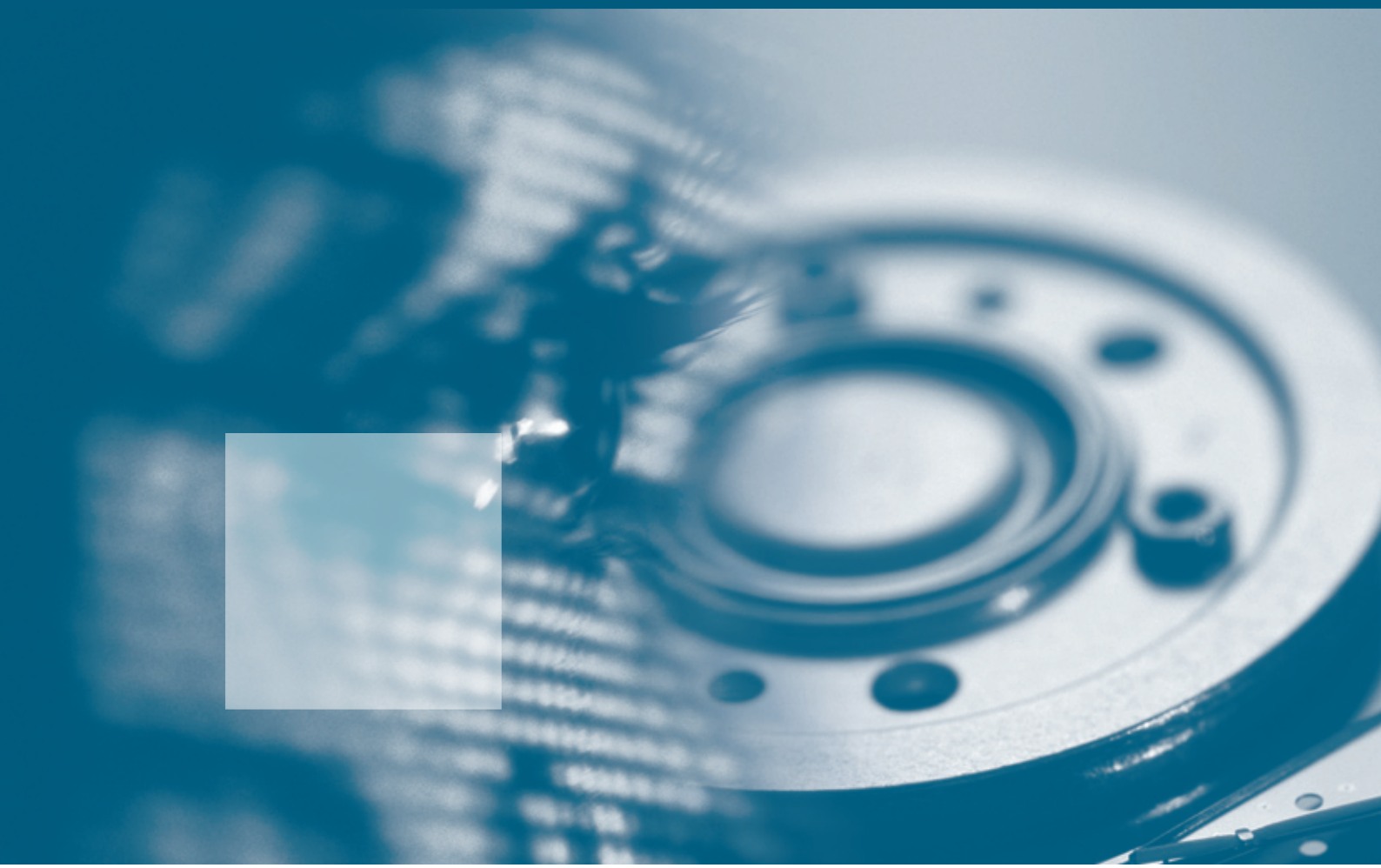

Verschlüsselung von Bestandsdaten aus Rechenzentrumssicht

BITKOM

Impressum

Herausgeber:	BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. Albrechtstraße 10 A 10117 Berlin-Mitte Tel.: 030.27576-0 Fax: 030.27576-400 bitkom@bitkom.org www.bitkom.org
Ansprechpartner:	Holger Skurk Tel.: 030.27576-250 h.skurk@bitkom.org
Verantwortliches BITKOM-Gremium:	AK Speichertechnologien
Stand::	April 2009
Gestaltung / Layout:	Design Bureau kokliko / Anna Müller-Rosenberger (BITKOM)
Copyright:	BITKOM 2009

Verschlüsselung von Bestandsdaten aus Rechenzentrumssicht

BITKOM

Inhaltsverzeichnis

1 Einleitung

Der sorgsame Umgang mit gespeicherten Daten gehört zu einer der wichtigsten Unternehmenspflichten. Dies gilt sowohl für der Schutz der eigenen Firmendaten gegen Angriffe von außen, als auch im Innenverhältnis, so dass nur autorisierte Mitarbeiter einen Zugriff auf bestimmte Daten haben. Insbesondere für personenbezogene Daten müssen hier ausreichende Schutzmaßnahmen getroffen werden.

Angriffspunkte ergeben sich sowohl wenn Daten elektronisch oder physikalisch übertragen werden, als auch wenn Daten gespeichert werden (nachfolgend als Bestandsdaten bezeichnet). Für den Schutz der Daten während der Übertragung gibt es schon seit längerer Zeit etablierte praxisgerechte Methoden. Exemplarisch sollen hier nur Virtual Private Networks (VPN) genannt werden.

Anders sieht es im Bereich der Bestandsdatenverschlüsselung aus. Neue Methoden haben sich hier erst in letzter Zeit etabliert und sind nun allgemein einsetzbar.

In der Presse gibt es zahlreiche Berichte über Schäden, die entstehen, wenn z.B. Sicherungsbänder verloren gehen und die Gefahr besteht, dass nicht autorisierte Personen auf diese Daten (insbesondere mit personenbezogenen Daten) zugreifen könnten. In den USA gibt es Gesetze, die genau vorschreiben, was unternommen werden muss, falls ein derartiger Fall eintritt. Unter anderem müssen potentiell Betroffene unterrichtet werden. Dies bedeutet zum einen direkte Kosten, zum anderen dürften aber die indirekten Kosten durch Image-Verluste etc. um ein Vielfaches höher sein.

