Bundesamt
für Sicherheit in der
Informationstechnik

DER.3.1 Audits und Revisionen

1. Beschreibung

1.1. Einleitung

Audits und Revisionen sind grundlegend für jedes erfolgreiche Managementsystem für Informationssicherheit (ISMS). Nur wenn etablierte Sicherheitsmaßnahmen und -prozesse regelmäßig daraufhin überprüft werden, ob sie noch wirksam, vollständig, angemessen und aktuell sind, lässt sich der Gesamtzustand der Informationssicherheit beurteilen. Audits und Revisionen sind somit ein Werkzeug, um ein angemessenes Sicherheitsniveau festzustellen, zu erreichen und aufrechtzuerhalten. Durch Audits und Revisionen ist es möglich, Sicherheitsmängel und Fehlentwicklungen zu erkennen und entsprechende Gegenmaßnahmen zu ergreifen.

Als Audit (audire = hören, zuhören) wird eine systematische, unabhängige Prüfung von Aktivitäten und deren Ergebnissen bezeichnet. Dabei wird geprüft, ob definierte Anforderungen wie Normen, Standards oder Richtlinien eingehalten werden. In einer Revision (revidieren = kontrollieren, prüfen) wird untersucht, ob Dokumente, Zustände, Gegenstände oder Vorgehensweisen korrekt, wirksam und angemessen sind. Im Gegensatz zum Audit muss die Revision nicht unbedingt unabhängig erfolgen. Zudem kann die Revision im Sinne einer Wartung auch bereits die Nachbesserung umfassen.

1.2. Zielsetzung

Der Baustein DER.3.1 *Audits und Revisionen* definiert Anforderungen an Audits und Revisionen mit dem Ziel, die Informationssicherheit in einer Institution zu verbessern, Fehlentwicklungen auf diesem Gebiet zu vermeiden und Sicherheitsmaßnahmen und -prozesse zu optimieren.

1.3. Abgrenzung und Modellierung

Der Baustein ist auf den gesamten Informationsverbund anzuwenden. Das betrifft interne Audits (Erstparteien-Audits) und Revisionen sowie Audits bei Dienstleistenden der Institution (Zweitparteien-Audits) oder anderen Institutionen, mit denen die Institution eine Partnerschaft eingegangen ist. Zertifizierungsaudits (Drittparteien-Audits) werden in diesem Baustein nicht berücksichtigt.

Ebenso wird die für Bundesbehörden verpflichtende IS-Revision nicht betrachtet. Diese wird im Baustein DER 3.2 *Revisionen auf Basis des Leitfadens IS-Revision* behandelt.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein DER.3.1 *Audits und Revisionen* von besonderer Bedeutung.

2.1. Unzureichende oder nicht planmäßige Umsetzung von Sicherheitsmaßnahmen

Das Schutzniveau einer Institution hängt davon ab, dass Sicherheitsmaßnahmen vollständig und korrekt umgesetzt werden. Insbesondere in der kritischen Phase von Projekten oder unter bestimmten Rahmenbedingungen kann es aber vorkommen, dass Sicherheitsmaßnahmen temporär ausgesetzt werden. Wird dann vergessen, sie wieder zu reaktivieren, kann ein zu niedriges Sicherheitsniveau entstehen.

2.2. Wirkungslose oder nicht wirtschaftliche Umsetzung von Sicherheitsmaßnahmen

Werden Sicherheitsmaßnahmen umgesetzt, ohne dabei bestimmte Aspekte aus der Praxis zu berücksichtigen, sind die Maßnahmen eventuell wirkungslos. Beispielsweise ist es sinnlos, den Eingangsbereich mit Drehkreuzen abzusperren, wenn Mitarbeitende das Gebäude einfach durch einen offenen Seiteneingang betreten können.

