Kurzgutachten

Auditverfahren gemäß § 43 Abs. 2 LDSG

Kommunale IT-Standards für Kommunen in Schleswig-Holstein

Zentrale Komponenten – kits.system

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Datum : 04.09.2007
Aktenz. : 16.01/05.011
Telefon : 0431 988 1200
Fax : 0431 988 1223
E-Mail : mail@datenschutzzentrum.de

Inhaltsverzeichnis

1	**Gegenstand des Datenschutz-Audits**	**5**
1.1	Datenschutzziele	5
1.2	Darstellung des Auditgegenstands	6
1.3	Dokumentation des Auditgegenstands	8
2	**Feststellung zu den sicherheitstechnischen Elementen des Datenschutzmanagementsystems**	**10**
2.1	Integriertes Datenschutz- und Sicherheitsmanagementsystem	10
2.1.1	Aufbauorganisation	11
2.1.2	Ablauforganisation	12
2.2	Change-Management	13
2.2.1	Aufbauorganisation	13
2.2.2	Ablauforganisation	14
2.3	Räume und Gebäude	15
2.3.1	Rechenzentrum Altenholz	15
2.3.2	Administrative Büroräume	15
2.3.3	Serverraum beim kommunalen Nutzer	15
2.3.4	Schutzschrank beim kommunalen Nutzer	16
2.4	Rechnersysteme	17
2.4.1	Domänencontroller LANDSH.DE	18
2.4.2	Patchmanagementserver LANDSH.DE-SMS1	18
2.4.3	Zentrale Domänencontroller KV	19
2.4.4	Dezentraler Domänencontroller KV	19
2.4.5	SMS-Server	20
2.4.6	Administrative Clients	21
2.4.7	Testsysteme	22
2.5	Netzwerk	22
2.6	Virenschutz	22
2.7	Zentraler Verzeichnisdienst	24
2.7.1	Design Domäne LANDSH.DE	25
2.7.2	Design Domäne KV	25
2.7.3	Protokollierung	26
2.7.4	Berichtswesen	28
2.7.5	Administration durch Dataport	30
2.7.6	Administration durch den kommunalen Nutzer	30

2.8 Mailverbund 30

3 Datenschutzrechtliche Bewertung 32

3.1 Prüfungsverlauf 32

3.2 Rechtliche Anforderungen 33

3.3 Zusammenfassende Bewertung 34

1 Gegenstand des Datenschutz-Audits

Das Unabhängige Landeszentrum für Datenschutz (ULD) hat mit dem Finanzministerium Schleswig-Holstein und dem Kommunalen Forum für Informationstechnik (KomFITe.V. – im Folgenden KomFIT) vertraglich vereinbart, ein Datenschutzbehördenaudit nach § 43 Abs. 2 LDSG durchzuführen.

Gegenstand des Datenschutzaudits sind Konzept und Betrieb der zentralen Komponenten des kommunalen Systemkonzeptes KITS (kits.system), seine Auftragsverhältnisse, die Implementierung in einer Beispielskommune sowie die Zusammenarbeit mit KomFIT.

Das **Finanzministerium** ist als Betreiber der zentralen Komponenten von KITS (kits.system) Daten verarbeitende Stelle im Sinne der Hinweise zur Durchführung des Datenschutz-Behördenaudits (HDSA, Tz B 1) und damit **Auftraggeber des Audits im Sinne des § 43 Abs. 2 LDSG.**

Als gemeinsame Koordinierungs- und Beratungsstelle des Städteverbandes Schleswig-Holstein, des Schleswig-Holsteinischen Landkreistages und des Schleswig-Holsteinischen Gemeindetages für den Bereich der kommunalen Informations- und Kommunikationstechnik, **finanziert und begleitet** KomFIT e.V. die Komnzeption und den Betrieb von kits.system sowie **das Audit**.

1.1 Datenschutzziele

Das Finanzministerium und KomFIT e.V. haben für die zentralen Komponenten von KITS folgende **Datenschutzziele** festgelegt:

- Umsetzung der gesetzlichen und vertraglichen Vorgaben
- Gewährleistung der Ordnungsmäßigkeit der Datenverarbeitung
- Gewährleistung der Integrität und Verfügbarkeit der zentralen Systeme
- Schutz vertraulicher Informationen
- Minimierung der Gefährdung der Systeme der KITS-Nutzer durch die zentralen Systeme
- Minimierung der Gefährdung der zentralen Systeme durch KITS-Nutzer

1.2 Darstellung des Auditgegenstands

Die Kommunalen Landesverbände in Schleswig-Holstein haben in Abstimmung mit der Projektgruppe „IT-Standards“ des KomFIT e.V. Dataport beauftragt, das für die Landesbehörden entwickelte Landessystemkonzept IKOTECH-III auf kommunale Anforderungen anzupassen.

Die Ziele des kommunalen Systemkonzeptes sind

- der Auf- und Ausbau weitestgehend zentral administrierbarer Dienste, unter anderem ein zentraler Verzeichnisdienst, ein einheitlicher Mailverbund und ein umfassender Virenschutz sowie
- die Entwicklung eines modernen, multimediafähigen Büroarbeitsplatzes als Basis für die Nutzung kommunaler Fachanwendungen.

Genau wie das Landessystemkonzept ist das Gesamtkonzept KITS in zwei Teilbereiche untergliedert.

Der Teilbereich „kits.büro“ umfasst die dezentralen Komponenten von KITS, die von den Mitarbeiterinnen und Mitarbeiter der kommunalen Nutzer lokal genutzt werden. Im Allgemeinen handelt es sich hierbei um die Büroarbeitsplätze, die dazugehörende Peripherie und Server für die jeweiligen Fachverfahren. „kits.büro“ ist nicht Auditgegenstand.

Der Teilbereich **„kits.system**“ umfasst die zentralen Komponenten von KITS, die von allen Nutzern gemeinsam genutzt werden und bildet den **Gegenstand des Audits**.

Die folgende Abbildung beschreibt KITS einschließlich kits.büro, kits.system und die für KITS relevanten Komponenten aus IKOTECH-III.

Der **Auditgegenstand** umfasst im Einzelnen:

- die Domänencontroller KV-DC1 und KV-DC2 (Bereich K I),
- die KITS-Übergabeserver (Bereich K IIa)
- den zentralen KITS-Administrationsbereich mit den administrativen Arbeitsplätzen (Bereich K IV).

Auf den Systemen des Auditgegenstands werden **drei Anwendungen** betrieben:

- ein **zentraler Verzeichnisdienst**, basierend auf dem Active Directory des Herstellers Microsoft
- ein **einheitlicher Mailverbund**, basierend auf Microsoft Exchange
- ein **zentrales Antivirenmanagement**, basierend auf der Antivirensoftware des Herstellers McAfee.

Nicht Bestandteil des Audits ist das IKOTECH-III Basissystem. Dieses wurde jedoch bei der Überprüfung der sicherheitstechnischen Aspekte des Datenschutzmanagementsystems betrachtet (vgl. Abschnitt 2.4.1).

Ebenfalls nicht Bestandteil des Audits sind die Bereiche K IIb, K III, K V und K VI. Diese sind Bestandteil von kits.büro. Im Rahmen der Darstellung unter Textziffer 2 wird jedoch auf die sicherheitstechnischen Wechselwirkungen zu kits.system eingegangen.

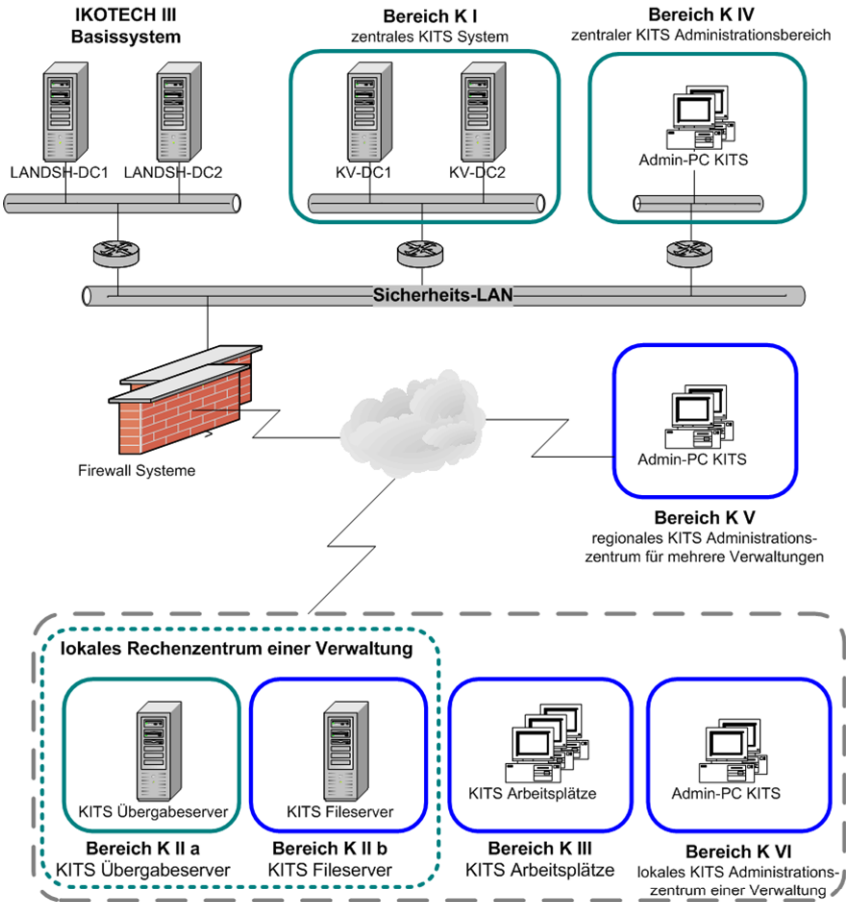


Abbildung 1: Überblick über KITS

1.3 Dokumentation des Auditgegenstands

Die zentralen Komponenten von KITS sind in mehreren Konzeptdokumenten beschrieben. Dem Audit liegen die Dokumente in der Version KITS 2.0 zu Grunde. Detailliert wird in einzelnen Dokumenten auf

- die zentralen Dienste,
- den Aufbau und Konfiguration der zentralen KITS Infrastruktur,
- die Administration der zentralen Infrastruktur und der Arbeitsplätze sowie
- die gemeinsame Nutzung eines Active Directory mit dem Land

eingegangen.

Dataport hat für KITS zusätzlich eine Reihe von internen Arbeitsanweisungen getroffen. Das Finanzministerium, Dataport und KomFIT haben für den Betrieb und die Weiterentwicklung von KITS (kits.system) vertragliche Vereinbarungen getroffen.