Grundsätzlich mag die Gesetzeslage in den USA und in den Europäischen Ländern unterschiedlich sein. Im Kern ergeben sich aber auch in den Europäischen Ländern dieselben Grundanforderungen. Sie sind möglicherweise nicht in spezifischen Gesetzen formuliert, können aber relativ leicht aus übergeordneten Gesetzen abgeleitet werden.

Es ergeben sich Fragen wie: An welchen Orten soll eine Verschlüsselung von Bestandsdaten durchgeführt werden und wie sollen die notwendigen Schlüssel verwaltet werden? Im Gegensatz zur Verschlüsselung während der Übertragung, wo temporäre Schlüssel zum Einsatz kommen, müssen bei der Bestandsdatenverschlüsselung die Schlüssel über den gesamten Lebenszyklus der Daten hinweg sicher verwahrt werden.

Die heute verfügbare Technologie zur Verschlüsselung von Bestandsdaten kann an unterschiedlichen Orten in der Speicherinfrastruktur eingesetzt werden. Damit können angepasste Lösungen entsprechend der Risikoanalyse realisiert werden. In diesen Konzepten müssen auch die Wechselwirkungen zu anderen Storage-Anwendungen berücksichtigt werden.

Dieser Leitfaden wendet sich an Systemarchitekten und Entscheider, die sich einen generellen Überblick über das Thema Bestandsdatenverschlüsselung aus Rechenzentrumssicht verschaffen wollen.

2 Szenarien für den Einsatz von Verschlüsselung

Im nachfolgenden sollen wesentliche Szenarien beschrieben werden, die eine Verschlüsselung von Bestandsdaten fast zwingend erscheinen lassen bzw. demonstrieren, wo eine Verschlüsselung von Bestandsdaten höchst empfehlenswert ist. Es handelt sich hierbei nur um eine kleine Auswahl und keine vollständige Liste:

- Wenn Sicherungsmedien mit sensiblen Daten die gesicherte Umgebung eines Rechenzentrums verlassen.
- Wenn die ordnungsgemäße Entsorgung von nicht mehr benötigten Datenträgern gewährleistet werden muss.
- Wenn sicherstellt werden muss, dass alle replizierten Daten gelöscht werden.
- Wenn mandantenfähige Umgebungen benötigt werden

Tabelle: Szenarien, in denen Verschlüsselung von Bestandsdaten äußerst sinnvoll ist

2.1 Sicherungsmedien außerhalb der Rechenzentrumsumgebung

Jedes Rechenzentrum erstellt in regelmäßigen Abständen Sicherungsbestände auf transportablen Medien. Transportable Medien sind heute im Wesentlichen Magnetband-Kassetten, es kommt aber auch eine Vielzahl von anderen Medien in Betracht. Diese Datenträger werden sowohl für die operationale Datenwiederherstellung als auch für Desaster Recovery benötigt. Operationale Datenwiederherstellung bedeutet, dass bei Ausfall von einzelnen lokalen Komponenten die Daten aus lokalen Sicherungsbeständen wieder hergestellt werden. Desaster Recovery hingegeben bedeutet, dass weder die lokalen Originaldaten noch die lokalen Sicherungsdaten zur Verfügung stehen. Solche Datenverluste können insbesondere bei Elementarschäden, wie Überflutung, Brand, Erbeben etc., eintreten. Um sich gegen diese Fälle abzusichern, werden Sicherungsmedien in entfernte Standorte ausgelagert. Die Sicherungsmedien verlassen somit die besonders abgesicherten Rechenzentrumsumgebungen. Das Risiko eines Verlustes oder Diebstahls erhöht sich erheblich. Falls sensible Daten in unverschlüsselter Form auf den Sicherungsmedien stehen, ist es für unautorisierte Personen relativ leicht, die Daten zu lesen und die Daten für kriminelle Zwecke zu nutzen.

2.2 Ordnungsgemäße Entsorgung von Datenträgern

Am Ende ihres Lebenszyklus müssen Datenträger entsorgt werden. Datenträger enthalten aber in der Regel sensible Daten. Ein einfaches Löschen der Daten, bevor der Datenträger entsorgt wird, reicht bei weitem nicht aus, um sicherzustellen, dass nicht autorisierte Personen auf die sensiblen Daten zugreifen können. Aus diesem Grund haben sich unterschiedliche Prozesse herauskristallisiert, wie Datenträger zu behandeln sind, bevor die Restmaterialien entsorgt bzw. wiederverwertet werden können. Der Bereich reicht vom mehrfachen Überschreiben mit unterschiedlichen Bit-Mustern bzw. von der Behandlung mit starken Magnetfeldern bis zum völligen physikalischen Zerstören der Datenträger.[1] Gemeinsam ist diesen Verfahren, dass die Prozesse sich in der Regel über die gesicherten Rechenzentrumsgrenzen hinaus erstrecken und zusätzliche Instanzen / Personen eingeschaltet werden. Eine Abwicklung dieser konventionellen Methoden innerhalb des eigenen Rechenzentrums stößt schnell an Grenzen. Eine sichere Behandlung der Datenträger erfordert Spezialausrüstung, die sich einzelne Rechenzentren oft nicht leisten können. Gründe für den Einsatz von Spezialausrüstung liegen in den immer härter / resistenter werdenden Oberflächen der Datenträger und den verbesserten Methoden, aus Restdatenbeständen Originaldatenbestände wieder rekonstruieren zu können.

1 Siehe BITKOM Leitfaden „Sicheres Datenlöschen“, verfügbar unter http://www.bitkom.org/de/publikationen/38337_52528.aspx

Falls aber auf den Datenträgern die Daten in verschlüsselter Form abgelegt wurden und bei der Verschlüsselung starke Verschlüsselungen ordnungsgemäß angewendet wurden, ist ein Zugriff auf die Daten sinnlos, da eine Interpretation ohne Schlüssel nach heutigem Kenntnisstand nicht möglich sein sollte.