Ebenso können Einzelmaßnahmen ergriffen werden, die wirtschaftlich nicht sinnvoll sind. So ist für den Schutz von Informationen mit einer normalen Vertraulichkeit ein sauber implementiertes Rechte- und Rollenkonzept besser geeignet und wirtschaftlicher als eine komplexe, zertifikatsbasierte Verschlüsselung des Fileservers.

2.3. Unzureichende Umsetzung des ISMS

In vielen Institutionen überprüft der oder die Informationssicherheitsbeauftragte selbst, ob Sicherheitsmaßnahmen umgesetzt wurden. Oft wird darüber aber die Prüfung des eigentlichen ISMS vergessen, insbesondere da dies durch unabhängige Dritte erfolgen sollte. Dadurch könnten die Prozesse eines ISMS ineffizient oder nicht angemessen umgesetzt sein. In der Folge kann das Sicherheitsniveau der Institution beeinträchtigt werden.

2.4. Unzureichende Qualifikation der Prüfenden

Sind die Personen, die ein Audit oder eine Revision durchführen sollen, nicht ausreichend qualifiziert oder bereiten sich ungenügend auf die Prüfungen vor, schätzen sie den Sicherheitszustand einer Institution möglicherweise falsch ein. Dies könnte zu fehlenden oder sogar falschen Korrekturmaßnahmen im Prüfbericht führen. Im schlimmsten Fall hat dies dann eine zu hohe und damit nicht wirtschaftliche bzw. eine zu niedrige und damit sehr risikobehaftete Absicherung der Informationen zur Folge.

2.5. Fehlende langfristige Planung

Werden Audits und Revisionen nicht langfristig und zentral geplant, kann es passieren, dass einzelne Bereiche sehr häufig und andere überhaupt nicht geprüft werden. Dadurch ist es nur sehr schwer oder gar nicht möglich, den Sicherheitszustand des Informationsverbunds einzuschätzen.

2.6. Fehlende Planung und Abstimmung bei der Durchführung eines Audits

Wenn ein Audit mangelhaft geplant und nicht ausreichend mit der Institution abgestimmt wurde, sind während der Vor-Ort-Prüfung eventuell nicht alle benötigten Personen anwesend. Dadurch lassen sich dann möglicherweise einzelne Bereiche überhaupt nicht auditieren. Auch wenn die Termine für die einzelnen Bereiche zu eng gesetzt wurden, könnte die Untersuchung nur oberflächlich durchgeführt werden, weil zu wenig Zeit eingeplant wurde.

2.7. Fehlende Abstimmung mit der Personalvertretung

In Audits und Revisionen können auch Aspekte geprüft werden, aus denen sich Rückschlüsse auf die Leistung von Mitarbeitenden ziehen lassen. Somit könnten diese Prüfungen als Leistungsbeurteilung gewertet werden. Wird die Personalvertretung nicht beteiligt, kann dies zu Verstößen gegen das geltende Mitbestimmungsrecht führen.

2.8. Absichtliches Verschweigen von Abweichungen

Mitarbeitende könnten befürchten, dass bei der Prüfung ihre Fehler aufgedeckt werden, und darum versuchen, Sicherheitsprobleme zu kaschieren. Dadurch könnte ein falsches Bild über den tatsächlichen Status quo vermittelt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins DER.3.1 *Audits und Revisionen* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	Auditteam, Institutionsleitung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

DER.3.1.A1 Definition von Verantwortlichkeiten (B) [Institutionsleitung]

Die Institutionsleitung MUSS eine Person benennen, die dafür zuständig ist, Audits bzw. Revisionen zu planen und zu initiieren. Dabei MUSS die Institutionsleitung darauf achten, dass keine Interessenkonflikte entstehen.

Die Institution MUSS die Ergebnisse der Audits und Revisionen dazu verwenden, um die Sicherheitsmaßnahmen zu verbessern.

