »Governance« ein Schlagwort etabliert, das inzwischen ebenfalls längst weite Kreise gezogen hat. Unter »IT-Governance« oder auch »eGovernance« versteht man das Abbilden von unternehmensinternen Regelungen über das Computersystem, damit



### Über die Applied Security GmbH (apsec)

Seit mehr als zwölf Jahren am Markt tätig, ist das Unternehmen Applied Security GmbH, kurz apsec, Spezialist für Informationssicherheit im öffentlichen Dienst, Gesundheitswesen und Finanzdienstleistungssektor. Applied Security gehört zu den »Top 15«-Unternehmen der deutschen IT-Sicherheit. Im Bereich der IT-gestützten Unternehmenssteuerung (eGRC) arbeitet apsec mit EMC/RSA zusammen. Der amerikanische IT-Konzern verfügt mit der Managementkonsole »RSA Archer« über eines der umfangreichsten Tools zur elektronischen Unternehmensführung.

[www.apsec.de](http://www.apsec.de)

## 5

diese in Form von Arbeitsroutinen umgesetzt werden können. Der elektronische Weg spart dabei nicht nur die Verwendung großen Papiermengen. Es lässt sich überdies sicherstellen, dass festgelegte Vorgaben auch bei den Mitarbeiterinnen und Mitarbeitern »ankommen«.

Und nicht zuletzt können auch eine Vielzahl von Faktoren IT-gestützt erfasst, aufgezeichnet und zur Verfügung gestellt werden, die für eine effektive Kontrolle erforderlich sind. Über die elektronische Steuerung lassen sich nahezu alle Faktoren festle-

gen, die für ein Unternehmen relevant sind – bis hin zu einer Unternehmenskultur, die sich zuverlässig in den Arbeitsalltag überführen lässt. In diesem Sinne können auch Partner- und Lieferantennetzwerke in die Kontrolle und Steuerung mit einbezogen werden, wenn sie an das IT-System angebunden sind. So bietet sich eine effektive Möglichkeit, allen Beteiligten einen klaren und verbindlichen Kurs vorzugeben.

Wer die für ihn gültigen Compliance-Vorschriften einhalten möchte, sollte nicht mit Tunnelblick unterwegs sein. Denn die erforderlichen Maßnahmen sind in der Regel eng mit anderen Bereichen verzahnt, die gleichfalls einer Steuerung bedürfen. Hier wäre beispielsweise der gesamte Bereich des Risikomanagements zu nennen. Denn viele Compliance-Vorschriften beziehen sich nur auf einen Teil der Maßnahmen, die dazu geeignet sind, das unternehmerische Risiko zu verringern.

### Standardisierte Sicherheit

Was darüber hinaus zu tun bleibt, regeln Industrienormen wie die ISO 27001 für Informationssicherheit. Sie nimmt unter anderem das Risikomanagement ganz genau unter die Lupe. Wer Compliance-Anforderungen in sein Risikomanagement integriert, kann deshalb beachtliche Synergieeffekte erzielen, da viele Kennzahlen nicht mehr doppelt und dreifach erfasst werden müssen. Und die Steuerungsgrup-

### Über den Autor

**Dr. Volker Scheidemann** ist Marketingleiter bei der Applied Security GmbH (apsec) und Autor zahlreicher Fachbeiträge. Seit mehr als zehn Jahren hält er im Rahmen unterschiedlicher Veranstaltungen Vorträge zu IT-Sicherheitsthemen.