2.3 Gleichzeitiges Löschen aller replizierten Daten

Für operationale Wiederherstellung, Desaster Recovery, Testzwecke, statistische Auswertungen etc. werden Replikate angelegt. In den ersten beiden Fällen haben diese Daten eine definierte Lebenszeit. In den beiden anderen Fällen hängt die Lebenszeit der Daten von den sie nutzenden Anwendungen ab. Für jede Nutzungsart wird es unterschiedliche Lebenszeiten geben, und die Daten werden auf unterschiedlichen Datenträgern an unterschiedlichen Orten gespeichert. Insbesondere aus den Datenschutzgesetzen ergeben sich Anforderungen, dass zu bestimmten Ereignissen alle (und auch alle replizierten Daten) gelöscht werden müssen. In einer konventionellen Umgebung muss der Betreiber über alle Replikate Buch führen und dann alle Replikate mit der notwendigen Sorgfalt löschen. Dies gestaltet sich umso komplizierter, je mehr Replikate angefertigt wurden und je komplexer die Konfiguration ist.

Mit Hilfe der Verschlüsselung kann dieser Prozess wesentlich einfacher und sicherer abgewickelt werden. Wenn die Originaldaten und die Replikate mit ein und demselben Schlüssel verschlüsselt wurden, genügt es, den Schlüssel zu zerstören. Damit kann weder auf die Originaldaten noch auf die Replikate zugegriffen werden.

2.4 Mandantenfähige Umgebungen

Wenn ein Betreiber Rechenzentrumsleistung an andere Firmen verkauft oder vermietet, muss er sicherstellen, dass die Nutzer, die in der Regel unabhängige Firmen sind, nicht auf Daten der anderen Firmen zugreifen können. Dies kann heute mit Storage Virtualisierung, Partitioning, Zugriffssystemen etc. realisiert werden. Das Problem liegt aber in der Vielzahl von Punkten, wo die entsprechenden Zugriffsfunktionen aufgesetzt und permanent aktualisiert werden müssen. Dieses Problem kann auch mit Verschlüsselung gelöst werden. Wenn die Verschlüsselung bereits bei den Clients aufgesetzt wird, dann sind alle dazwischen liegenden Komponenten bis hin zur Datenablage automatisch auch mit abgesichert. Ein Beispiel wäre ein Backup-Service. Ein zentraler Dienstleister sichert von unterschiedlichen Firmen die Daten in ein zentrales Rechenzentrum. Da die Daten bereits an der Quelle (beim Kunden) verschlüsselt werden, bekommen weder der Dienstleister noch andere Firmen Einblick in die Daten.

3 Medien, auf denen Verschlüsselung einzusetzen ist

Daten können auf einer Vielzahl von unterschiedlichen Medien gespeichert werden. Für Backups haben sich im Enterprise-Bereich insbesondere Hochleistungsbandgeräte und seit einiger Zeit auch Virtuelle Tape-Libraries (VTL) durchgesetzt. Das Fassungsvermögen einzelner Cartridges reicht bis in den TeraByte-Bereich hinein. In kleinen Betrieben sind häufig optische Medien im Back-up-Bereich zu beobachten. Wechselplatten und Flash-basierte Medien erobern sich weitere Bereiche. Daneben gibt es auch noch weitere Technologien.

Wenn ein sicheres Löschen mit konventionellen Methoden durchgeführt werden soll, dann müssen unterschiedliche physikalische Eigenschaften betrachtet werden, um beurteilen zu können, welche Sicherheit eine bestimmte Methode erreichen kann. Dies ist komplex und oft nicht abschließend beantwortet. Verschlüsselung ist jedoch unabhängig von der physikalischen Aufzeichnungsart. Zur Beurteilung der Sicherheit gibt es relativ wenige Parameter, die zu betrachten sind.

4 Wo kann Bestandverschlüsselung angesetzt werden

Wie bereits oben beschrieben, kann die Verschlüsselung an unterschiedlichen Stellen innerhalb der Speicher-Infrastruktur aufgesetzt werden.

4.1 Verschlüsselung in den Anwendungen

Um eine durchgehende Sicherheit zu erreichen, muss eine Verschlüsselung in den Anwendungen realisiert werden. Damit ergibt sich eine sogenannte End-to-End Verschlüsselung. Nachteilig ist, dass diese Verschlüsselung erhebliche Ressourcen in den Anwendungsservern in Anspruch nimmt und in der Praxis jede Anwendung dazu tendiert, unterschiedliche Mittel und Methoden für die Verschlüsselung zu verwenden. Die Durchsetzung von unternehmensweiten Vorgaben wird erschwert. Das Risiko, dass einzelne Anwendungen nicht den Standards entsprechen und damit zum Sicherheitsrisiko werden, steigt. Darüber hinaus ist noch zu beachten, dass Verschlüsselungsmethoden nach bestimmten Zeitintervallen an neue Risikopotentiale angepasst werden müssen. Es kann durchaus sein, dass eine definierte Schlüssellänge neuen Analysemethoden nicht mehr standhält. Dies gilt prinzipiell auch für den Algorithmus selbst. Das heißt, nach einer bestimmten Zeit müssen Schlüssellängen und eventuell sogar die Verschlüsselungsmethode an neue Anforderungen angepasst werden. Falls diese Funktionen in einer Vielzahl von Anwendungen verteilt sind, ist dies mit einem entsprechend hohen Aufwand verbunden.

Es muss klar sein, dass obige Argumentation im Wesentlichen nur bei einer eher unkoordinierten und nicht sachgerecht angewendeten Verschlüsselung greift. Es wird viele Einsatzfälle geben, wo eine Verschlüsselung in einzelnen Anwendungen die richtige Lösung darstellt.

4.2 Backup-Software in den Anwendungsservern

Eine erste Zentralisierung ergibt sich, wenn die Verschlüsselungsfunktionen in der Backup-Software genutzt werden. Da die Verschlüsselung im Anwendungsserver abläuft, werden auch entsprechende Ressourcen in Anspruch genommen. Diese Ressourcen stehen dann den Anwendungen nicht mehr zur Verfügung. An dieser Stelle ist aber zu differenzieren, ob die Verschlüsselung auf jedem Client durchgeführt oder ob die Daten von den Client in unverschlüsselter Form von den Clients zu einem Storage- respektive Medien-Server übertragen werden und dann der Storage- respektive Medien-Server die Daten verschlüsselt und in verschlüsselter Form auf die Sicherungsmedien ausgibt.