DER.3.1.A2 Vorbereitung eines Audits oder einer Revision (B)

Vor einem Audit oder einer Revision MUSS die Institution den Prüfgegenstand und die Prüfungsziele festlegen. Das betroffene Personal MUSS unterrichtet werden. Abhängig vom Untersuchungsgegenstand MUSS die Personalvertretung über das geplante Audit oder die geplante Revision informiert werden.

DER.3.1.A3 Durchführung eines Audits (B) [Auditteam]

Bei einem Audit MUSS das Auditteam prüfen, ob die Anforderungen aus Richtlinien, Normen, Standards und anderen relevanten Vorgaben erfüllt sind. Die geprüfte Institution MUSS die Anforderungen kennen.

Das Auditteam MUSS bei jedem Audit eine Dokumentenprüfung sowie eine Vor-Ort-Prüfung durchführen. Beim Vor-Ort-Audit MUSS das Auditteam sicherstellen, dass es niemals selbst aktiv in Systeme eingreift und keine Handlungsanweisungen zu Änderungen am Prüfgegenstand erteilt.

Das Auditteam MUSS sämtliche Ergebnisse eines Audits schriftlich dokumentieren und in einem Auditbericht zusammenfassen. Der Auditbericht MUSS der zuständigen Stelle in der Institution zeitnah übermittelt werden.

DER.3.1.A4 Durchführung einer Revision (B)

Bei einer Revision MUSS das Revisionsteam prüfen, ob die Anforderungen vollständig, korrekt, angemessen und aktuell umgesetzt sind. Die Institution MUSS festgestellte Abweichungen so schnell wie möglich korrigieren. Die jeweiligen Revisionen MÜSSEN mit einer Änderungsverfolgung dokumentiert werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

DER.3.1.A5 Integration in den Informationssicherheitsprozess (S)

Die Institution SOLLTE eine Richtlinie zur internen ISMS-Auditierung vorgeben. Außerdem sollte sie eine Richtlinie zur Lenkung von Korrekturmaßnahmen erstellen. Die Richtlinien SOLLTEN vorgeben, dass regelmäßige Audits und Revisionen ein Teil des Sicherheitsprozesses sind und durch diesen initiiert werden.

Der oder die ISB SOLLTE sicherstellen, dass die Ergebnisse der Audits und Revisionen in das ISMS zurückfließen und dieses verbessern. Der oder die ISB SOLLTE die durchgeführten Audits und Revisionen und deren Ergebnisse in den regelmäßigen Bericht an die Institutionsleitung aufnehmen. Auch SOLLTE dort festgehalten werden, welche Mängel beseitigt wurden und wie die Qualität verbessert wurde.

DER.3.1.A6 Definition der Prüfungsgrundlage und eines einheitlichen Bewertungsschemas (S)

Die Institution SOLLTE eine einheitliche Prüfungsgrundlage für Audits festlegen. Für die Bewertung der Umsetzung von Anforderungen SOLLTE ein einheitliches Bewertungsschema festgelegt und dokumentiert werden.

DER.3.1.A7 Erstellung eines Auditprogramms (S)

Der oder die ISB SOLLTE ein Auditprogramm für mehrere Jahre aufstellen, das alle durchzuführenden Audits und Revisionen erfasst. Für das Auditprogramm SOLLTEN Ziele definiert werden, die sich insbesondere aus den Institutionszielen sowie aus den Informationssicherheitszielen ableiten.

Der oder die ISB SOLLTE Reserven für unvorhergesehene Ereignisse in der jährlichen Ressourcenplanung vorsehen. Das Auditprogramm SOLLTE einem eigenen kontinuierlichen Verbesserungsprozess unterliegen.

DER.3.1.A8 Erstellung einer Revisionsliste (S)

Der oder die ISB SOLLTE eine oder mehrere Revisionslisten pflegen, die den aktuellen Stand der Revisionsobjekte sowie die geplanten Revisionen dokumentieren.