KomFIT hält die gesamte für KITS relevante Dokumentation vor und ist zuständig für ihre fortlaufende Aktualisierung.

Die gesamte KITS-Dokumentation ist **Gegenstand des Audits** und wurden einer ausführlichen **Begutachtung** unterzogen (siehe Tz. 2). Es handelt sich hierbei um die folgenden Dokumente:

Konzeptdokumente KITS 2.0

- Zentrale Komponenten V. 2.0
- Installation und Konfiguration zentraler Systeme V. 2.0
- Gruppenrichtlinien für die zentralen Systeme V. 2.0
- KITS Testumgebung V. 2.0
- Administrationskonzept V. 2.0
- Patchmanagement für kits.system V. 2.0
- Konfiguration Antivirensoftwaremanagement V. 2.0
- Berichtswesen im zentralen Antivirensoftware-Management V. 2.0
- Namenskonzept V. 2.0
- Standardsoftware V. 2.0
- Glossar V. 2.0
- Dezentrale Komponenten V. 2.0
- Installation und Konfiguration dezentraler Systeme V. 2.0
- Gruppenrichtlinien für die dezentralen Systeme V. 2.0
- Migrationskonzept V. 2.0
- Terminalserverkonzept V. 2.0
- Absicherung von USB-Ports V. 2.0
- Servervirtualisierung V. 2.0

- Sicherheitskonzept V. 2.0
- Risikoanalyse V. 2.0 (nicht Bestandteil des frei verfügbaren KITS-Konzepts)

Verträge

- Vertrag über die Beschaffung von IT-Dienstleistungen zwischen dem Finanzministerium und Dataport (EVB-IT Vertrag)
    - Anlage 1: Leistungsbeschreibung
    - Anlage 2: Datenschutz
    - Anlage 3: Service Level Agreements
    - Anlage 4: Sicherheitsmaßnahmen
    - Anlage 5: Obliegenheiten
- Vertrag über die Nutzung der zentralen Infrastruktur des kommunalen IT-Standards für Kommunen in Schleswig-Holstein (KITS) zwischen dem Land Schleswig-Holstein vertreten durch das Finanzministerium und dem Nutzer (Muster)
    - Anlage 1: Leistungsbeschreibung
    - Anlage 2: Datenschutz
    - Anlage 3: Service Level Agreements
    - Anlage 4: Sicherheitsmaßnahmen
    - Anlage 5: Obliegenheiten
- Vertrag über Dienstleistungen im Rahmen eines integrierten Datenschutz- und Sicherheitsmanagements zwischen dem Land Schleswig-Holstein vertreten durch das Finanzministerium und dem Kommunalen Forum für Informationstechnik der Kommunalen Landesverbände in Schleswig-Holstein (KomFIT e. V.)
    - Anlage 1: KITS-Change Management – Durchführungsbestimmungen

Betriebsdokumentation Dataport

- Rücksicherung / Wiederherstellung eines Übergabeservers V. 2.0
- Verhalten bei Sicherheitsvorfällen
- Sicherung der Server im Rechenzentrum
- Dataport IT-Sicherheitsleitlinie
- Dienstvereinbarung über die Nutzung des Bürokommunikationssystems bei Dataport
- IT-Sicherheits- und Datenschutzmanagementhandbuch
- Kryptokonzept
- Organisationshandbuch Version 0.1
- Anweisung: Passwortverwendung bei Dataport
- Dataport Personalmanagementhandbuch Version 0.1
- Sicherheitsrichtlinie Windows Server Version 0.83
- Betriebsprinzip Zentrale Datensicherung
- Zentrale Storagekomponenten Sicherheitsbetrachtung
- Arbeitsanweisung für die Regelarbeiten im Support Version 1.1

2 Feststellung zu den sicherheitstechnischen Elementen des Datenschutzmanagementsystems

2.1 Integriertes Datenschutz- und Sicherheitsmanagementsystem

Das Finanzministerium, Dataport und KomFIT haben ein gemeinsames Datenschutz- und Sicherheitsmanagementsystem (DSMS) für den Betrieb der zentralen KITS-Komponenten (kits.system) aufgebaut. Das DSMS ist im Dokument „Integriertes Datenschutz- und Sicherheitsmanagementsystem (DSMS)“ beschrieben.

Im DSMS werden Werkzeuge, Maßnahmen und Verantwortlichkeiten zusammengefasst, die ein dauerhaft hohes und nachhaltiges Datenschutz- und Datensicherheitsniveau umsetzen und gewährleisten sollen.

Sicherheitskonzept und integriertes Datenschutz- und Sicherheitsmanagementsystem dienen zur Erfüllung der folgenden gesetzlichen Vorgaben:

- Landesdatenschutzgesetz Schleswig-Holsten (LDSG)
- Datenschutzverordnung Schleswig-Holstein (DSVO)
- Handlungsanweisung zur Durchführung des Datenschutz-Behördenaudits (HDSA)

Das Sicherheitskonzept für kits.system und das DSMS orientieren sich an den Vorgaben der folgenden Standards BSI 100-1, 100-2 und 100-3 in Verbindung mit den IT-Grundschutz-Katalogen des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Die in diesen Standards dargestellten Sicherheitsmaßnahmen und Prozesse sind **Stand der Technik** im Sinne des § 5 Abs. 2 LDSG anzusehen.

Das DSMS definiert:

- Leitlinien und Ziele des integrierten Datenschutz- und Sicherheitsmanagements,
- den Geltungsbereich des Managementsystems,
- die Aufbauorganisation,
- die Ablauforganisation,
- die Werkzeuge, derer sich das Datenschutz- und Sicherheitsmanagement bedient,
- und das Berichtswesen zum Themenkreis Datenschutz und Datensicherheit.

Die **Gesamtverantwortung** für die IT-Sicherheit von kits.system liegt beim Finanzministerium Schleswig-Holstein. Im Finanzministerium wird die Leitung des DSMS dem Bereich VI 54 übertragen. Die Leitungsfunktion besteht vornehmlich darin, eine Kopfstelle für das Datenschutz- und Sicherheitsmanagement zu bilden.

Die Verantwortung eines Teils des operativen Sicherheitsmanagements ist durch vertragliche Vereinbarungen auf **KomFIT** übertragen. KomFIT übernimmt insbesondere die weitere Planung und Fortentwicklung des Sicherheitskonzepts sowie des Konzepts für das DSMS.

Dataport verfügt über ein eigenes, dataportweites gültiges Sicherheitsmanagement. Das ISMS wurde vom ULD am 27. August 2007[1] im Rahmen eines Konzeptaudits zertifiziert. In dem Audit wurde festgestellt, dass dieses ISMS bereits in Teilbereichen ausgerollt worden ist.

Für den Betrieb von kits.system wurden die Integration des ISMS von Dataport in das übergeordnete Sicherheitsmanagement bereits in wesentlichen Teilen vollzogen.

Über eine definierte Schnittstelle im Bereich des Betriebs von kits.system wird eine korrekte Implementierung des lokalen Sicherheitsmanagements für KITS in das übergreifende Sicherheitsmanagement bei Dataport sichergestellt.

2.1.1 Aufbauorganisation

Im Finanzministerium ist die Rolle der **des Sicherheitsmanagers** für kits.system eingerichtet.

Die Sicherheitsmanagerin oder der Sicherheitsmanager[2] ist **gesamtverantwortlich** für die Aufbau- und Ablauforganisation des integrierten Datenschutz- und Sicherheitsmanagementsystems. Er kontrolliert regelmäßig die korrekte Durchführung der Prozesse des DSMS, die Angemessenheit der Sicherheitskonzeption und die Wirksamkeit der Sicherheitsmaßnahmen. Der Sicherheitsmanager bewertet Maßnahmen und Risiken fachlich weisungsfrei. Er stellt die Schnittstelle zum übergreifenden Sicherheitsmanagement im Finanzministerium her und sorgt vor allem für eine Koordination des Sicherheitsprozesses mit der Sicherheitskonzeption des übergeordneten Standards IKOTECH-III. Bei Störungen in der Aufbau- oder Ablauforganisation entscheidet der Sicherheitsmanager abschließend über einzuleitende Maßnahmen.

Bei KomFIT ist die Rolle des **Sicherheitsbeauftragten** für KITS (kits.system) eingerichtet.

Der Sicherheitsbeauftragte KomFIT ist verantwortlich für die organisatorische und technische Weiterentwicklung der Sicherheitskonzeption von kits.system.

[1] https://www.datenschutzzentrum.de/audit/kurzgutachten/a0717/index.htm

[2] Die nachfolgend verwendeten männlichen Bezeichnungen gelten für beide Geschlechter gleichermaßen.

Bei Dataport ist ein **Sicherheitskoordinator** für den Betrieb von kits.system eingerichtet.

Der Sicherheitskoordinator bei Dataport stellt die Schnittstelle zum dataport-internen Sicherheitsmanagement (ISMS) her.

Zur Koordinierung in Fragen des Datenschutzes und der Datensicherheit im Kreise der KITS-Anwender ist ein **Sicherheitsgremium** eingerichtet.

Über das Sicherheitsgremium können die Nutzer Ihre Pflichten im Sinne der Auftragsdatenverarbeitung gemäß § 17 LDSG für kits.system erfüllen. Über das Sicherheitsgremium wird eine Schnittstelle zur lokalen Sicherheitsorganisation des KITS-Anwenders – in der Regel Datenschutzbeauftragte, Dienststellenleitung und IT-Bereich – hergestellt.

2.1.2 Ablauforganisation

Im DSMS sind Prozesse definiert für

- regelmäßige Kontrollen,
- anlassbezogene Kontrollen,
- die Behandlung von Sicherheitsvorfällen,
- die Integration von Datenschutz und Datensicherheit in den Betrieb und die weitere Entwicklung von kits.system
- eine Dokumentation des gesamten Sicherheitsprozesses und
- ein regelmäßiges Berichtswesen zu Datenschutz und Datensicherheit

Das DSMS sieht vor, dass zumindest jährlich alle getroffenen Sicherheitsmaßnahmen auf Angemessenheit und korrekte Umsetzung geprüft werden.

Der Sicherheitsmanager kann anlassbezogene Kontrollen durchführen.