4.3 Multipath Software

Einige Hersteller haben bereits angekündigt, dass Verschlüsselung in die jeweilige Multipath Software integriert wird. Multipath Software ist dort sinnvoll, wo ein Speichersystem über zwei oder über mehrere physikalische Pfade an den Server angeschlossen ist. Die Multipath Software ist in der Regel in der Treiber-Ebene angesiedelt und überwacht die Ein-/Ausgaben. Falls erkannt wird, dass Ein-/Ausgaben über einen Pfad nicht mehr abgewickelt werden können, schaltet die Multipath Sofware auf einen noch intakten Pfad um. MultiPath Software stellt neben dem Umschalten und Zurückschalten von Pfaden auch oft Funktionen für Load-Balancing bereit. Multipath Software arbeitet in der Regel nur mit dem block-orientierten Online-Storage (LUNs) zusammen. Der Ansatz hat den Vorteil, dass Verschlüsselung unabhängig

von der Plattentechnologie oder vom Alter der genutzten Plattenperipherie genutzt werden kann. Bezüglich der Ressourcenbelegung gelten dieselben Anmerkungen wie bei der Verschlüsselung in den Anwendungen oder in der Backup-Software.

4.4 Fibre Channel Switch

Etwas tiefer in der Storage-Infrastruktur in Richtung Speicher-Medien sind Fibre Channel Switches zu sehen. Verschlüsselung ist bereits in einigen Fibre Channel Switches verfügbar bzw. angekündigt. Die Verschlüsselung wird in der Regel in der Hardware der Switches durchgeführt. Andere Ressourcen in den Anwendungsservern werden nicht belastet. Aufgrund der Realisierung in der Hardware sollten sich keine wesentlichen Verzögerungen der Pakete bzw. eine Reduzierung des Durchsatzes ergeben.

4.5 Explizite Verschlüsselungsboxen / -appliances

Schon seit Längerem sind externe Verschlüsselungsboxen am Markt. Diese Lösungen arbeiten nach dem sogenannten In-line Verfahren. Das heißt, diese Boxen werden in den Fibre-Channel-Pfad / NAS geschaltet. Alle Daten durchlaufen diese Appliance und werden entsprechend den eingestellten Regeln verschlüsselt. Im Gegensatz zu den oben beschriebenen Lösungen ist hier das Thema Verfügbarkeit besonders zu beachten. Bei den oben beschriebenen Lösungen ist durch die normale Konfiguration bereits das Thema Verfügbarkeit definiert. Z.B. werden in Fibre-Channel Konfigurationen auch in Konfigurationen ohne Verschlüsselung in der Regel zwei Switches vorhanden sein, um im Fehlerfall alternative Pfade nutzen zu können. Dieser Grundsatz muss auch bei externen Verschlüsselungsboxen beachtet werden.

4.6 In Endgeräten - speziell in Bandgeräten

Als relativ neue Entwicklung ist die Hardware-Verschlüsselung in den Bandgeräten anzusehen. Damit ergeben sich keine nennenswerten negativen Auswirkungen auf den Durchsatz. Es ist offensichtlich, dass zur Verschlüsselung die Bandgeräte über einen Schlüssel verfügen müssen. Hierzu gibt es verschiedene Methoden. Eine Variante besteht darin, dass die Anwendung (normalerweise Backup-Anwendung) den Schlüssel innerhalb des Datenstroms mitliefert. In diesem Fall ist die Anwendung für das Schlüsselmanagement zuständig. Eine weitere Variante ist, dass das Bandgerät sich über eine gesicherte Kommunikationsverbindung direkt an ein eigenständiges Schlüsselmanagement wendet. Dabei sollten sich die Partner über digitale Zertifikate autorisieren.

4.7 In den Festplatten

Mit FDE (Full Disk Encryption) entwickelt sich ein Standard, der die Verschlüsselung wie bei Bandgeräten in der Geräteelektronik vorsieht. Eine Herausforderung ergibt sich in der Integration in die Controller-Umgebung, da FDE-Platten - unter anderem im Rahmen von MultiPath-Funktionen - problemlos zugreifbar sein müssen. Auch muss es möglich sein, Platten von einem Controller auf einen anderen Controller zu verlagern.

5 Schlüssel Management

5.1 Verschlüsselungsvorgang

Wie oben bereits angemerkt, ist die Basis für die sichere Ablage von Daten die Verschlüsselung. Dabei spielen der Algorithmus selbst und die Schlüssellänge eine wesentliche Rolle. Beispielsweise wird der AES Algorithmus (Advanced Encryption Standard) mit einer Schlüssellänge von 256 Bits heute nach herrschender Meinung als sicher eingeordnet. Daraus darf aber nicht geschlossen werden, dass andere Algorithmen als unsicher einzustufen wären. Mit Fortschritt der Technik kann sich eine Einschätzung, was als sicher anzusehen ist, durchaus ändern. Nach Ablauf einer bestimmten Zeit ist es wahrscheinlich, dass größere Schlüssellängen oder sogar andere Algorithmen erforderlich werden, um z.B. den gestiegenen Möglichkeiten einer „Brute Force Attack“ standzuhalten. Mit „Brute Force Attack“ ist gemeint, dass jede Schlüsselkombination systematisch auf das verschlüsselte Material angewandt und geprüft wird, ob sich die Daten damit entschlüsseln lassen. In Abhängigkeit der Schlüssellänge, des verwendeten Algorithmus und der Anzahl der Versuche, die innerhalb einer bestimmten Zeiteinheit durchgeführt werden können, lässt sich die durchschnittlich erforderliche Zeit errechnen, um den passenden Schlüssel zu finden. Darüber hinaus gibt es noch weitere Parameter, die in diese Gleichung eingehen. Z.B. spielt die Schlüsselqualität eine wesentliche Rolle. Schlüssel, die auf leicht erratbaren Grundmustern bestehen (z.B. Namen, Geburtsdaten etc.) sind wesentlich schwächer einzustufen als Schlüssel, die mit einem Zufallszahlengenerator erzeugt wurden. Die Generierung von Schlüsseln ist bereits eine Aufgabe des Schlüsselmanagements, was nachfolgend diskutiert werden soll.