## Weiterführende Links

### Produkte

...❖ fideAS file enterprise

Data Leakage Prevention und Verschlüsselung unternehmensweit

- » Transparente Verschlüsselung
- » Optimal für den unternehmensweiten Einsatz
- » Data Leakage Prevention

[www.apsec.de/deutsch/downloads/fideas-file-enterprise/](http://www.apsec.de/deutsch/downloads/fideas-file-enterprise/)

...❖ fideAS sign

Geld sparen mit der digitalen Signatur – mit fideAS sign sofort möglich

- » Zur automatischen Erzeugung qualifizierter elektronischer Signaturen in jeder Anwendung

[www.apsec.de/deutsch/downloads/fideas-sign/](http://www.apsec.de/deutsch/downloads/fideas-sign/)

...❖ fideAS health

Sichere Datenübermittlung im Gesundheitswesen

- » Zur sicheren Übertragung von Meldedaten an die Krankenkassen

[www.apsec.de/deutsch/downloads/fideas-health/](http://www.apsec.de/deutsch/downloads/fideas-health/)

...❖ fideAS web

Sicherheit für Onlineformulare –

flexibler Einsatz für Webanwendungen

[www.apsec.de/deutsch/downloads/fideas-web/](http://www.apsec.de/deutsch/downloads/fideas-web/)

...❖ fideAS smile

Kryptografisches Programmier-Toolkit zur Entwicklung eigener Anwendungen

- » Toolkit für die schnelle und einfache Entwicklung eigener kryptografischer Lösungen

[www.apsec.de/deutsch/downloads/fideas-smile/](http://www.apsec.de/deutsch/downloads/fideas-smile/)

...❖ fideAS miniCA

Digitale Zertifikate für Ihre Anwendungen

- » Trustcenter out-of-the-box
- » Zertifizierung einfach, schnell und kostengünstig selbst vornehmen

[www.apsec.de/deutsch/downloads/fideas-minica/](http://www.apsec.de/deutsch/downloads/fideas-minica/)

...❖ fideAS mail

Schnelle, einfache und sichere Kommunikation per E-Mail mit fideAS mail

- » E-Mail-Verschlüsselung
- » Empfänger benötigt keine Ent-

schlüsselungs-Software

- » Patentierte ESW-Technologie

[www.apsec.de/deutsch/downloads/fideas-mail/](http://www.apsec.de/deutsch/downloads/fideas-mail/)

...❖ CoSign

Eine verbindliche elektronische Unterschrift – einfach und kostengünstig

[www.apsec.de/deutsch/downloads/cosign/](http://www.apsec.de/deutsch/downloads/cosign/)

### Veranstaltungen

Download: Vortrag – 7 goldene Regeln der Data Leakage Prevention

[www.apsec.de/deutsch/downloads/veranstaltungen/](http://www.apsec.de/deutsch/downloads/veranstaltungen/)

### Lösungen

[www.apsec.de/deutsch/loesungen/](http://www.apsec.de/deutsch/loesungen/)

[www.apsec.de](http://www.apsec.de)

## 7

pe spart mit einem integrierten Vorgehen weitere Redundanzen ein. So entstehen übergeordnete Systeme, die weit mehr sicherstellen als nur eine gesetzeskonforme Datenverarbeitung.

Auch der Status von Arbeitsprozessen lässt sich mit dieser Systematik bequem überblicken – und zwar inklusive aller daran beteiligten Komponenten. Das so gewonnene integrierte Gesamtbild des Unternehmens erleichtert es dem Management, eine ganzheitliche und nachhaltige Perspektive einzunehmen. Auf der Grundlage ihrer eigenen Interessen werden miteinander verknüpfte Fachabteilungen dann Informationen austauschen und ihre Handlungsmechanismen zusammenführen. Wer seine Risiken kennt und priorisieren kann, dem genügt die Konzentration auf Schlüsselindikatoren – die Grundvoraussetzung für mehr Effizienz.