Die Behandlung von Sicherheitsvorfällen wird in zwei Schritten durchgeführt:

In der ersten Stufe hat die Behebung des Sicherheitsvorfalls und die Information der von dem Vorfall Betroffenen absolute Priorität:

- Alle KITS-Nutzer werden informiert. Der Sicherheitsbeauftragte KomFIT entscheidet über die angemessene Art der Benachrichtigung.
- Der Sicherheitsbeauftragte KomFIT benachrichtigt den Sicherheitskoordinator bei Dataport und den Sicherheitsmanager im Finanzministerium.
- Der Sicherheitsbeauftragte KomFIT beruft ein Vorfallmanagementteam ein. Die Zusammensetzung richtet sich nach Schwere und Ausmaß des Vorfalls.
- Das Vorfallmanagementteam koordiniert die Bearbeitung des Sicherheitsvorfalls und trifft die notwendigen Maßnahmen zur Behebung.

Zur späteren Nachbereitung werden alle mit dem Sicherheitsvorfall verbundenen Vorgänge und Entscheidungen nachvollziehbar **dokumentiert**. Zur Bearbeitung von Sicherheitsvorfällen werden außerdem technische Unterlagen, wie Protokolle oder für den Vorfall besonders relevante System-Meldungen, gespeichert und archiviert. Der Sicherheitsbeauftragte KomFIT ist verantwortlich für die Dokumentation der Sicherheitsvorfälle.

In der zweiten Stufe wird der Sicherheitsvorfall nachbereitet. In einem Bericht **bewertet** der Sicherheitsbeauftragte KomFIT die bereits dokumentierten Vorgänge, Entscheidungen und Maßnahmen. Der Bericht soll darüber hinaus ermöglichen, Verbesserungen an den Notfallstrategien vorzunehmen und bekannte Fehler zu vermeiden.

Der Sicherheitsbeauftragte KomFIT stellt sicher, dass in der Fortentwicklung des KITS-Konzepts, des Sicherheitskonzepts sowie des Konzepts für das DSMS die hohen Anforderungen für Integrität, Verfügbarkeit und Vertraulichkeit erfüllt werden. Er ist in sämtliche Prozesse der Fortentwicklung eingebunden und definiert in Fragen der Sicherheit und des Datenschutzes die notwendigen Maßnahmen.

Zusammen mit den aktuellen Versionen der KITS-Dokumentation werden sämtliche Berichte des Sicherheitsmanagements bei KomFIT vorgehalten. Diese Sicherheitsdokumentation enthält zusätzlich alle sicherheitsrelevanten Dataport-internen Regelungen und Dokumentationen für kits.system.

Der Sicherheitsbeauftragte KomFIT fertigt unter Leitung des Sicherheitsmanagers und in Zusammenarbeit mit dem Sicherheitsgremium bzw. Anwenderkreis sowie dem Sicherheitskoordinator bei Dataport einen **jährlichen Sicherheitsbericht** an.

Der jährliche Sicherheitsbericht enthält:

- die Dokumentation der aufgetretenen Sicherheitsvorfällen,
- sicherheitsrelevanten Änderungen in der KITS-Konzeption oder -Ablaufumgebung (kits.system),
- Kurzberichte zu den durchgeführten, regelmäßigen Sicherheitskontrollen und
- Kurzberichte zu den anlassbezogenen Sicherheitskontrollen.

2.2 Change-Management

Zur koordinierten Weiterentwicklung von kits.system wird in KITS ein an ITIL angelehnter Change-Prozess genutzt. Der Change-Prozess ist detailliert in einem eigenen KITS 2.0 – Konzept festgelegt. Über den Change-Prozess kontrollieren die kommunalen Nutzer die Entwicklungen in kits.system.

2.2.1 Aufbauorganisation

Über die Annahme und die Freigabe von Änderungen an kits.system entscheidet ein Change

Advisory Board (CAB). Die Geschäftsführung des CAB liegt bei KomFIT. Mitglieder des CAB sind jeweils ein Vertreter jedes kommunalen Nutzers sowie der Geschäftsführer des CAB. Stimmberechtigt ist jeweils ein Vertreter der Nutzer.

Das Finanzministerium hat im CAB Gaststatus, hat jedoch bei domänenübergreifenden Änderungen ein beschränktes Veto-Recht (vgl. folgenden Abschnitt).

2.2.2 Ablauforganisation

Änderungen an kits.system können initiiert werden von:

- den Nutzern durch ihren jeweils benannten Vertreter im CAB,
- dem Vertreter des Finanzministeriums
- dem Auftragnehmer Dataport oder
- der Geschäftsstelle KomFIT

Änderungsanträge werden bei KomFIT schriftlich oder per E-Mail eingereicht. KomFIT klassifiziert und priorisiert die eingehenden Änderungsanträge gegenüber dem CAB in einer Stellungnahme.

KomFIT empfiehlt dem CAB, Änderungsanträge abzulehnen, wenn ihre Umsetzung unwirtschaftlich ist oder wenn die Umsetzung die Sicherheit des Gesamtsystems erkennbar bedroht.

Das CAB kann Standard-Changes definieren, die von KomFIT direkt ohne vorherige Beschlussfassung des CAB beauftragt werden können.

KomFIT darf Dataport direkt mit der Umsetzung einer Änderung beauftragten, wenn eine schnelle Umsetzung aus Sicherheitsgründen oder anderen wichtigen Gründen zwingend geboten ist und ein Umlaufverfahren nicht rechtzeitig beendet werden kann (Notkompetenz). Die Mitglieder des CAB werden unverzüglich per E-Mail oder telefonisch über die Änderung und ihre Gründe zu informieren. Das CAB kann die Änderung nachträglich rückgängig machen oder ändern.

Jedes Mitglied des CAB kann in den Fällen des Abs. 1 Nr. 1 sowie des Abs. 3 die Berücksichtigung der Stellungnahme der Sicherheitsbeauftragten des Auftraggebers sowie des ULD verlangen. Hat ein Änderungsantrag domänenübergreifende Auswirkungen (z.B. Schemaerweiterungen), dann holt KomFIT zuvor die Zustimmung des Finanzministeriums ein. Die Zustimmung darf nur bei Änderungen verweigert werden, die die Stabilität des Gesamtsystems beeinträchtigen. Fällt die Stellungnahme negativ aus, so setzt sich KomFIT zur Neuformulierung des Antrags mit dem Antragsteller ins Benehmen.

Dataport prüft die Änderungen in der Testumgebung, dokumentiert die Ergebnisse und bewertet sie in einer Stellungnahme. Das CAB entscheidet anhand der Testergebnisse über die Umsetzung in der Echtumgebung. Bei positiver Beschlussfassung beauftragt KomFIT Dataport mit der Umsetzung.

KomFIT informiert das Finanzministerium über die beauftragte Änderung.

2.3 Räume und Gebäude

2.3.1 Rechenzentrum Altenholz

Die folgenden Komponenten werden durch Dataport am Standort Altenholz im Rechenzentrum betrieben:

- Domänencontroller LANDSH-DC1 und LANDSH-DC2
- Patchmanagementsystem LANDSH-SMS1
- Domänencontroller KV-DC1 und KV-DC2

Das Rechenzentrum beherbergt darüber hinaus die zentralen Komponenten des Landesnetzes (vgl. Tz 2.5).

Dataport stellt sicher, dass

- nur authentifizierte und autorisierte Personen Zutritt zum Rechenzentrum haben,
- der Zutritt zum Rechenzentrum protokolliert wird,
- das Rechenzentrum ausreichend klimatisiert ist,
- das Rechenzentrum mit wirksamen Brandmelde- und -bekämpfungsanlagen ausgestattet ist,
- die im Rechenzentrum betriebenen IT-Systeme an eine unterbrechungsfreie Stromversorgung angeschlossen sind.

2.3.2 Administrative Büroräume

Dataport nutzt zur Administration und für die allgemeine Betreuung der Nutzer herkömmliche Büroräume. Über eine gesonderte Arbeitsanweisung ist zusätzlich zu den allgemeinen Regelungen bei Dataport sichergestellt, dass die hierfür genutzten Räume beim Verlassen zu verschließen sind.

Der direkte Außenbereich des Gebäudes ist videoüberwacht. Die Videoaufzeichnungen werden ständig durch einen Wachdienst überprüft.

2.3.3 Serverraum beim kommunalen Nutzer

Das Finanzministerium trifft mit jedem kommunalen Nutzer vertragliche Vereinbarungen über die Nutzung von kits.system. Der kommunale Nutzer sichert zu

- den Serverraum in einem funktionsfähigen und ordnungsgemäßen Zustand zu halten.
- den für die Installation und den Betrieb des Übergabeservers erforderlichen Platz in einem geeigneten und abgesicherten Serverraum mit Strom und Er-

dung zur Verfügung zu stellen.

- den Beschäftigten Dataport bzw. den von ihr Beauftragten das Betreten des Serverraumes während der üblichen Dienstzeiten zu gestatten, soweit dies zur Installation des Übergabeservers sowie aus Service- und Wartungsgründen erforderlich ist.
- den Serverraum bzw. den Aufbauort des Übergabeservers vor einem unberechtigten Zugriff der eigenen Beschäftigten sowie Dritter durch geeignete Maßnahmen zu sichern.

Im Serverraum der kommunalen Nutzer werden die dezentralen Domänencontroller betrieben. Auf diesen ist eine Kopie aller im Active Directory gespeicherten Daten aller kommunalen Nutzer gespeichert. Diese Konfiguration führt nach der Schutzbedarfsfeststellung zu einem hohen Schutzbedarf für die Integrität und der Vertraulichkeit der auf diesem System gespeicherten Daten. Eine Kompromittierung eines dezentralen Domänencontrollers führt nach Herstelleraussagen dazu, dass nahezu sämtliche Daten des Verzeichnisdienstes überprüft und in großen Teilen neu aufgebaut werden müssen.

Das Finanzministerium kann allein durch vertragliche Zusicherungen nicht das für die Domänencontroller erforderliche Sicherheitsniveau garantieren. Aus diesem Grund wird als zusätzliche Sicherheitsmaßnahme im Serverraum des kommunalen Nutzers ein Schutzschrank (angelehnt an wesentliche Teile der Anforderungen der Norm EN 14450) aufgestellt, der in Verbindung mit den vertraglichen Zusicherungen ein ausreichendes Sicherheitsniveau für den Schutzbedarf der dezentralen Domänencontroller bietet. Der Schutzschrank kann auch für andere sicherheitsrelevante Komponenten unter Kontrolle des Finanzministeriums genutzt werden.

2.3.4 Schutzschrank beim kommunalen Nutzer

Um die physikalischen Sicherheit der dezentralen Domänencontroller zu gewährleisten, wird ein gesondert gesicherter Schutzschrank genutzt.

Der Schutzschrank ist geeignet, einen Angreifer mit mittlerem Hebel- oder Schlagwerkzeug (Vorschlaghammer, Brecheisen…) hinreichenden Widerstand zu leisten.