5.2 Anforderungen an ein Verschlüsselungssystem

5.2.1 Zuweisung von Schlüsseln

Für die Verschlüsselung muss der Administrator dem Datenstrom einen Schlüssel zuweisen, der dann im Verschlüsselungsalgorithmus verwendet wird. Datenstrom wird hier als abstrakter Begriff verwendet. In der Praxis ist es nicht unüblich, dass z.B. eine Library oder eine Gruppe von Bandgeräten mit ein und demselben Schlüssel arbeiten. In der Regel besteht aber auch die Möglichkeit, feingranular, z.B. für jede LUN / WWN oder für jedes Volumen, einen eigenen Schlüssel zu vergeben. Grundsätzlich sollten die Schlüssel automatisch generiert werden. Nur eine automatische Generierung, basierend auf einem zuverlässigen Zufallsgenerator, garantiert sichere Schlüssel.

Zur leichteren Handhabung und zur Abbildung komplexerer Zusammenhänge werden diese Daten oft in einem logischen Konstrukt zusammengefasst (Zuordnung der Schlüssel zu den Datenströmen). Darüber hinaus werden in Sicherheitsregeln oder (Policies) festgelegt, was verschlüsselt werden soll. Datenströme, die nicht von einer Sicherheitsregel oder von einem Crypto-Container betroffen sind, werden im Klartext durchgereicht.

Als Implementierungsvariante ist zu sehen, ob eine bestimmte Menge von Schlüsseln im Voraus oder ob die Schlüssel einzeln bei Bedarf generiert werden.

Um ein WWN-Spoofing wirksam zu unterbinden, sollte ergänzende Authentisierungssoftware bereitstehen. Dazu wird ein Client auf den Backup-Host geladen. Die Authentisierung erfolgt dann zusätzlich zu den Standard Fibre-Channel Funktionen, wie zum Beispiel über die Abprüfung der WWN oder der Port-Zuweisung.

5.2.2 Speicherung der Schlüssel

Die Schlüssel werden standardmäßig in einer Konfigurationsdatei in verschlüsselter Form gespeichert. Damit können sie auf einfache Weise mit Standardmethoden gesichert werden. Dies eröffnet auch die Exportierbarkeit der Konfigurationsdatei und der verschlüsselten Schlüssel in ein anderes Verschlüsselungssystem. Die aktive Nutzung der Schlüssel ist jedoch nur dann möglich, wenn im neuen System der zugehörige Master-Schlüssel zur Verfügung steht.

Einzelne Schlüssel werden systemseitig nicht automatisch gelöscht, da sie während der gesamten Lebenszeit der Sicherungsmedien vorhanden sein müssen. Eine Bereinigung von alten Schlüsseln sollte nur über externen Anstoß erfolgen.

Zusätzlich kann der Schlüssel auch auf dem eigentlichen Sicherungsmedium in verschlüsselter Form gespeichert werden. Auf diese Schlüssel muss nur zugegriffen werden, falls die Konfigurationsdatei nicht mehr verfügbar ist.

5.2.3 Schlüsselwiederherstellung für Desaster Recovery Szenarien

Im Bereich der Möglichkeiten zur Schlüsselwiederherstellung gibt es kontroverse Diskussionen. Auf der einen Seite wird argumentiert, dass eine ordnungsgemäße Sicherung der verschlüsselten Schlüssel ausreichen sein sollte, um auch alle Anforderungen an ein Desaster Recovery Management erfüllen zu können. Auf der anderen Seite gibt es am Markt Konzepte, die auf einem Master-Schlüssel und zusätzlich explizit generierten Wiederherstellungs-Schlüsseln basieren. Da im ersten Fall die normalen konventionellen Methoden greifen, soll im Nachfolgenden etwas tiefer auf das zweite Konzept eingegangen werden.

Der Master-Schlüssel, mit denen die eigentlichen Schlüssel verschlüsselt werden, ist gerade bei der verschlüsselten Ablage von Daten auf den Medien der zentrale Punkt. Ohne den Master-Schlüssel können die Daten nicht mehr entschlüsselt werden (da die eigentlichen Schlüssel auch verschlüsselt sind). Die Schlüssel müssen auch noch nach sehr langen Zeiträumen zur Verfügung stehen. Dazu muss der Zugang zum Verschlüsselungssystem immer gewährleistet sein. Wenn aufgrund eines fehlenden Schlüssels Daten aus Sicherungsbeständen nicht mehr rekonstruiert werden könnten, würde dies vermutlich schnell das Aus für eine Firma bedeuten. Es gibt zwei grundsätzliche Szenarien, bei denen der Master-Schlüssel nicht mehr verfügbar ist. Zum einen kann, aus welchen Gründen auch immer, der Master-Schlüssel verloren gehen. Dies kann jedoch bei genügender Sorgfalt ausgeschlossen werden. Zum anderen muss ein Master-Schlüssel regeneriert werden, wenn z.B. die Verschlüsselungshardware ausgetauscht wird. Dieser Fall ist konzeptionell insbesondere in Disaster-Recovery Szenarien vorzusehen. In einem derartigen Szenario geht man davon aus, dass am betroffenen Standort alle Geräte nicht mehr verfügbar sind und dass am Ausweichstandort mit anderen Geräten weitergearbeitet werden muss. Unter der Voraussetzung, dass über Replikation die verschlüsselten Daten bereits an den Ausweichstandort übertragen wurden, muss zusätzlich die Verschlüsselungsinfrastruktur aktualisiert werden. Dies erfolgt, wie bei einem verlorenem Master-Schlüssel, über eine Schlüsselwiederherstellungsfunktion. Dabei hat die so genannte Recovery-Officer-Group die zentrale Rolle. Die Gruppe ist eine vertrauenswürdige Personengruppe, von denen jeder einen persönlichen Wiederherstellungsschlüssel (bzw. Smart Card) besitzt. Dabei reicht ein einzelner Wiederherstellungsschlüssel nicht aus, um einen Master-Schlüssel wiederherzustellen. Es müssen im Minimum zwei Wiederherstellungsschlüssel zusammenarbeiten, damit der Master Schlüssel rekonstruiert werden kann. Die Anzahl der notwendigen

Wiederherstellungsschlüssel wird bei der Installation des Verschlüsselungssystems entsprechend den Sicherheitsanforderungen festgelegt. Diese Anzahl dient dann als Quorum, welches mindest erfüllt sein muss. Es ist selbstverständlich, dass die Wiederherstellungs-Schlüssel (z.B. Smart Cards) in besonders gesicherten Umgebungen aufzubewahren sind, so dass auf diese Schlüssel auch im Falle eines katastrophalen Ereignisses (Überflutung, Erdbeben, Brand etc.) noch zugegriffen werden kann.