### Mehr Durchblick in der Unternehmenssteuerung

Als wesentlicher Nutzen einer IT-gestützten Unternehmenssteuerung sei deshalb der Zugewinn an Transparenz genannt. Mehr Transparenz entsteht dann, wenn

die unternehmerischen Kernbereiche – also IT, Finanzen und Operations/Produktion ihre Kontrollinstrumente bündeln. Über geeignete Management-Konsolen lässt sich auf diese Weise eine Vielzahl von Vorgängen gleichzeitig überblicken. Das macht jedoch nicht nur die Abläufe transparent. Vielmehr lässt sich auch leicht erkennen, welche Werte in den Produktivprozess eingebracht werden. Denn alle relevanten Kennzahlen stehen jederzeit unmittelbar zur Verfügung. Auf dieser Basis lassen sich sowohl die organisationsinternen Bedürfnisse als auch der Informationsbedarf von Geschäftspartnern leichter erfüllen. Insofern wird IT-Governance immer mehr zum Schlüssel für eine effektivere Unternehmensteuerung, da sie früher ungeahnte Kosteneinsparungs- und Effizienzsteigerungspotenziale erschließt. Dabei werden gesetzliche Regelungen und die Auswirkungen der Globalisierung den Druck zur ganzheitlichen Betrachtung und Steuerung noch weiter erhöhen. Es lohnt sich also, eine übergeordnete Perspektive einzunehmen. Wer dabei professionelles Prozess-Know-how einbezieht, kann zusätzlich von externer Expertise profitieren. ■

### Data Leakage Prevention



### Datenklau?

Schützen  
Sie sich mit  
fideAS® file  
enterprise.

Die kostenlose  
Testversion gibt  
es nur bei uns!

[www.apsec.de](http://www.apsec.de)

**apsec**  
applied security

# Revisionssicheres Auditing

## Kontrollmechanismen und Instrumente für das IT-Management

Zu einem vollständigen und effizienten Sicherheitskonzept gehört auch die »innere Sicherheit«. Hierzu ist der Einsatz von Kontrollmechanismen und Instrumenten für das IT-Management erforderlich.

❖ Bernd Reder, freier Autor

Kein Firmenchef möchte sich Nachlässigkeit nachsagen lassen, wenn es um Unternehmenssicherheit geht. Deshalb wird auch in Firewalls, Intrusion-Prevention, Antivirensoftware oder Unified-Threat-Management investiert. Und doch holen sich nach wie vor viele ein blaues Auge, weil sie die innere Sicherheit vernachlässigen. Dabei kann ohne die richtigen internen Vorkehrungen jeder, der umfangreiche Admin-Rechte hat oder sich solche verschafft, ganz einfach auf unternehmenskritische Daten zugreifen, sie manipulieren, kopieren oder löschen. Die Spuren werden mit Hilfe manipulierter Log-Dateien verwischt. Die Folgen tun weh: Kosten, Reputationsverlust und Anklage drohen.



Die Administratoren und Entwickler der IT-Infrastruktur eines Unternehmens – seien sie fest angestellt oder auch als externe Dienstleister engagiert – sind die Macher im Unternehmensnetz. Die Chefs der Firmen-IT garantieren den reibungslosen Betrieb, sie verantworten ein großes Stück Unternehmens-

## 9

erfolg und besetzen damit eine Position mit großer Verantwortung. Es ist allerdings auch ein höchst sensibler Posten, denn er hat mit den unternehmensrelevanten Daten zu tun, den Kronjuwelen einer Firma.

### Transparenz plus Vertrauen

Das Vertrauen des Geschäftsführers in seine IT-Abteilung ist Voraussetzung für eine funktionierende Zusammenarbeit. Aber es ist keine Frage des Vertrauens oder Misstrauens, sondern nur vernünftig, wenn sichergestellt wird, dass das Tun und Lassen der IT-Verantwortlichen transparent und nachvollziehbar ist. Firmenchefs müssen rekonstruieren und überblicken können, welche für ihr Unternehmen wichtigen Prozesse ablaufen, welche Aktionen angestoßen werden und was mit ihren Daten passiert. Schließlich haften sie mit aller Konsequenz sowie mit allen rechtlichen und finanziellen Folgen. Ein Verlust der Daten oder ein verschuldeter oder unverschuldeter Missbrauch kann strafrechtliche Konsequenzen nach sich ziehen: Wenn dem Unternehmen nachgewiesen werden kann, dass es nachlässig gearbeitet hat, dass seine Schutzmechanismen lückenhaft waren oder regulative Forderungen verletzt wurden.