DER.3.1.A9 Auswahl eines geeigneten Audit- oder Revionsteams (S)

Die Institution SOLLTE für jedes Audit bzw. für jede Revision ein geeignetes Team zusammenstellen. Es SOLLTE eine Person benannt werden, die das Audit oder die Revision leitet. Diese SOLLTE die Gesamtverantwortung für die Durchführung der Audits bzw. der Revisionen tragen.

Die Größe des Audit- bzw. Revisionsteams SOLLTE dem Prüfbereich entsprechen. Die Institution SOLLTE insbesondere die Kompetenzanforderungen der Prüfthemen sowie die Größe und die örtliche Verteilung des Prüfbereichs berücksichtigen. Die Mitglieder des Audit- bzw. Revisionsteams SOLLTEN angemessen qualifiziert sein.

Die Neutralität des Auditteams SOLLTE sichergestellt werden. Darüber hinaus SOLLTE auch das Revisionsteam unabhängig sein. Werden externe Dienstleistende mit einem Audit oder einer Revision beauftragt, SOLLTEN diese auf ihre Unabhängigkeit hin überprüft und zur Verschwiegenheit verpflichtet werden.

DER.3.1.A10 Erstellung eines Audit- oder Revisionsplans (S) [Auditteam]

Vor einem Audit oder einer größeren Revision SOLLTE ein Audit- bzw. Revisionsplan erstellt werden. Bei Audits SOLLTE der Auditplan Teil des abschließenden Auditberichts sein. Der Auditplan SOLLTE während des gesamten Audits fortgeschrieben und bei Bedarf angepasst werden. Kleinere Revisionen SOLLTEN anhand der Revisionsliste geplant werden.

Die Institution SOLLTE genügend Ressourcen für das Audit- bzw. Revisionsteam vorsehen.

DER.3.1.A11 Kommunikation und Verhalten während der Prüfungen (S) [Auditteam]

Das Auditteam bzw. Revisionsteam SOLLTE klare Regelungen dafür aufstellen, wie das Audit- bzw. Revisionsteam und die Mitarbeitenden der zu prüfenden Institution bzw. Abteilung miteinander Informationen austauschen. Das Auditteam SOLLTE durch geeignete Maßnahmen sicherstellen, dass die bei einem Audit ausgetauschten Informationen auch vertraulich und integer bleiben.

Personen, die das Audit begleiten, SOLLTEN NICHT die Prüfungen beeinflussen. Zudem SOLLTEN sie zur Vertraulichkeit verpflichtet werden.

DER.3.1.A12 Durchführung eines Auftaktgesprächs (S) [Auditteam]

Das Auditteam bzw. das Revisionsteam SOLLTE ein Auftaktgespräch mit den betreffenden Ansprechpartnern oder Ansprechpartnerinnen führen. Das Audit- bzw. Revisionsverfahren SOLLTE erläutert und die Rahmenbedingungen der Vor-Ort-Prüfung abgestimmt werden. Die jeweiligen Verantwortlichen SOLLTEN dies bestätigen.

DER.3.1.A13 Sichtung und Prüfung der Dokumente (S) [Auditteam]

Die Dokumente SOLLTEN durch das Auditteam anhand der im Prüfplan festgelegten Anforderungen geprüft werden. Alle relevanten Dokumente SOLLTEN daraufhin geprüft werden, ob sie aktuell, vollständig und nachvollziehbar sind. Die Ergebnisse der Dokumentenprüfung SOLLTEN dokumentiert werden. Die Ergebnisse SOLLTEN auch in die Vor-Ort-Prüfung einfließen, soweit dies sinnvoll ist.

DER.3.1.A14 Auswahl von Stichproben (S) [Auditteam]

Das Auditteam SOLLTE die Stichproben für die Vor-Ort-Prüfung risikoorientiert auswählen und nachvollziehbar begründen. Die ausgewählten Stichproben SOLLTEN dokumentiert werden. Wird das Audit auf der Basis von Baustein-Zielobjekten und Anforderungen durchgeführt, SOLLTEN diese anhand eines vorher definierten Verfahrens ausgewählt werden. Bei der Auswahl von Stichproben SOLLTEN auch die Ergebnisse vorangegangener Audits berücksichtigt werden.