Weitergehende Überlegungen sind erforderlich, wenn man sich auch auf Szenarien vorbereitet, wo kein Verschlüsselungssystem mehr vorhanden ist respektive beschafft werden kann. Es muss dann entweder der Master-Schlüssel oder die einzelnen Verschlüsselungsschlüssel aus dem System in einer abgesicherten Weise exportiert werden, so dass sie als Entschlüsselungsschlüssel genutzt werden können. Das Prinzip beruht wiederum auf der Schlüssel-Wiederherstellung mittels eines Quorums von Wiederherstellungsschlüsseln, jedoch nicht innerhalb des Verschlüsselungssystems, sondern außerhalb. Es ist offensichtlich, dass dies auf der einen Seite manche Bedenken ausräumen kann, falls die Daten auch ohne Verschlüsselungssystem wiederhergestellt werden müssen. Auf der anderen Seite werden aber Angriffspunkte geschaffen, da elementare Entschlüsselungsinformationen außerhalb des Verschlüsselungssystems gespeichert werden. Falls dieser Prozess nicht mit äußerster Sorgfalt durchgeführt wird, entstehen erhebliche Risiken.

5.2.4 Sicherheitsdomänen

Hilfreich ist, wenn unterschiedliche Sicherheitsdomänen definiert werden können. Eine Sicherheitsdomäne besteht dabei aus einer oder mehreren Verschlüsselungssystemen. Für jede Sicherheitsdomäne müssen die Schlüsselmaterialen so abgeschottet sein, dass ein Administrator nur seine Domäne beeinflussen kann. Dies gilt auch für die oben beschriebenen Schlüsselwiederherstellungsfunktionen.

Sicherheitsdomänen sind z.B. erforderlich, falls mandantenfähige Umgebungen aufgesetzt werden müssen.

5.2.5 Regel-basierte Arbeitsweise

Über Regeln wird definiert, welche Bereiche verschlüsselt werden sollen. Die Definition muss so erfolgen, dass der Systemadministrator die Anforderung auf einfache Weise umsetzen kann. Die Bildung von Gruppen und Anwendung von gemeinsamen Funktionen auf die Gruppen erleichtert die Arbeitsweise erheblich. Klare Strukturen in der Administration sind die Voraussetzung zur lückenlosen Umsetzung von Sicherheitsvorgaben.

5.2.6 Sichere Kommunikation und Hardened OS

Es ist eine Selbstverständlichkeit, dass die Kanäle zur Administration des Verschlüsselungssystems über sichere Verbindungen aufgebaut werden. Geeignete Mittel sind z.B. Secure Sockets Layer (SSL) oder Secure Shell (SSH). Über das SSL Interface wird dann z.B. das Web GUI über das sichere HTTPS gefahren. Die Authentisierung sollte neben dem Userid / Passwort-Mechanismus optional auch eine Authentisierung über Smart Cards ermöglichen. Eine Absicherung über ein Public-Key Verfahren inklusive eines digitalen Zertifikates ist eine weitere Option. Damit wird sichergestellt, dass Meldungen zwischen dem Client und der Management-Console den Anforderungen an die Referenzarchitektur entsprechen.

5.2.7 Andere Administrationsprotokolle, wie z.B. SNMP, sollten nur Lesezugriff ermöglichen.

Grundsätzlich muss das Verschlüsselungssystem selbst den Anforderungen eines besonders abgeschotteten Systems entsprechen. Unter anderem dürfen keine nicht benötigten Services laufen, alle nicht benötigten Ports müssen gesperrt sein, etc. Die Eigenschaften können

unter den Begriff „Hardened OS“ zusammengefasst werden.

5.2.8 Verfügbarkeit via Cluster

In Enterprise-Umgebungen werden in der Regel höchste Anforderungen an die Verfügbarkeit gestellt. Daraus leitet sich fast zwingend eine Cluster-Konfiguration ab. Innerhalb des Clusters erfolgt dann ein automatisches Failover, falls ein Verschlüsselungssystem nicht mehr zur Verfügung stehen sollte. Der Failover innerhalb einer Cluster-Konfiguration muss transparent erfolgen. Die Teilnehmer in der Cluster-Konfiguration müssen die Konfigurationsdaten permanent über einen sicheren Kanal aktualisieren.

Abhängig von den Sicherheitsanforderungen, kann eine Cluster-Konfiguration aus zwei oder auch aus mehreren Knoten bestehen. Idealerweise sollte kein fixer Master im Cluster bestehen. Die Zuweisung der Master-Rolle sollte entsprechend der jeweiligen Aufgabe bzw. der Knoten-Verfügbarkeit dynamisch erfolgen.

5.2.9 Rollen-basierte Administration

Für die Administration muss die Definition von Rollen-basierten Administratoren möglich sein. Im Minimum muss zwischen einem Administrator mit Superrechten, dem Schlüsselwiederherstellungsbereich und normalen Usern unterschieden werden können. Ideal ist, wenn der Administrator mit Superrechten nur Aufgaben auf andere Administratoren delegieren kann. Die anderen Administratoren werden dann genau mit den Rechten ausgestattet, die sie für ihre Arbeit benötigen.