### Unwissenheit schützt nicht

Die Transparenz der Aktivitäten innerhalb des Unternehmensnetzes ist folglich für Unternehmen kein »nice to have«, sondern ein strategischer und über-

lebenswichtiger Teil des Unternehmenserfolgs und Teil der Unternehmens-Compliance. Die neueste Studie des Beratungshauses Bearing Point »Agenda 2015« beschreibt das Compliance-Management als stetig wachsende Herausforderung. Die Einführung und Anwendung von IT-unterstützten Compliance-Prozessen und Kontrollmechanismen spielt dabei eine wichtige Rolle.

### Vorteile der Shell Control Box

- » Transparente Kontrolle und Protokollierung remote-administrativer Zugriffe,
- » Revisionssicherheit durch Verschlüsselung, Signatur und Zeitstempel der Aufzeichnungen,
- » führt den Nachweis, dass regulative Forderungen und Standards erfüllt und eingehalten werden,
- » Schutz der Administratoren durch unverfälschte Aufzeichnung der Daten,
- » Mehrfachverschlüsselung der Aufzeichnungen bietet Schutz vor Missbrauch (Vier-Augen-Prinzip),
- » revisionssichere Aufzeichnungsdaten liefern die Basis für Analysen, Troubleshooting, Kontrolle und Überwachung,
- » gewährleistet als forensisches Werkzeug hohes Zeiteinsparungspotential bei der Fehlersuche und Analyse,
- » integrierte Reporting-Tools und visuelle Darstellung der Aufzeichnungen.

**Dokumentationen »**

## 10

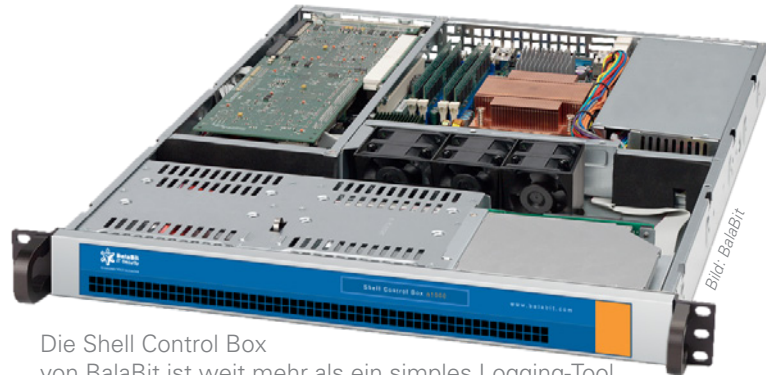
Ein aktuelles Whitepaper des Marktforschungshauses IDC, **»Compliance is More Than Just Cost«** vom Mai 2011, bestätigt, dass europäische Banken im Jahr 2010 rund zehn Prozent des gesamten IT-Budgets für Compliance-Maßnahmen ausgegeben haben. Die Analysten erwarten, dass dieser Prozentsatz 2011 auf 15 bis 20 Prozent steigen wird.

Die deutschen Gesetze fordern eindeutig die Einhaltung und Durchsetzung bestimmter Vorschriften und Regularien und damit ein höheres Maß an IT-Sicherheit. Stellvertretend seien hier das BDSG, SOX, Euro SOX, Basel II, HIPAA und PCI-DSS genannt. Unternehmen müssen Kontrolle und Revisionssicherheit ihrer Geschäftsprozesse gewährleisten beziehungsweise kontinuierlich durch neue Anforderungen verstärken, sonst riskieren sie Strafen und Regressansprüche. Die vier wichtigen Punkte der IT-Sicherheit:

- » Schutz der Vertraulichkeit,
- » Schutz der Integrität,
- » Sicherstellen der Verfügbarkeit sowie
- » Sicherstellen der Nachvollziehbarkeit.