DER.3.1.A15 Auswahl von geeigneten Prüfmethoden (S) [Auditteam]

Das Auditteam SOLLTE für die jeweils zu prüfenden Sachverhalte geeignete Methoden einsetzen. Außerdem SOLLTE darauf geachtet werden, dass alle Prüfungen verhältnismäßig sind.

DER.3.1.A16 Ablaufplan der Vor-Ort-Prüfung (S) [Auditteam]

Das Auditteam SOLLTE den Ablaufplan für die Vor-Ort-Prüfung gemeinsam mit der Institution erarbeiten. Die Ergebnisse SOLLTEN im Auditplan dokumentiert werden.

DER.3.1.A17 Durchführung der Vor-Ort-Prüfung (S) [Auditteam]

Zu Beginn der Vor-Ort-Prüfung SOLLTE das Auditteam ein Eröffnungsgespräch mit der betreffenden Institution führen. Danach SOLLTEN alle im Prüfplan festgelegten Anforderungen mit den vorgesehenen Prüfmethoden kontrolliert werden. Weicht eine ausgewählte Stichprobe vom dokumentierten Status ab, SOLLTE die Stichprobe bedarfsorientiert erweitert werden, bis der Sachverhalt geklärt ist. Nach der Prüfung SOLLTE das Auditteam ein Abschlussgespräch führen. Darin SOLLTE es kurz die Ergebnisse ohne Bewertung sowie die weitere Vorgehensweise darstellen. Das Gespräch SOLLTE protokolliert werden.

DER.3.1.A18 Durchführung von Interviews (S) [Auditteam]

Das Auditteam SOLLTE strukturierte Interviews führen. Die Fragen SOLLTEN knapp, präzise und leicht verständlich formuliert werden. Zudem SOLLTEN geeignete Fragetechniken eingesetzt werden.

DER.3.1.A19 Überprüfung des Risikobehandlungsplans (S) [Auditteam]

Das Auditteam SOLLTE prüfen, ob die verbleibenden Restrisiken für den Informationsverbund angemessen und tragbar sind. Es SOLLTE außerdem prüfen, ob sie verbindlich durch die Institutionsleitung getragen werden. Maßnahmen, die grundlegend zur Informationssicherheit der gesamten Institution beitragen, DÜRFEN NICHT in diese Risikoübernahme einfließen.

Das Auditteam SOLLTE stichprobenartig verifizieren, ob bzw. wie weit die im Risikobehandlungsplan festgelegten Maßnahmen umgesetzt sind.

DER.3.1.A20 Durchführung einer Abschlussbesprechung (S) [Auditteam]

Das Auditteam SOLLTE mit der auditierten Institution eine Abschlussbesprechung durchführen. Darin SOLLTEN die vorläufigen Auditergebnisse dargelegt werden. Die weiteren Tätigkeiten SOLLTEN vorgestellt werden.

DER.3.1.A21 Auswertung der Prüfungen (S) [Auditteam]

Nach der Vor-Ort-Prüfung SOLLTE das Auditteam die gewonnenen Informationen weiter konsolidieren und auswerten. Nachdem auch nachgeforderte Dokumentationen und zusätzliche Informationen ausgewertet wurden, SOLLTEN die geprüften Maßnahmen endgültig bewertet werden. Um die nachgeforderten Dokumentationen bereitstellen zu können, SOLLTE das Auditteam der Institution ein ausreichendes Zeitfenster gewähren. Dokumente, die bis zum vereinbarten Termin nicht eingegangen sind, SOLLTEN als nicht existent gewertet werden.