Abbildung 2: Schutzschrank

Der Serverschrank wurde vom Hersteller durch zusätzliche Sicherheitsmaßnahmen gesichert, unter anderem durch

- den Austausch der Glastüren durch Stahlblechtüren,
- die Erweiterung des Schließsystems der Türen auf eine Mehrfachverriegelung,
- die Sicherung sämtlicher von außen erreichbarer Schraubverbindungen durch Schlossschrauben,
- eine zusätzliche Sicherung von Deckel und Bodenteilen gegen Aufkantversuche sowie
- den Einsatz eines Sicherheits-Schließzylinders.

2.4 Rechnersysteme

Die Installation und Konfiguration der für den Betrieb von kits.system genutzten Rechnersysteme ist detailliert in den einzelnen Dokumenten des Konzepts KITS 2.0 (vgl. Tz 1.3) beschrieben.

Im Folgenden wird auf die wesentlichen Sicherheitsmaßnahmen eingegangen, die auf den jeweiligen Systemen getroffen worden sind.

Sämtliche Systeme beziehen Authentifizierungs- und Autorisierungsdaten aus dem zentralen Verzeichnisdienst (Microsoft Active Directory). Zusätzlich werden wesentliche Sicherheitsmaßnahmen zentral über den Verzeichnisdienst durchgesetzt (Gruppenrichtlinien). Eine genauere Darstellung der sicherheitstechnischen Elemente des Active Directories findet sich im Abschnitt 2.7.

2.4.1 Domänencontroller LANDSH.DE

Die Domänencontroller für LANDSH.DE sind nicht Auditgegenstand. Sie haben jedoch direkten Einfluss auf die Sicherheit von KITS. Die Angemessenheit und korrekte Umsetzung der für KITS wesentlichen Sicherheitsmaßnahmen auf diesen Domänencontrollern sind aus diesem Grund in diesem Audit überprüft worden.

Die zwei Domänencontroller für die Root-Domäne LANDSH.DE sind identisch installiert und konfiguriert. Die Installation folgt dem Minimalprinzip, d.h. jedes System ist lediglich mit der für den Betrieb notwendigen Software versehen. Bei der Installation oder Konfiguration verwendete Passworte sind bei Dataport nach einem einheitlichen Verfahren hinterlegt (vgl. Tz. 2.7.5).

Beide Domänencontroller sind mit einer aktuellen Version der Antivirensoftware ausgestattet. Die Aktualität wird durch ein zentrales Antivirenmanagement innerhalb von IKOTECH-III überwacht. Die Systeme sind mit aktuellen Patches und Updates ausgestattet. Die Inventarisierung und Installation der Patches und Updates erfolgt über eine zentrale Lösung (Systems Management Server von Microsoft, SMS).

Die Domänencontroller sind an die zentrale Datensicherung im Dataport Rechenzentrum angeschlossen.

Die Domänencontroller sind nach Vorgaben des Herstellers für den Betrieb als Domänencontroller konfiguriert und werden in Anlehnung an seine Empfehlungen für den Betrieb eines Active Directories betrieben.

2.4.2 Patchmanagementserver LANDSH.DE-SMS1

Das Patchmanagement ist gegenüber dem Change-Management klar abgegrenzt. Mit der Umsetzung des Patchmanagements hat das Finanzministerium Dataport beauftragt. Dataport hat hierzu einen internen Prozess aufgesetzt, der sich auf den Prozess zum Management von CERT-Meldungen stützt. Dieser Prozess sieht die folgenden Schritte vor:

- Meldungen über potentielle Sicherheitslücken und die für die Behebung zur Verfügung stehende Patches werden daraufhin untersucht, ob sie für kits.system relevant sind und hinsichtlich der Kritikalität in vier Kategorien bewertet.
- Als für kits.system relevant eingestufte Patches werden in der Testumgebung eingespielt, getestet und bei einem positiven Testergebnis für die Einspielung in die jeweiligen Produktionssysteme freigegeben.
- Freigegebene Patches werden über den SMS-Server zentral in Form von Softwarepaketen auf den Produktionssystemen eingespielt.
- Der gesamte Prozess der Patchanalyse, Testinstallation, Freigabe und Kontrolle wird dokumentiert.

2.4.3 Zentrale Domänencontroller KV

Die Installation und Konfiguration der Domänencontroller ist in den KITS Konzepten detailliert beschrieben.

Die beiden Domänencontroller sind identisch installiert und konfiguriert. Die Softwareausstattung auf den Systemen folgt dem Minimalprinzip.

Administrativer Zugriff auf die Domänencontroller ist nur Benutzern mit domänenadministrativen Rechten möglich. Die Vergabe dieser Rechte ist durch ein eigenes Konzept geregelt (vgl. Tz 2.7.5).

Die Domänencontroller unterliegen den Regelungen und Prozessen des zentralen Antivirenmanagements (vgl. Tz. 2.6) und werden durch ein zentrales Patchmanagement (vgl. Tz. 0) mit explizit freigegebenen Patches und Updates versorgt.

Die Daten der Domänencontroller werden durch die zentrale Lösung zur Datensicherung im Rechenzentrum bei Dataport gesichert. Dataport hat die getroffenen Sicherheitsmaßnahmen in einer internen Betriebsdokumentation und entsprechenden Sicherheitskonzepten und Leitlinien dokumentiert und festgelegt, deren Umsetzung durch konkrete Arbeitsanweisungen gewährleisten wird. Der Zugriff auf die hochsensiblen Authentifizierungs- und Autorisierungsdaten des zentralen Verzeichnisdienstes ist auf wenige Personen begrenzt. In detaillierten Anweisungen ist sowohl die Datensicherung als auch die Rücksicherung der Daten geregelt. Dataport führt regelmäßige Rücksicherungstests durch, um die Funktionsfähigkeit der Datensicherung zu überprüfen.

2.4.4 Dezentraler Domänencontroller KV

Die dezentralen Domänencontroller werden gemäß den im KITS-Konzept genannten Hardwareanforderungen von dem kommunalen Nutzer beschafft und durch Dataport im Auftrag des Finanzministeriums installiert und konfiguriert.

Die Installation und Konfiguration der Domäncontroller ist im KITS-Konzept detailliert vorgegeben.

Der Virenschutz und das Patchmanagement werden analog zum Vorgehen bei den zentralen Domänencontrollern der Domäne KV umgesetzt.

Die Daten der dezentralen Domänencontroller werden durch ein unabhängiges Backupverfahren gesichert. Da sich die Server in verschlossenen Serverschränken befinden und damit ein Bandlaufwerk nicht zugänglich wäre, erfolgt die Sicherung in Dateien. Diese Sicherungsdateien werden von einem anderen Server aus auf ein Sicherungsmedium mitgesichert.

Auf den dezentralen Domänencontrollern befinden sich sowohl Daten des jeweiligen kommunalen Nutzers (Exchange-Postfächer) als auch die Domänendaten aller anderen kommunalen Nutzer (Domänendaten). Aus diesem Grund werden die Daten bei

der Sicherung getrennt behandelt und teilweise verschlüsselt.

Die Sicherung der Domänendaten auf dem dezentralen Domänencontroller wird in eine verschlüsselte Datei geschrieben. Lediglich Dataport hat Zugriff auf die hierfür benötigten Schlüssel.

Die Daten des kommunalen Nutzers werden getrennt von den Domänendaten in einen eigenen Bereich gesichert und nicht verschlüsselt.

Die verschlüsselten Domänendaten und die Daten des kommunalen Nutzers können von dem kommunalen Nutzer in sein eigenes Backupsystem übernommen werden, sämtliche Domänendaten bleiben hierbei jedoch stets vor unberechtigter Einsichtnahme gesichert. Im Falle einer Wiederherstellung eines Domänencontrollers entschlüsselt Dataport nach der Rücksicherung die verschlüsselten Domänendaten und stellt die lokale Kopie des Verzeichnisdienstes wieder her.

2.4.5 SMS-Server

Die Inventarisierung und Installation der für einen sicheren Betrieb von kits.system notwendigen Updates und Patches wird zentral durchgeführt.

Hierzu nutzt Dataport den bereits für IKOTECH-III bereitgestellten SMS-Server. Auf dem SMS-Server sind für die KITS-Systeme vom IKOTECH-III-Betrieb unabhängige Gruppen zur Steuerung der Patchverteilung eingerichtet worden.

Sämtliche Patches und Updates werden vor der Freigabe in der Produktivumgebung in einer KITS-eigenen Testumgebung auf mögliche Fehler getestet (vgl. Tz. 2.4.7).