### Transparenz erfordert die richtigen Lösungen

Ohne internen Schutz kann jeder, der umfangreiche Admin-Rechte hat oder sich solche verschafft, auf sensible, unternehmenskritische Daten zugreifen,



Die Shell Control Box von BalaBit ist weit mehr als ein simples Logging-Tool. Sie erfasst, analysiert und dokumentiert Aktivitäten von privilegierten IT-Nutzern und Systemverwaltern.

sie manipulieren, kopieren oder löschen – und seine Spuren durch manipulierte Log-Dateien verwischen. Üblicherweise speichern Firmen unternehmenskritische Daten auf einem zentralen Server, auf den nur spezielle Anwendungen, wie die Buchhaltungssoftware, zugreifen können. Um den gesetzlichen Anforderungen zu genügen, müssen solche Anwendungen Logs und Berichte generieren. Das reicht aber bei weitem nicht aus: Denn gewöhnlich registrieren die Systeme nur die Zugriffe auf die Datensätze innerhalb der Applikation. Was Systemadministratoren, autorisierte Mitarbeiter und externe Dienstleister mit den Daten machen, bleibt im Dunkeln.

### Lückenlose Kontrolle mit der Shell Control Box

Um lückenlose und aussagekräftige Beweismittel zu erhalten, die rechtssicher belegen, was im Unter-

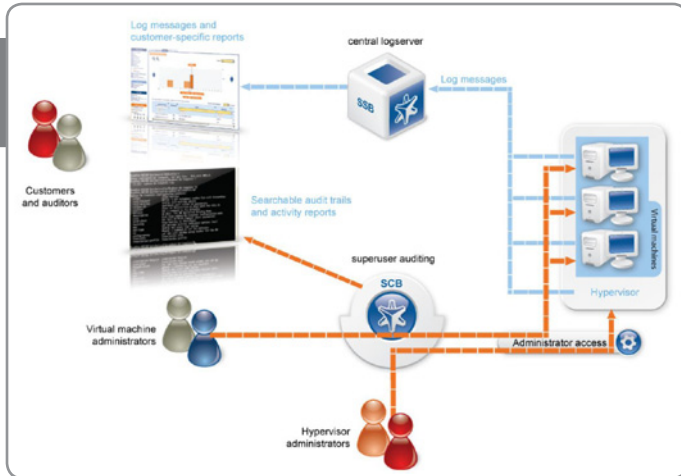


Bild: BalaBit

Auch Banken setzen verstärkt auf Cloud-Computing, etwa im Rahmen einer »Private Cloud«. Die Shell Control Box (SCB) erfasst und protokolliert auch in solchen komplexen IT-Umgebungen administrative Zugriffe.

nehmensnetz administrativ passiert, sind spezielle Lösungen notwendig: BalaBit IT Security ist ein Pionier und Marktführer in diesem Segment und stellt mit der Shell Control Box, kurz SCB, ein System zur Verfügung, das die Anforderungen der Unternehmen an Nachvollziehbarkeit und Transparenz erfüllt.

Mit Hilfe dieser Lösung werden die Aktivitäten bei Server-Zugriffen kontrolliert und lückenlos aufgezeichnet und Fehlerquellen ebenso beweissicher dokumentiert wie absichtliches Fehlverhalten. Die SCB kontrolliert und protokolliert die Zugriffe transparent auf Protokollebene. Die dabei entstehenden Aufzeichnungen, sogenannte Audit Trails, werden ver-

schlüsselt und signiert abgelegt. Die SCB liefert damit beweiskräftige Dokumentationen und die Basis für forensische Analysen. Zudem archiviert sie alle Vorkommnisse innerhalb der IT und der Geschäftsprozesse. Der komplette Administrationsvorgang wird übersichtlich visuell dargestellt.