DER.3.1.A22 Erstellung eines Auditberichts (S) [Auditteam]

Das Auditteam SOLLTE die gewonnenen Erkenntnisse in einen Auditbericht überführen und dort nachvollziehbar dokumentieren.

Die geprüfte Institution SOLLTE sicherstellen, dass alle betroffenen Stellen innerhalb einer angemessenen Frist die für sie wichtigen und notwendigen Passagen des Auditberichts erhalten.

DER.3.1.A23 Dokumentation der Revisionsergebnisse (S)

Die Ergebnisse einer Revision SOLLTEN einheitlich durch das Revisionsteam dokumentiert werden.

DER.3.1.A24 Abschluss des Audits oder der Revision (S) [Auditteam]

Nach dem Audit bzw. der Revision SOLLTE das Auditteam alle relevanten Dokumente, Datenträger und IT-Systeme zurückgeben oder vernichten. Das SOLLTE mit der geprüften Institution abgestimmt werden. Aufbewahrungspflichten aus gesetzlichen oder anderen verbindlichen Anforderungen SOLLTEN hierbei entsprechend berücksichtigt werden. Der oder die ISB SOLLTE alle für das Audit- oder Revisionsteam genehmigten Zugriffe wieder deaktivieren oder löschen lassen.

Mit der geprüften Institution SOLLTE vereinbart werden, wie mit den Ergebnissen umzugehen ist. Dabei SOLLTE auch festgelegt werden, dass die Auditergebnisse nicht ohne Genehmigung der geprüften Institution an andere Institutionen weitergeleitet werden dürfen.

DER.3.1.A25 Nachbereitung eines Audits (S)

Die Institution SOLLTE die im Auditbericht oder bei einer Revision festgestellten Abweichungen oder Mängel in einer angemessenen Zeit abstellen. Die durchzuführenden Korrekturmaßnahmen inklusive Zeitpunkt und Zuständigkeiten SOLLTEN dokumentiert werden. Auch abgeschlossene Korrekturmaßnahmen SOLLTEN dokumentiert werden. Die Institution SOLLTE dazu ein definiertes Verfahren etablieren und einsetzen.

Gab es schwerwiegende Abweichungen oder Mängel, SOLLTE das Audit- bzw. Revisionsteam überprüfen, ob die Korrekturmaßnahmen durchgeführt wurden.

DER.3.1.A26 Überwachen und Anpassen des Auditprogramms (S)

Das Auditprogramm SOLLTE kontinuierlich überwacht und angepasst werden, sodass Termine, Auditziele, Auditinhalte und die Auditqualität eingehalten werden.

Mithilfe der bestehenden Anforderungen an das Auditprogramm und mit den Ergebnissen der durchgeführten Audits SOLLTE überprüft werden, ob das Auditprogramm angemessen ist. Bei Bedarf SOLLTE es angepasst werden.

DER.3.1.A27 Aufbewahrung und Archivierung von Unterlagen zu Audits und Revisionen (S)

Die Institution SOLLTE Auditprogramme sowie Unterlagen zu Audits und Revisionen entsprechend den regulatorischen Anforderungen nachvollziehbar und revisionssicher ablegen und aufbewahren. Dabei SOLLTE sichergestellt werden, dass lediglich berechtigte Personen auf Auditprogramme und Unterlagen zugreifen können. Die Institution SOLLTE die Auditprogramme und Unterlagen nach Ablauf der Aufbewahrungsfrist sicher vernichten.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

DER.3.1.A28 ENTFALLEN (H)

Diese Anforderung ist entfallen.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization hat in der Norm „ISO 19011:2011“ Richtlinien zur Auditierung von Managementsystemen beschrieben.

Die International Organization for Standardization hat in der Norm „ISO ISO/IEC 27007:2011“ Richtlinien zur Auditierung eines ISMS beschrieben.

Das Information Security Forum hat im Dokument „The Standard of Good Practice for Information Security“ Richtlinien zur Auditierung eines ISMS beschrieben.