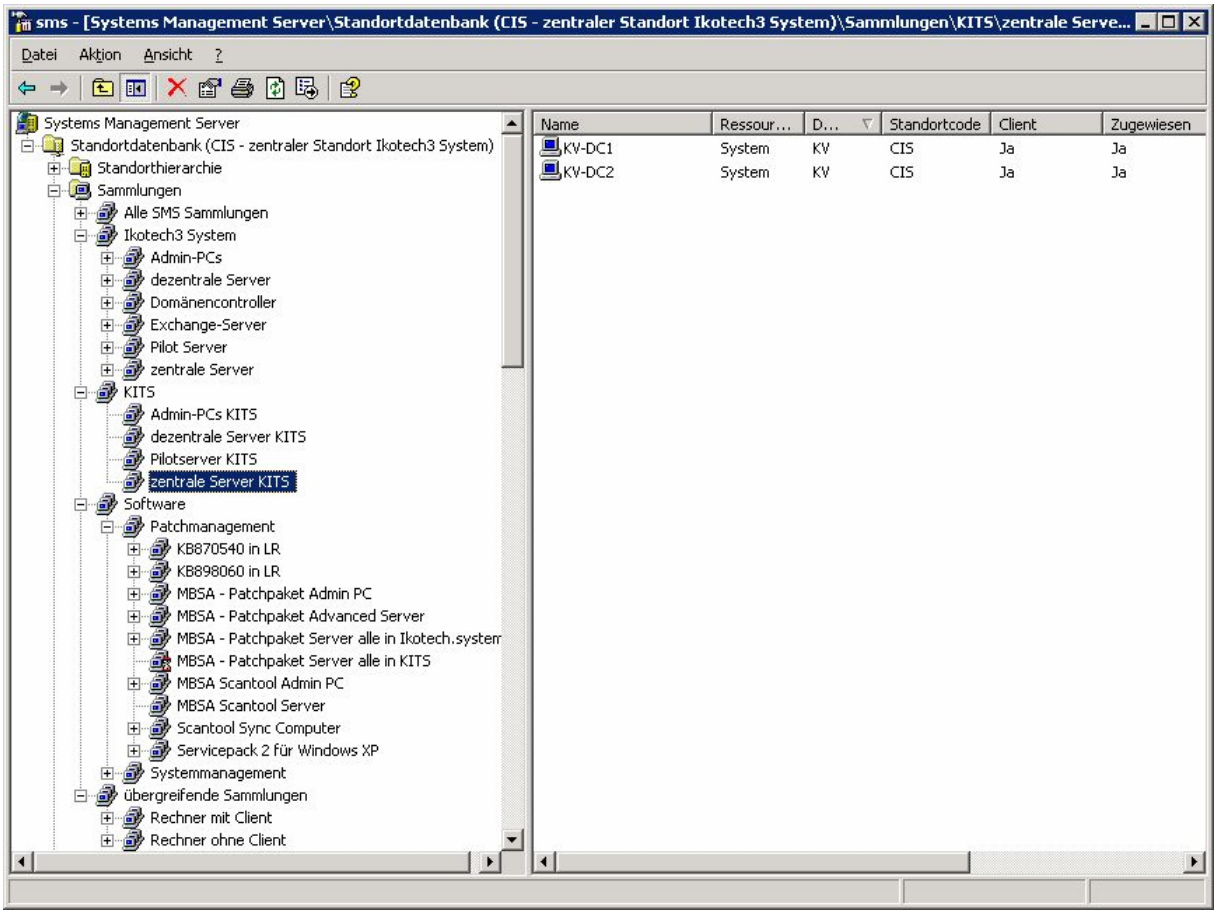


Abbildung 3: Beispielansicht der SMS-Konsole

2.4.6 Administrative Clients

Dataport setzt für die Administration von kits.system exklusiv hierfür bereitgestellte administrative Clients ein. Die Clients werden mit derselben Infrastruktur wie die Domänencontroller mit Patches, Updates und einem aktuellen Antivirenschutz versehen.

Die Konfiguration der administrativen Clients erfolgt weitestgehend durch spezielle Gruppenrichtlinien. Auf den Clients ist nur die Software installiert, die zwingend für die Administration des Active Directories benötigt wird.

Die Administrations-Clients befinden sich in Büroräumen am Standort Altenholz von Dataport. Auf den Clients befinden sich keinerlei Informationen, die bei Verlust der Integrität des jeweiligen Clients KITS gefährden. Insbesondere wird durch gesonderte Einstellungen gemäß einer Gruppenrichtlinie das Zwischenspeichern von Anmeldeinformationen deaktiviert. Ein Diebstahl eines Clients oder eine nicht ordnungsgemäße Aussonderung hat somit keinen direkten Einfluss auf die Sicherheit des Gesamtsystems.

Die administrativen Clients befinden sich in einem eigenen Netzsegment ohne direk-

te Verbindung zum Dataport Hausnetz. Jeder KITS-Administrator nutzt zwei getrennte Clients: einen Hausnetzclient für die normale Bürokommunikation und einen KITS-Administrationsclient für die Arbeit in kits.system.

2.4.7 Testsysteme

Wesentliche Änderungen an kits.system, die Auswirkungen auf den Verfahrensbetrieb oder das Sicherheitsniveau von kits.system oder aber kits.büro haben könnten, unterliegen einem Change-Management (vgl. Tz. 2.2).

Zur Vorbereitung von Changes werden sämtliche Änderungen zunächst in einer Testumgebung durchgeführt.

Hierzu ist eine eigene Domäne TESTKV aufgebaut worden, die über Domänencontroller, administrative Clients und eine prototypischen Umgebung für kits.büro verfügt. Die Testumgebung folgt den Vorgaben der KITS-Konzeption.

In der Testumgebung werden keine Daten der Produktivumgebung verwendet, eine Spiegelung der Daten der Produktivumgebung in die Testumgebung findet nicht statt.

2.5 Netzwerk

KITS (kits.system) nutzt für die Anbindung der dezentralen Komponenten von kits.system das Landesnetz Schleswig-Holstein. Das Landesnetz wurde 2006 durch das Unabhängige Landeszentrum für Datenschutz nach § 43 Abs. 2 LDSG auditiert. Die Sicherheitskonzeption des Landesnetzes ist in der Generaldokumentation des Landesnetzes zusammengefasst.

In der Sicherheitsstrategie der Generaldokumentation des Landesnetzes wird für alle Komponenten des Landesnetzes gleichermaßen ein hoher Schutzbedarf vorausgesetzt. Dieser Schutzbedarf wird bezüglich der Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit der Daten ermittelt.

In Verbindung mit den für das Produkt Active Directory getroffenen Sicherheitsmaßnahmen und dem im Landesnetz für alle angeschlossenen Nutzer einheitlichen Sicherheitsniveau werden für den Betrieb von kits.system umfangreiche Sicherheitsmaßnahmen zur Absicherung des Datentransfers getroffen.

2.6 Virenschutz

KITS bietet allen Komponenten ein zentrales Antivirensoftware-Management (AVM). Die für den Betrieb der zentralen Komponenten (kits.system) verwendeten IT-Systeme sind vollständig an diese Lösung angebunden.

Für die zentrale Verwaltung und Kontrolle sämtlicher Systeme kommt der sogenannte ePolicy Orchestrator Server (ePO Server) der Firma Network Associates zum Ein-

satz. Über diesen wird die Antivirensoftware – McAfee VirusScan, GroupShield für Exchange – konfiguriert und administriert.

Über den ePO Server werden alle Parameter für die Antivirensoftware festgelegt. Zur Kommunikation zwischen der Antivirensoftware und dem ePO Server wird auf jedem IT-System ein sogenannter ePO Agent installiert, der ebenfalls über den ePO Server konfiguriert und administriert wird.

Für die zentralen und dezentralen Domänencontroller sowie für die Arbeitsplätze zur Administration der zentralen Services ist der Einsatz des zentralen AVM obligatorisch.

Über die eingesetzte Antivirensoftware wird sichergestellt, dass

- die Client-Komponenten des Virenschutzes zentral installiert, administriert und konfiguriert werden,
- Updates automatische und manuelle verteilt werden und
- Berichte zur Aktualität und Vollständigkeit des Virenschutzes zentral erstellt werden.

Kommunale Nutzer können die zentral bereitgestellten Berichte über die Aktualität einzelner Systeme und die Vollständigkeit des Virenschutzes sowie zusätzlich zur lokalen Anzeige auf den Systemen über Virenfunde abrufen.

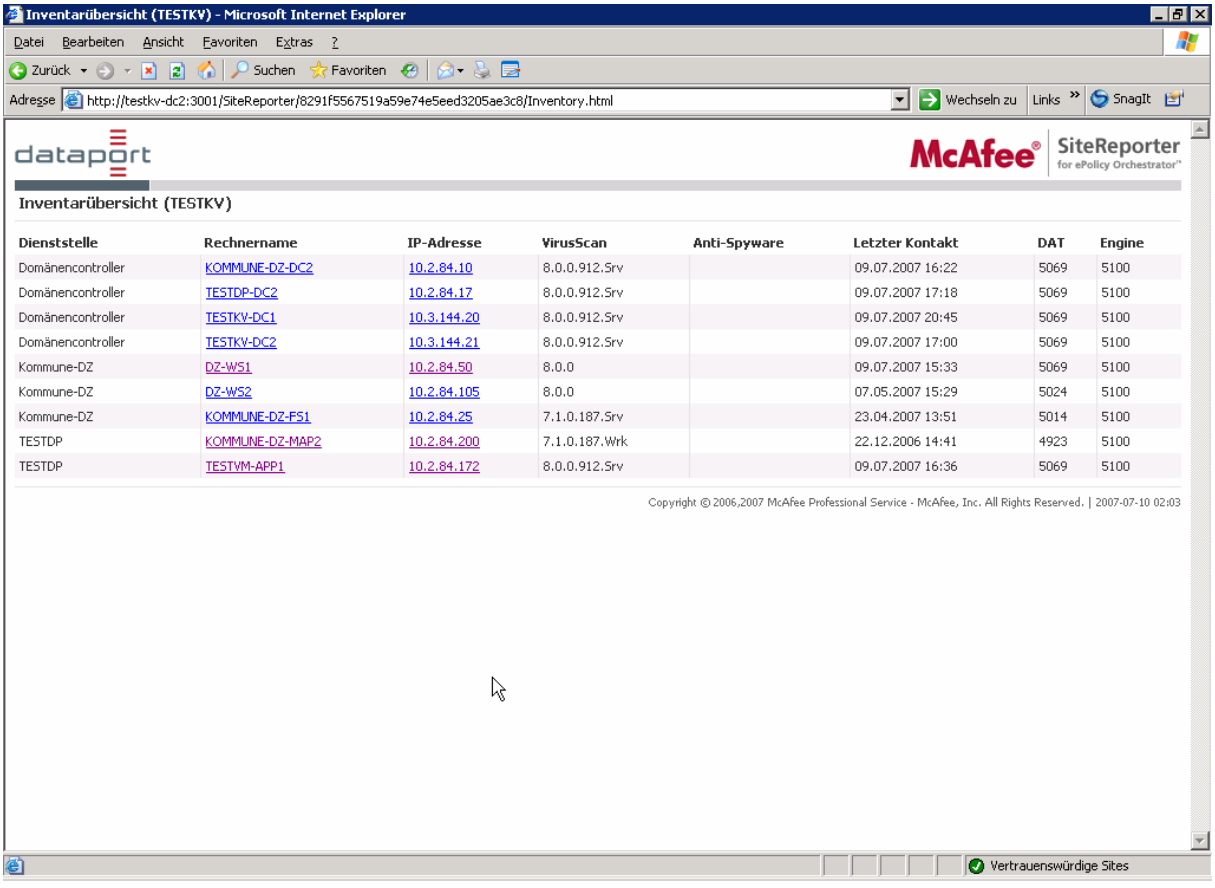


Abbildung 4: Beispieldarstellung des AV-Reportings

2.7 Zentraler Verzeichnisdienst

Das Finanzministerium setzt für die Realisierung eines zentralen Verzeichnisdienstes das Active Directory von Microsoft ein.

Unter einer gemeinsamen Root-Domäne wird in einem sogenannten Forest zum einen die IKOTECH-III-Infrastruktur des Landes als auch die KITS-Infrastruktur des kommunalen Bereichs betrieben.

Der Name der Root-Domäne ist „LANDSH.DE“. Die IKOTECH-III-Domäne wird mit „LR“ bezeichnet, die KITS-Domäne mit „KV“.