## Anwendungsbereich Outsourcing und Cloud

Die Mehrheit der Unternehmen betreibt heute ihre Anwendungen nicht mehr selbst. Portale, Online-Shops, Unternehmenssoftware – viele geschäftskritische Applikationen werden an spezialisierte Partner übergeben oder »über die Cloud« via Internet bezogen. Dies birgt neben den Vorteilen auch Risiken – für beide Seiten. Zwar sind die Regeln und Inhalte der Zusammenarbeit mit dem externen Dienstleistern in den Service-Level-Agreements oder kurz SLA genau beschrieben, doch bei Nichterfüllung und Schadensfällen gibt es immense Grauzonen. Wenn die Leistung nun aber nicht oder fehlerhaft erbracht wurde, stellt sich die Frage, wer verantwortlich war. Oftmals arbeiten Kunde und Outsourcer an den gleichen Systemen, Applikationen und Daten.

Hier ist der Einsatz der SCB sowohl für Auftraggeber als auch für deren Dienstleister sinnvoll. Denn damit lässt sich eindeutig belegen, wer bei welchem Zugriff durch sein Verhalten die Fehler und Probleme



Video: Die Shell Control Box unterstützt Unternehmen dabei, die Compliance-Anforderungen an Nachvollziehbarkeit und Transparenz lückenlos umzusetzen. Auch Kunden gegenüber lässt sich damit jederzeit nachweisen, dass korrekt gearbeitet wurde.

me ausgelöst hat. Es kann somit der beweiskräftige Nachweis geführt werden, wer von den Vertragspartnern seine Sorgfaltspflicht verletzt hat. Der Dienstleister kann zudem mit der SCB nicht nur die Arbeit der eigenen Administratoren überprüfen und protokollieren, sondern dem Kunden gegenüber auch seine Leistungsfähigkeit und Effizienz dokumentieren.

## Anwendungsbereich Thin-Clients

Die SCB kann die von Thin-Client-Lösungen verwendeten Protokolle aufzeichnen und bietet so erstmals die Möglichkeit, auch die Aktivitäten auf Clients durchgängig zu überprüfen.

## Anwendungsbereich Angriffsanalysen

Nahezu ideal ist die SCB für den Betrieb von Honey-pot-Systemen. Denn das Gerät zeichnet auf, wann und wie sich Angreifer in die Server einhacken – ohne Angreifern die Möglichkeit zu lassen, die Aufzeichnungen zu verfälschen oder sogar zu löschen.

## Anwendungsbereich Echtzeitüberwachung von Dateizugriffen

Für Data-Leakage-Prevention- oder kurz DLP-Systeme kann die SCB den Zugriff auf den Netzwerkverkehr ermöglichen, der bisher nicht zu kontrollieren war. Dadurch ist es jetzt erstmals möglich, auch verschlüsselte Protokolle wie SSH und SFTP in die Echtzeitüberwachung mit einzubeziehen.

## Anwendungsbereich SSH-Kontrolle

Viele Unternehmen müssen SSH-Verbindungen zulassen, in denen man letztlich jedes Protokoll tunneln kann. Dafür gab es bisher keine nennenswerten Kontrollmöglichkeiten. Mit der SCB können Anwender vorgeben, welche Art von Datenverkehr – beispielsweise Shell, SCP, SFTP, Port-, X11- oder Agent-Forwarding – in einer SSH-Verbindung erlaubt ist. ■

## Über BalaBit

BalaBit IT Security wurde 2000 in Budapest gegründet und beschäftigt Stand Mitte 2011 über 100 Mitarbeiter. Das Unternehmen ist international tätig, zentrale Funktionen wie Entwicklung, Marketing und Support sind im Budapester Headquarter angesiedelt. Seit 2007 ist BalaBit mit einer GmbH in München vertreten, von der aus der Vertrieb in der D/A/CH-Region gesteuert wird. Der Vertrieb basiert auf einem Distributions- und Partnermodell. Darüber hinaus ist BalaBit weltweit über ein Partnernetzwerk präsent. Die Produkte sind bei führenden Unternehmen aus den Bereichen Finanzdienstleistungen, Telekommunikation, Luft- und Raumfahrt und dem Gesundheitswesen im Einsatz. Zu den Kunden zählen zudem Behörden und öffentliche Einrichtungen.