5.2.9 Sicheres Logging und Monitoring

Jedes Verschlüsselungssystem muss ein sicheres Logging realisieren. Die Log-Informationen sollten dabei zusätzlich an einen entfernten Log-Server im Netzwerk geschickt werden können. Um die Netzbelastung gering zu halten, sollte eine Auswahl der zu verschickenden Log-Informationen möglich sein. Damit die Vollständigkeit und Unverfälschtheit der Logs überprüft werden kann, sollten die Log-Informationen signierbar sein. So lässt sich u.a. feststellen, dass die Log-Meldungen authentisch sind, dass die Quelle und die Zeitstempel korrekt sind und dass keine Meldungen im Log-Datenstrom fehlen.
Neben den Logs zu bestimmten Ereignissen sollten auch Informationen zum Durchsatz erfasst werden. Die Log-Informationen sollten gleichzeitig an mehrere entfernte Stellen übertragbar sein.

In diesen Bereich fällt auch das Erzeugen von Meldungen über Standardschnittstellen, wie z.B. SNMP oder E-Mail.

Zur Überprüfung der Performance sollten umfangreiche Statistiken erfasst und in graphischer Aufbereitung bereitgestellt werden.

5.2.10 Schutz vor mechanischen Eingriffen

Zur Erfüllung höchster Sicherheitsanforderungen muss das Verschlüsselungssystem erkennen, wenn mechanische Eingriffe erfolgen. In derartigen Fällen muss sich das Verschlüsselungssystem selbst sperren. Ein darüber hinaus gehender Schutz ist, dass sofort alle Schlüssel (Master-Schlüssel und Verschlüsselungs-Schlüssel) zerstört werden.

Beispielsweise könnte ein Angreifer versuchen, die speziell gesicherte Hardware mit der Verschlüsselungskernkomponente, die zwangsweise den Verschlüsselungsschlüssel temporär im Klartext halten muss, zu entfernen. Der Angreifer würde dann mit externen Analysemethoden versuchen, diesen Verschlüsselungs-Schlüssel auszulesen. Durch das Erkennen von mechanischen Eingriffen und der darauf folgenden Zerstörung des Schlüsselmaterials führt dies nicht zum Erfolg.

5.2.11 Zurücksetzen in den Urzustand

Falls das Verschlüsselungssystem in anderen Umgebungen genutzt werden soll, muss eine Funktion

bereitgestellt werden, die alle Informationen auf dem System so löscht, dass aus der alten Umgebung keine Informationen rekonstruiert werden können. Das Verschlüsselungssystem muss in den Urzustand zurücksetzbar sein.

5.2.12 Sonstige Anforderungen

Verschlüsselung ist eine wirksame Methode, um nicht autorisierten Zugriff zu unterbinden. Es gibt aber Szenarien, bei denen nicht zwingend eine Verschlüsselung erforderlich ist, aber überprüft werden soll, ob der einmal gespeicherte Inhalt beim Einlesen dem entspricht, wie er auf das Band geschrieben wurde. Digitale Signaturen sind die Basis für derartige Überprüfungen.

Digitale Signaturen stellen ein Siegel für eine Nachricht bereit. Durch die Bildung eines Hash-Wertes kann überprüft werden, ob der Inhalt der Nachricht identisch mit der ist, die mit dem privaten Schlüssel unterschrieben wurde. Wie eine handschriftliche Unterschrift wird die digitale Signatur an die Nachricht angehängt und damit der Sender identifiziert. Hier stellt sich die Frage, wie überprüft werden kann, ob die Nachricht vom eigentlichen Sender oder von jemand anderem kommt, der den privaten Schlüssel benutzt, um eine nicht autorisierte Nachricht zu unterschreiben. Die Lösung liegt in der Nutzung von Zertifikaten, die von einer „Certificate Authority“ ausgegeben wurden. Damit kann die Identität des Senders durch den Empfänger verifiziert werden.

Dazu wird der Private-Key[2] des Zertifikats im Hash-Algorithmus genutzt, welcher die digitale Signatur erstellt. Der Sender erstellt einen Hash-Wert der Meldung. Dieser Hash-Wert wird mit dem Private Key des Zertifikats verschlüsselt, so dass eine Signatur erzeugt werden kann, die dann an die Meldung angehängt werden kann. Die Meldung kann dann versendet werden und der Sender erstellt von der empfangenen Meldung auch einen Hash-Wert. Die Signatur wird mit dem Public Key des Zertifikates entschlüsselt und die beiden Hash-Werte werden verglichen. Wenn die beiden Hash-Werte übereinstimmen, dann ist die Meldung verifiziert.

Zertifikate haben nur eine begrenzte Gültigkeitsdauer. Aus diesem Grund muss ein System die Möglichkeit zur Nach-Signierung von bereits bestehenden Signaturen bieten.

2 Private Key und Public Key werden in einem vorgelagerten Verfahren erstellt. Private Key und Public Key sind so aufeinander abgestimmt, dass eine sichere Verschlüsselung und Entschlüsselung möglich ist.

6 Zertifizierungen

Im vorherigen Kapitel wurden einige wichtige Anforderungen an ein Verschlüsselungssystem gestellt. Dies ist aber nur ein Ausschnitt der Anforderungen, falls ein Schlüsselsystem den höchsten Ansprüchen genügen soll. Verschiedene Organisationen sind auf dem Gebiet der Standardisierung dieser Anforderungen tätig. Exemplarisch kann hierfür „Federal Information Processing Standards (FIPS)“ genannt werden, welche mit FIPS 140.2 eine breit beachtete Standardisierung veröffentlicht hat.