Die folgende Abbildung verdeutlicht die Domänenstruktur:

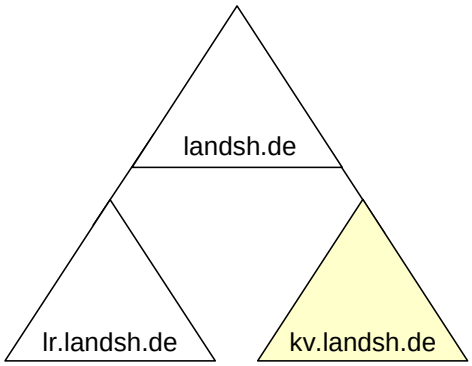


Abbildung 5: Domänenstruktur

Der Forest ist auf mehrere Domänencontroller (vgl. Tz 2.4) verteilt. Die Domänendaten werden sternförmig über mehrere Stufen auf die dezentralen Domänencontroller (vgl Tz 2.4.4) repliziert.

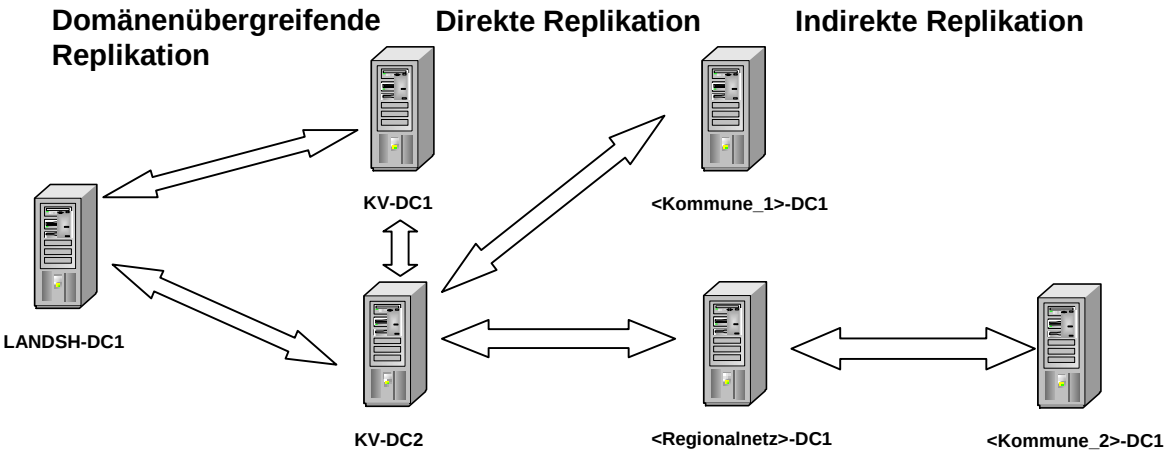


Abbildung 6: Replikation

Durch die sternförmige Replikation ist sichergestellt, dass keine direkte Kommunikation einzelner KITS-Nutzer untereinander auf Basis der AD-Protokolle möglich ist.

2.7.1 Design Domäne LANDSH.DE

Das Design der Root-Domäne LANDSH.DE folgt den Vorgaben von Microsoft. Es wird das Konzept der „leeren“ Domäne umgesetzt: In der Domäne befinden sich außer den für administrative Zwecke genutzten Konten und den Domänencontrollern keinerlei weiteren Objekte.

Die Verwendung von administrativen Rechten ist in einem eigenständigen Administrationskonzept festgelegt (vgl. Tz. 2.7.5)

Die für die Forest-weite Nutzung benötigten Rechte des „Organisations-Administrators“ werden standardmäßig nicht vergeben, die dafür genutzte Gruppe hat keine Mitglieder. Werden die Rechte eines Organisations-Administrators benötigt, so wird ausschließlich nach schriftlicher Anforderung auf Basis eines Tickets im Dataport-weiten Ticketsystem ein Domänen-Administrator der Root-Domäne mit den Rechten eines Organisations-Administrators versehen. Die Vergabe und der Entzug dieser Rechte werden im Trouble-Ticket-System von Dataport dokumentiert.

2.7.2 Design Domäne KV

Für das Design der Domäne KV sind detaillierte Vorgaben im KITS Konzept vorhanden.

Jedem kommunalen Nutzer wird eine eigene Organisationseinheit (OU) bereitgestellt. Die OU wird bereits vorstrukturiert. Administrative Arbeitsplätze werden von normalen Büroarbeitsplätzen getrennt verwaltet, indem diese jeweils in getrennte Unter-OUs aufgeteilt werden.

Zur strukturierten Vergabe der Berechtigungen auf diesen Unterbereichen im AD werden eigene Berechtigungsgruppen definiert, über die der kommunale Nutzer eigenständig verfügen kann.

Nach Anlegen dieser initialen Struktur werden sämtliche administrativen Rechte an der OU mit allen untergeordneten OUs an den kommunalen Nutzer übertragen und den Domänenadministratoren alle Rechte entzogen. Dataport hat danach ohne Mitwirkung des kommunalen Nutzers und unter Einhaltung des Administationskonzepts (vgl. Tz. 2.7.5) keine administrativen Zugriffsmöglichkeiten auf die Datenverarbeitung des jeweiligen kommunalen Nutzers.

KITS stellt den kommunalen Nutzern vordefinierte zentrale Gruppenrichtlinien bereit, die durch eine Vielzahl von administrativen Einstellungen eine automatisierte Konfiguration seiner IuK-Umgebung erlauben. Die Gruppenrichtlinien werden bei der erstmaligen Konfiguration der OU des kommunalen Nutzers standardmäßig aktiviert. Der kommunale Nutzer kann unter Nutzung seiner eigenen administrativen Rechte die Nutzung dieser Gruppenrichtlinien rückgängig machen, um beispielsweise eigene Richtlinien zu aktivieren. Änderungen an den Gruppenrichtlinien werden als Change im Rahmen des Change-Managements (vgl. Tz. 2.2) durchgeführt.

Die Überprüfung sowie die weitere Pflege der Rechte auf der eigenen OU obliegen der Verwaltung. Hierzu werden dem Nutzer angepasste Standard-Werkzeuge von Microsoft sowie eine detaillierte Änderungsprotokollierung und ein ausführliches Berichtswesen bereitgestellt.

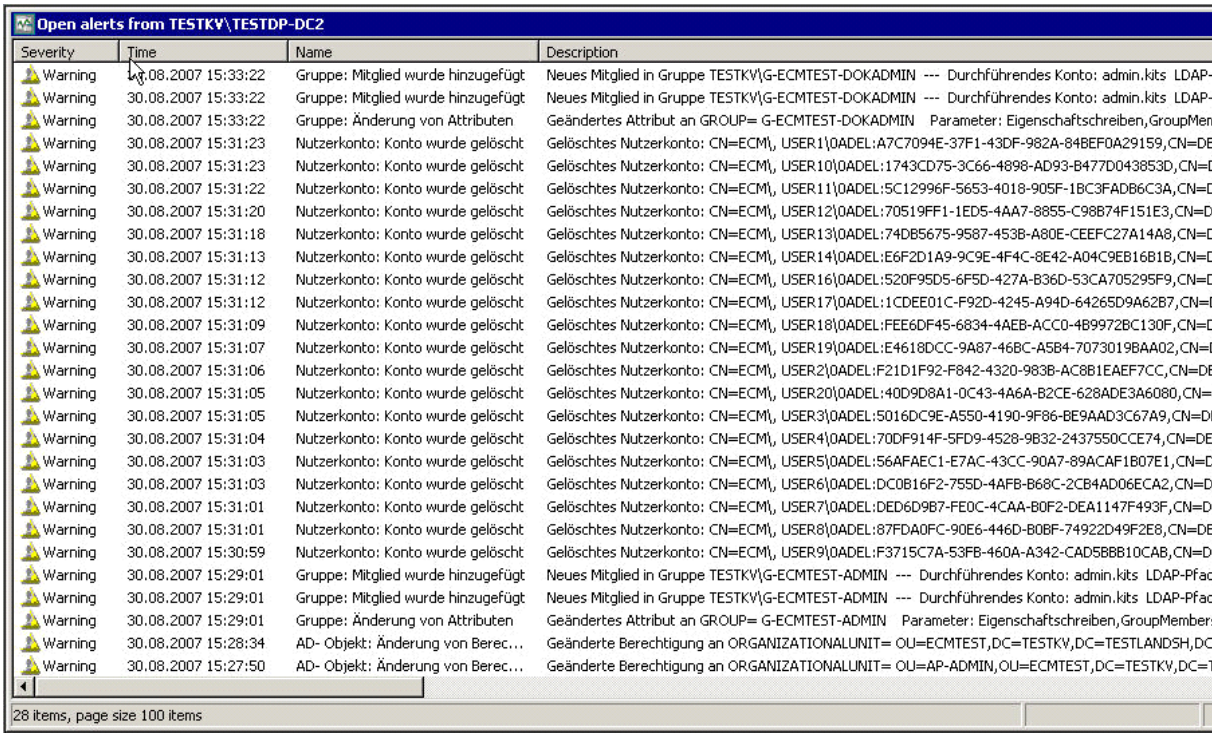
2.7.3 Protokollierung

Dataport führt eine detaillierte Protokollierung der Aktivitäten und Änderungen im Active Directory durch. Die Protokollierung wird in einer vom KITS-Betrieb unabhängigen Einheit an einem anderen Standort durchgeführt, um Interessenskollisionen bei der Ausgestaltung und Auswertung der Protokolldaten weitestgehend auszuschließen.

Die Protokollfunktionen des Active Directories sind ohne weitere technische oder organisatorische Maßnahmen für den Betrieb mit mehreren eigenständigen Daten verarbeitenden Stellen gemäß LDSG nicht ausreichend. Innerhalb KITS wird aus diesem Grund eine zusätzliche Lösung eines Drittherstellers (NetIQ) eingesetzt, die die hohen Anforderungen an die Protokollierung und Auswertung der Protokolldaten umsetzen kann.

Die Protokollierung erfolgt revisionssicher, d.h. technisch und organisatorisch von der Domänenadministration getrennt. Art und Umfang der Protokollierung sowie der Umgang mit Protokolldaten und Revision werden in einem Fachkonzept festgelegt.

Kommunale Nutzer können somit sämtliche für den eigenen IT-Betrieb relevanten Betriebs- und Änderungsereignisse im Active Directory einfach erfassen.