Das BalaBit Portfolio unterteilt sich in zwei Produktlinien.

BalaBits Produkt syslog-ng darf zu Recht als einer der meistverkauften Log-Prozessoren bezeichnet werden, syslog-ng setzt einen Quasi-Standard in diesem Bereich. Die Erfolgsstory basiert auf dem konsequenten Engagement im Open-Source-Umfeld. Die Open-Source-Variante wurde gezielt weiterentwickelt und um die kommerzielle Premium Edition erweitert, die spezielle Features für die revisionssicheren Logübertragungen und -speicherungen sowie umfangreichen Plattformsupport enthält. Als weiteren Schritt wird dieses Produkt als syslog-ng Store Box-Appliance mit deutlich erweitertem Funktionsumfang angeboten. Eine VMware Variante der syslog-ng



**BalaBit**  
IT Security

Store Box komplettiert das Portfolio. BalaBits Stärke ist der Bereich Log-Lifecycle-Management und die Einbeziehung einer Vielzahl heterogener Plattformen auf der Client-Seite.

Die Shell Control Box ist eine Lösung, die privilegierte IT-Zugriffe revisionssicher auditiert und kontrolliert. Die Anforderungen an Transparenz und Nachvollziehbarkeit der Prozesse nehmen ständig zu – in den Bereichen Compliance, SLA-Kontrolle, Recovery und Forensik ein unverzichtbarer Baustein in der IT-Architektur der Unternehmen. Die Shell Control Box zeichnet die gesamten administrativen Tätigkeiten in sogenannte Audit Trails auf und legt diese revisionssicher ab. Das Produkt wird als Appliance- und VMware-Lösung angeboten. Die Implementierung unterschiedlicher Integrationsmodi erlaubt es, das System schnell in das Unternehmensnetzwerk einzubinden, ohne Änderungen an Client- und Serversystemen durchzuführen. Die Shell Control Box als Multiprotokoll-Plattform für die Auditierung unterschiedlicher, im Rahmen der Administration verwendeter Zugriffsprotokolle ermöglicht durch ihre Architektur einen hocheffizienten Betrieb für die Anwender.

# Impressum

**Security Advisor ePublication** – Eine Publikation  
der [www.all-about-security.de](http://www.all-about-security.de)



**Verantwortlich für den redaktionellen Teil:**

Davor Kolaric,  
Alte Münchner Straße 12, 82407 Wielenbach,  
Tel: 0881-9247525,  
E-Mail: [info@all-about-security.de](mailto:info@all-about-security.de)

**Verantwortlich für Anzeigen:**

Davor Kolaric, Adresse wie oben

**Schlussredaktion:**

Dirk Glogau

**Layout / Satz:**

Uwe Klenner, Layout und Gestaltung,  
94036 Passau, Rittsteiger Str. 104,  
E-Mail: [info@layout-und-gestaltung.de](mailto:info@layout-und-gestaltung.de)

Mitteilung gemäß bayerischem Pressegesetz

**Besitzverhältnisse:**

[www.all-about-security.de](http://www.all-about-security.de),

Alte Münchner Straße 12, 82407 Wielenbach  
Alleingesellschafter: Davor Kolaric

**Urheberrecht:**

Alle in diesem Heft erscheinenden Beiträge sind urheberrechtlich geschützt. Alle Rechte, auch Übersetzungen und Zweitverwertung, vorbehalten. Reproduktionen, gleich welcher Art, nur mit schriftlicher Genehmigung des Verlags. Aus der Veröffentlichung darf nicht geschlossen werden, dass die beschriebenen Lösungen oder Bezeichnungen frei von gewerblichen Schutzrechten sind.

**Haftungshinweis:**

Trotz sorgfältiger inhaltlicher Kontrolle übernehmen wir keine Haftung für die Inhalte externer Links. Für den Inhalt verlinkter Seiten sind ausschließlich deren Betreiber verantwortlich.