Security Requirements for Cryptographic Modules -- 01 May 25 (Supersedes FIPS PUB 140-1, 1994 January 11)

This Federal Information Processing Standard (140-2) was recently approved by the Secretary of Commerce. It specifies the security requirements that will be satisfied by a cryptographic module, providing four increasing, qualitative levels intended to cover a wide range of potential applications and environments. The areas covered, related to the secure design and implementation of a cryptographic module, include specification; ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

Federal Information Processing Standard 140-2

7 Zu beachtende Randbedingungen

7.1 Granularität der Verschlüsselung

In der praktischen Anwendung stellt sich die Frage, was zwingend verschlüsselt werden muss, was verschlüsselt werden soll und wo es keine Notwendigkeit gibt, die Daten zu verschlüsseln. Verschlüsselung erfordert nicht unerhebliche Aufwände. Es müssen Investitionen in Hard- und Software getätigt werden, um ausreichend Ressourcen für die Verschlüsselung bereitstellen zu können. Die Umsetzung muss in einer exakten Planung erfolgen und eine permanente Anpassung an neue Gegebenheiten. Aus diesen Gründen ist es erforderlich, dass es die Technik erlaubt, nur bestimmte Datenströme zu verschlüsseln. Im Storage-Umfeld wird man dies an den standardmäßig adressierbaren Einheiten abbilden. Dies sind u.A.:

- Gesamte Partitionen in Bandbibliotheken
- Einzelne Geräte oder Gerätegruppen (Bandgeräte, Hard-Disks)
- Einzelne LUNs
- Einzelne Cartridges / Volumes
- Einzelne Save-Sets
- Datenströme von bestimmten Applikationen

Obige Liste zeigt nur Beispiele von Granularitäten auf. In den einzelnen Lösungen kann sich dies durchaus differenzierter darstellen.

7.2 Wechselwirkungen mit anderen Storage Anwendungen

Im Kapitel 44 wurde bereits beschrieben, an welchen Stellen Bestandsverschlüsselung heute realistischerweise eingesetzt werden kann. Dabei ist allerdings zu beachten, dass es Standard-Storage Anwendungen gibt, die ebenfalls an zentralen Stellen gewisse Dienste erbringen. Der Wirkerfolg der Standard-Storage Anwendungen hängt aber stark davon ab, in welcher Form die Daten vorliegen. Nachfolgend einige Beispiele.

Eine Komprimierung von verschlüsselten Daten wird keinen Erfolg haben. Verschlüsselte Datenströme werden keine regelmäßigen Datenstrukturen mehr aufweisen. Prinzipiell kann es sogar passieren, dass sich der Datenstrom verlängert, da Komprimierung immer einen gewissen Sockel an zusätzlichen Metadaten erzeugen muss. Das heißt, eine Komprimierung ist nur dann sinnvoll, wenn sie vor der Datenverschlüsselung durchgeführt wird. Damit bekommen die Reihenfolge und die Orte, wie und wo Komprimierung und Verschlüsselung durchgeführt werden, eine Schlüsselrolle.

Die gleiche Problematik ergibt sich mit Data De-Duplication. Data De-Duplication ist eine Technologie, um redundante Daten zu eliminieren. Am einfachsten kann die Technologie an Backup-Strömen erklärt werden. Nehmen wir an, dass zwei Full-Backups (Sicherung aller Dateien) hintereinander in den Data De-Duplication Prozess gegeben werden. Der Data De-Duplication-Prozess identifiziert sowohl innerhalb des ersten Full-Backup als auch zwischen den beiden Full-Backups Informationseinheiten, die mehrfach vorhanden sind. Falls eine Informationseinheit bereits einmal abgespeichert worden ist, wird diese Informationseinheit nicht nochmals gespeichert, sondern nur ein Zeiger auf die bereits abgespeicherte Informationseinheit erzeugt. Informationseinheiten haben dabei nicht das Granulat einer Datei, sondern brechen auch Dateien in geeignete Teile auf. State-of-the Art De-Duplication Lösungen arbeiten dabei mit variablen Längen. Damit braucht zum Beispiel bei einer größeren PowerPoint Datei, die an einen Kollegen gesendet wurde, der nur eine einzige Seite verändert hat, nur ein sehr geringer Prozentsatz neu abgespeichert zu werden. Falls die Verschlüsselung dieser beiden Dateien vor dem Data De-Duplication Prozess erfolgte, wird Data De-Duplication nicht mehr die inhaltliche Gleichheit der Informationseinheiten feststellen können.

Ein Virus-Schutzprogramm wird ähnliche Probleme haben, falls die Verschlüsselung vor dem Speichersystem durchgeführt wird und das eigentliche Virus-

Schutzprogramm direkt auf dem Speichersystem abläuft. Per Definition kann in diesem Fall das Virusschutzprogramm die Muster nicht mehr erkennen. In Folge müsste die Virus-Prüfung so platziert werden, dass die gelesenen Daten erst wieder entschlüsselt werden. Unter Umständen belastet dies die Storage-Infrastruktur erheblich.

Analog zu Virus-Schutzprogrammen sind Lösungen für Deep Data Classification zu sehen. Diese Lösungen scannen einen gesamten Bestand, z.B. in NAS-Systemen oder File Servern, auf bestimmte Inhalte in Dateien. Dazu muss die gesamte Datei durchgelesen werden. Falls die Deep Data Classification nach der Verschlüsselung aufgesetzt wird, kann sie keine Inhalte mehr erkennen.

8 Schlussbetrachtung

Die Betrachtung der in diesem Leitfaden dargestellten Szenarien zeigt, dass Verschlüsselung in bestimmten Bereichen fast als zwingend anzusehen ist. Das heißt, jeder Betreiber eines Rechenzentrums muss sich damit auseinander setzen und entsprechend der Bedrohungslage an geeigneter Stelle diese Möglichkeit nutzen. In der rein technischen Verschlüsselung haben sich heute allgemein akzeptierte Algorithmen durchgesetzt. Darüber hinaus muss aber gerade bei der Verschlüsselung von Bestandsdaten größtes Augenmerk auf das Schlüsselmanagement gelegt werden. Ein nicht mehr verfügbarer Schlüssel für verschlüsselte Bestandsdaten kann das Aus einer Firma bedeuten.

Zur Lösung dieser Aufgabe stehen heute leistungsfähige Schlüssel-Management Systeme zur Verfügung. Leider gibt es noch kein Schlüssel-Management System, welches sich industrieweit durchgesetzt hat. Es ist nicht ausgeschlossen, dass in einem Rechenzentrum möglicherweise zwei oder mehrere Schlüssel-Management Systeme parallel betrieben werden müssen. Weitere architekturbezogene Überlegungen sind erforderlich, um die richtigen Orte respektive die richtigen Reihenfolgen von Verschlüsselung und Standard-Storage Anwendungen zu etablieren, insbesondere, da einige Standard-Storage Anwendungen mit verschlüsselten Daten nicht mehr effizient arbeiten können.

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.200 Unternehmen, davon 900 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für bessere ordnungspolitische Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org