Open alerts from TESTKV\TESTDP-DC2

Severity	Time	Name	Description
Warning	30.08.2007 15:33:22	Gruppe: Mitglied wurde hinzugefügt	Neues Mitglied in Gruppe TESTKV\G-ECMTEST-DOKADMIN --- Durchführendes Konto: admin.kits LDAP-
Warning	30.08.2007 15:33:22	Gruppe: Mitglied wurde hinzugefügt	Neues Mitglied in Gruppe TESTKV\G-ECMTEST-DOKADMIN --- Durchführendes Konto: admin.kits LDAP-
Warning	30.08.2007 15:33:22	Gruppe: Änderung von Attributen	Geändertes Attribut an GROUP= G-ECMTEST-DOKADMIN Parameter: Eigenschaftschreiben,GroupMen
Warning	30.08.2007 15:31:23	Nutzerkonto: Konto wurde gelöscht	Gelöschtes Nutzerkonto: CN=ECM\, USER1\0ADEL:A7C7094E-37F1-43DF-982A-84BEF0A29159,CN=DE
Warning	30.08.2007 15:31:23	Nutzerkonto: Konto wurde gelöscht	Gelöschtes Nutzerkonto: CN=ECM\, USER10\0ADEL:1743CD75-3C66-4898-AD93-B477D043853D,CN=D
Warning	30.08.2007 15:31:22	Nutzerkonto: Konto wurde gelöscht	Gelöschtes Nutzerkonto: CN=ECM\, USER11\0ADEL:5C12996F-5653-4018-905F-1BC3FADB6C3A,CN=D
Warning	30.08.2007 15:31:20	Nutzerkonto: Konto wurde gelöscht	Gelöschtes Nutzerkonto: CN=ECM\, USER12\0ADEL:70519FF1-1ED5-4AA7-8855-C98B74F151E3,CN=D
Warning	30.08.2007 15:31:18	Nutzerkonto: Konto wurde gelöscht	Gelöschtes Nutzerkonto: CN=ECM\, USER13\0ADEL:74DB5675-9587-453B-A80E-CEEFC27A14A8,CN=D
Warning	30.08.2007 15:31:13	Nutzerkonto: Konto wurde gelöscht	Gelöschtes Nutzerkonto: CN=ECM\, USER14\0ADEL:E6F2D1A9-9C9E-4F4C-8E42-A04C9EB16B1B,CN=D
Warning	30.08.2007 15:31:12	Nutzerkonto: Konto wurde gelöscht	Gelöschtes Nutzerkonto: CN=ECM\, USER16\0ADEL:520F95D5-6F5D-427A-B36D-53CA705295F9,CN=D
Warning	30.08.2007 15:31:12	Nutzerkonto: Konto wurde gelöscht	Gelöschtes Nutzerkonto: CN=ECM\, USER17\0ADEL:1CDEE01C-F92D-4245-A94D-64265D9A62B7,CN=D
Warning	30.08.2007 15:31:09	Nutzerkonto: Konto wurde gelöscht	Gelöschtes Nutzerkonto: CN=ECM\, USER18\0ADEL:FEE6DF45-6834-4AEB-ACC0-4B9972BC130F,CN=D
Warning	30.08.2007 15:31:07	Nutzerkonto: Konto wurde gelöscht	Gelöschtes Nutzerkonto: CN=ECM\, USER19\0ADEL:E4618DCC-9A87-46BC-A5B4-7073019BAA02,CN=D
Warning	30.08.2007 15:31:06	Nutzerkonto: Konto wurde gelöscht	Gelöschtes Nutzerkonto: CN=ECM\, USER2\0ADEL:F21D1F92-F842-4320-983B-AC8B1EAEF7CC,CN=DE
Warning	30.08.2007 15:31:05	Nutzerkonto: Konto wurde gelöscht	Gelöschtes Nutzerkonto: CN=ECM\, USER20\0ADEL:40D9D8A1-0C43-4A6A-B2CE-628ADE3A6080,CN=
Warning	30.08.2007 15:31:05	Nutzerkonto: Konto wurde gelöscht	Gelöschtes Nutzerkonto: CN=ECM\, USER3\0ADEL:5016DC9E-A550-4190-9F86-BE9AAD3C67A9,CN=D
Warning	30.08.2007 15:31:04	Nutzerkonto: Konto wurde gelöscht	Gelöschtes Nutzerkonto: CN=ECM\, USER4\0ADEL:70DF914F-5FD9-4528-9B32-2437550CCE74,CN=DE
Warning	30.08.2007 15:31:03	Nutzerkonto: Konto wurde gelöscht	Gelöschtes Nutzerkonto: CN=ECM\, USER5\0ADEL:56AFAEC1-E7AC-43CC-90A7-89ACAF1B07E1,CN=D
Warning	30.08.2007 15:31:03	Nutzerkonto: Konto wurde gelöscht	Gelöschtes Nutzerkonto: CN=ECM\, USER6\0ADEL:DC0B16F2-755D-4AFB-B68C-2CB4AD06ECA2,CN=D
Warning	30.08.2007 15:31:01	Nutzerkonto: Konto wurde gelöscht	Gelöschtes Nutzerkonto: CN=ECM\, USER7\0ADEL:DED6D9B7-FE0C-4CAA-B0F2-DEA1147F493F,CN=D
Warning	30.08.2007 15:31:01	Nutzerkonto: Konto wurde gelöscht	Gelöschtes Nutzerkonto: CN=ECM\, USER8\0ADEL:87FDA0FC-90E6-446D-B0BF-74922D49F2E8,CN=DE
Warning	30.08.2007 15:30:59	Nutzerkonto: Konto wurde gelöscht	Gelöschtes Nutzerkonto: CN=ECM\, USER9\0ADEL:F3715C7A-53FB-460A-A342-CAD5BBB10CAB,CN=D
Warning	30.08.2007 15:29:01	Gruppe: Mitglied wurde hinzugefügt	Neues Mitglied in Gruppe TESTKV\G-ECMTEST-ADMIN --- Durchführendes Konto: admin.kits LDAP-Pfad
Warning	30.08.2007 15:29:01	Gruppe: Mitglied wurde hinzugefügt	Neues Mitglied in Gruppe TESTKV\G-ECMTEST-ADMIN --- Durchführendes Konto: admin.kits LDAP-Pfad
Warning	30.08.2007 15:29:01	Gruppe: Änderung von Attributen	Geändertes Attribut an GROUP= G-ECMTEST-ADMIN Parameter: Eigenschaftschreiben,GroupMember
Warning	30.08.2007 15:28:34	AD- Objekt: Änderung von Berec...	Geänderte Berechtigung an ORGANIZATIONALUNIT= OU=ECMTEST,DC=TESTKV,DC=TESTLAND5H,DC
Warning	30.08.2007 15:27:50	AD- Objekt: Änderung von Berec...	Geänderte Berechtigung an ORGANIZATIONALUNIT= OU=AP-ADMIN,OU=ECMTEST,DC=TESTKV,DC=T

28 items, page size 100 items

Abbildung 7: Beispiel Protokollierung

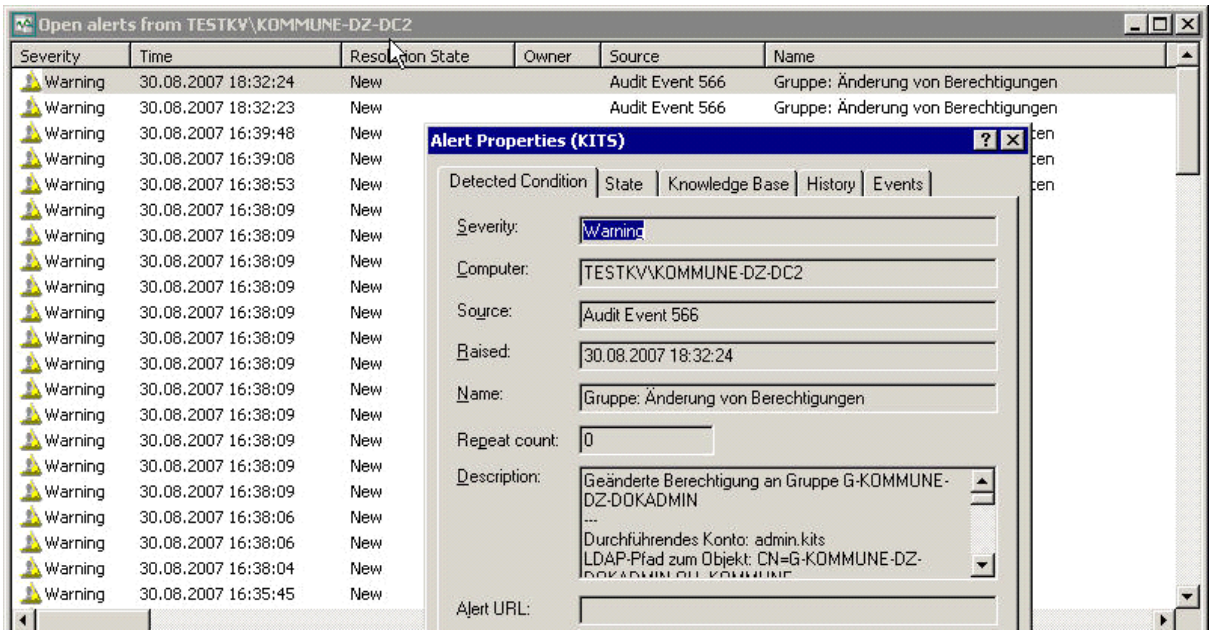


Abbildung 8: Detailansicht Protokolleintrag

2.7.4 Berichtswesen

Sowohl die erzeugten Protokolldaten als auch die Bestandsdaten des Active Directories – Benutzer, Gruppen, Computer, Organisationseinheiten, Gruppenrichtlinien – bilden die Grundlage zum einen für ein funktionierendes Sicherheitsmanagement in KITS, vor allem aber sind sie die Grundlage für die eigene Sicherheitskonzeption und –revision der kommunalen Nutzer.

Die für den Nutzer relevanten Objekte, Einstellungen, Änderungen und Protokolldaten des ActiveDirectory-Betriebs werden in aussagekräftigen Berichten zusammengefasst.

KITS stellt den kommunalen Nutzern zur Unterstützung ihrer Verantwortung für die eigenen Daten als Mittel zur Revision speziell auf den Anwendungsfall angepasste, vordefinierte Berichte zur Verfügung. Die Berichte werden regelmäßig erstellt. Änderungen seit dem letzten Bericht werden explizit dargestellt. Die Berichte können zusätzlich auf Anforderung eines kommunalen Nutzers erstellt und übermittelt werden. Das Berichtswesen ist Bestandteil des integrierten Datenschutz- und Sicherheitsmanagements.

Kommunale Nutzer können auf Anforderung bei Dataport zusätzlich spezialisierte Einzelberichte erstellen lassen.

Die Berichte stellen sicher, dass die Kommunalen Nutzer zusätzlich zur Nutzung der administrativen Programme des Herstellers auf einfache Art und Weise über eine komplette Dokumentation aller für den eigenen IT-Betrieb relevanten Parameter und Einstellungen verfügen. Auf diese Weise ermöglicht und unterstützt das Berichtswesen die kommunalen Nutzer bei der Erfüllung ihrer Aufgaben der Datenschutzkon-

trolle und IT-Revision.

Report Date	From Date	To Date	Platform
30.08.2007 17:54:39	22.08.2007	30.08.2007	Windows

	Group	User	Action	Date	Log Entries
4	g-ECMTEST-admin	admin.kits	Security Enabled Global Group Created	8/28/2007	1
5	g-ECMTEST-admin	admin.kits	Security Enabled Global Group Member Added	8/28/2007	1
6	g-ECMTEST-admin	admin.kits	Security Enabled Global Group Changed	8/28/2007	1
				Total	3

Report Date	From Date	To Date	Platform
30.08.2007 17:54:39	22.08.2007	30.08.2007	Windows

	Group	User	Action	Date	Log Entries
8	Server-Operatoren	admin.bodle	Security Enabled Local Group Member Added	8/28/2007	1
9	Server-Operatoren	admin.bodle	Security Enabled Local Group Changed	8/28/2007	1
				Total	2

Report Date	From Date	To Date	Platform
30.08.2007 17:54:39	22.08.2007	30.08.2007	Windows

	Group	User	Action	Date	Log Entries
12	Administrators	kruppaM	Security Enabled Local Group Member Added	8/22/2007	1
				Total	1

Abbildung 9: Detaileinträge Berichtswesen

2.7.5 Administration durch Dataport

Die Administration bei Dataport erfolgt über dedizierte Administrationsarbeitsplätze, die sich in einem vom Hausnetz von Dataport getrennten Netzsegment befinden.

Dataport hat die Administration des Active Directories in eigenständigen Dokumenten ausführlich geregelt. Für die Regeltätigkeiten im Betrieb des Active Directories, insbesondere die Störungsbehebung und die Bearbeitung von Nutzeranfragen, hat Dataport die Prozesse und Verantwortlichkeiten in einer Arbeitsanweisung festgelegt.

Zusätzlich werden die Vergabe und Nutzung administrativer Rechte in einem Administrationskonzept festgelegt. Auf Basis einer detaillierten Aufgabenanalyse werden die minimal benötigten administrativen Rechte aufgeführt. Auf Basis der benötigten Rechte werden die hieraus folgenden Standard-Rollen im AD identifiziert und einzelnen, personenbezogenen und ausschließlich für administrative Zwecke genutzten Accounts zugeordnet.

Die Nutzung domänenadministrativer Rechte wird streng reglementiert. Festgelegt ist, dass zu jedem Zeitpunkt domänenadministrative Rechte lediglich zwei personenbezogenen Accounts zugeordnet sind. Änderungen im Rahmen von Urlaubs- oder Vertretungsregelungen werden schriftlich unter Nutzung des Dataport-weiten Ticketsystems angefordert. Die Umsetzung wird im jeweiligen Ticket dokumentiert.

Änderungen an administrativen Gruppen werden über die im Abschnitt 2.7.3 beschriebene Protokollierung vermerkt. Die Protokollierung kann lediglich unter Ausnutzung domänenadministrativer Rechte beeinflusst werden. Jede Beeinflussung wird zuverlässig erkannt und als Sicherheitsvorfall durch das DSMS behandelt.

Die jeweils vergebenen administrativen Berechtigungen können jederzeit zusätzlich zu den vorhandenen Verwaltungsprogrammen des Herstellers über das im Abschnitt 2.7.4 beschriebene Berichtswesen eingesehen werden.

2.7.6 Administration durch den kommunalen Nutzer

Jeder Nutzer hat ausschließlich administrative Rechte auf der ihm zugeordneten Organisationseinheit (OU). Die von Microsoft vorgesehenen administrativen Programme sind durch Gruppenrichtlinien bereits so vorkonfiguriert, dass dem kommunalen Nutzer nur die für ihn relevanten Daten angezeigt werden.

2.8 Mailverbund

Auf den Domänencontrollern ist für den Aufbau eines KITS-weiten Mailverbunds Microsoft Exchange installiert.

Die auf den zentralen Domänencontrollern installierten Instanzen von Microsoft Ex-

change bilden die Kopfstelle für den Mailverbund innerhalb KITS. Diese Kopfstelle stellt alle notwendigen Übergänge zu weiteren Mailverbunden / Mailsystemen bereit, unter anderem dem IKOTECH-III-Mailverbund sowie einen SMTP-Übergang in das Internet.

Für jeden kommunalen Nutzer wird eine eigene administrative Gruppe mit einer entsprechenden Routinggruppe erstellt. Den Administratoren der Verwaltung wird das Recht „Administrator – Nur Ansicht“ auf ihre administrative Gruppe zugewiesen.

Ein administrativer Zugriff auf die Postfächer und Kalender der einzelnen Anwender ist grundsätzlich deaktiviert und kann nur mit administrativen Rechten eingerichtet werden. Die Berechtigungsvergabe auf alle Exchange-Objekte (Server, Postfächer, Gruppen, Administrative Einstellungen etc.) wird durch den zentralen Verzeichnisdienst gesteuert. Sämtliche Tätigkeiten und Änderungen werden durch die Protokollierung und das Berichtswesen dokumentiert und sind für den kommunalen Nutzer nachvollziehbar.

3 Datenschutzrechtliche Bewertung

3.1 Prüfungsverlauf

Das Audit **„Kommunale IT-Standards für Kommunen in Schleswig-Holstein– Zentrale Komponenten“** wurde vom Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein (ULD) in mehren Phasen begleitet.

In einzelnen Modulen wurden Teilaspekte der zentralen Infrastruktur von KITS (kits.system) betrachtet und im Rahmen einer Sachverhaltsdarstellung der Änderungsbedarf festgestellt.

In regelmäßigen Abständen fanden mit Dataport, KomFIT und dem Finanzministerium **Projektgruppensitzungen** statt, in denen die vom ULD festgestellten Sachverhalte diskutiert und Lösungen für die Verbesserung und Optimierung zur Erreichung der festgelegten Datenschutzziele erarbeitet wurden (vgl. Tz. 1).

Nach Abschluss aller Arbeiten und nach Erreichung der vom Finanzministerium und KomFIT festgelegten Ziele hat das ULD im August 2007 die **Begutachtungsphase** eingeleitet. Analysiert wurden insbesondere die konzeptkonforme Umsetzung der Sicherheitsmaßnahmen und technischen sowie organisatorischen Vorgaben für den Betrieb der zentralen Komponenten von KITS.

Vor Ort wurden sämtliche IT-Systeme sowie die notwendigen Betriebsprozesse einer **intensiven Begutachtung** unterzogen. Dazu gehörten insbesondere folgende Punkte:

- Das Sicherheitskonzept einschließlich Risikoanalyse
- Die Dokumentation der Maßnahmenumsetzung im GSTool
- Das Datenschutz- und Sicherheitsmanagementsystem einschließlich Patchmanagement
- Die revisionssichere Protokollierung und das Berichtswesen
- Umsetzung der festgelegten technischer Sicherheitsmaßnahmen auf den zentralen Domänenkontrollern

Stichprobenartig wurde die Umsetzung der dokumentierten Maßnahmen in den folgenden Bereichen überprüft:

- Umsetzung der festgelegten Maßnahmen in der Rechenzentrumsinfrastruktur bei Dataport
- Virenschutzmanagement

3.2 Rechtliche Anforderungen

Das Finanzministerium verarbeitet beim Betrieb der zentralen Komponenten von KITS (kits.system) personenbezogene Daten der kommunalen Nutzer in deren Auftrag. Das Finanzministerium hat durch vertragliche Vereinbarung Dataport mit dem Betrieb der zentralen Komponenten und KomFIT mit der Durchführung des Sicherheitsmanagements beauftragt.

Das **Landesdatenschutzgesetz** sowie die **Datenschutzverordnung** finden infolgedessen Anwendung. Die gesetzlichen Regelungen zur Datensicherheit erfordern die Umsetzung technischer und organisatorischer Maßnahmen nach dem Stand der Technik.

Technische und organisatorische Maßnahmen müssen zunächst im Sinne einer Vorgabe auf konzeptioneller Ebene beschrieben werden. Die Umsetzung der geplanten Maßnahmen muss detailliert dokumentiert werden.

Ein angemessenes IT-Sicherheitsniveau kann nur durch geplantes und organisiertes Vorgehen aller Beteiligten erreicht und aufrechterhalten werden. Voraussetzung für die sinnvolle Umsetzung und Erfolgskontrolle von Sicherheitsmaßnahmen ist eine systematische Vorgehensweise.

Dabei sind insbesondere folgende Rechtsvorschriften zu beachten:

- **Landesdatenschutzgesetz (LDSG)**

§ 4 Datenvermeidung und Datensparsamkeit

§ 5 Allgemeine Maßnahmen zur Datensicherheit

§ 6 Besondere Maßnahmen zur Datensicherheit bei Einsatz automatisierter Verfahren

§ 7 Verfahrensverzeichnis, Meldung

§ 8 Gemeinsame Verfahren und Abrufverfahren

§ 17 Verarbeitung personenbezogener Daten im Auftrag, Wartung

- **Datenschutzverordnung (DSVO)**

§ 3 Verfahrensdokumentation

§ 4 Verfahrenszweck

§ 5 Verfahrensbeschreibung

§ 6 Sicherheitskonzept

§ 7 Test und Freigabe

§ 8 Verfahrensübergreifende Dokumentation und Protokolle

Darüber hinaus sind interne Regelungen über die personelle und organisatorische Gestaltung der Datensicherheit zu treffen. Es muss gewährleistet sein, dass die datenschutzrechtlichen Anweisungen auch tatsächlich in konkrete Datensicherungsmaßnahmen umgesetzt werden und ihre Einhaltung durch das ISMS kontrolliert wird.

Die Verantwortlichen der kommunalen Nutzer müssen in die Lage versetzt werden, die Sicherheitsmaßnahmen und das daraus resultierende Sicherheitsniveau der zentralen Komponenten von kits.system einschätzen zu können. Im Rahmen vertraglicher Vereinbarungen werden diese Sicherheitsmaßnahmen im Sinne einer Weisung durch den kommunalen Nutzer an den Auftragnehmer schriftlich fixiert werden.

3.3 Zusammenfassende Bewertung

Im Rahmen des Audits **„Kommunale IT-Standards für Kommunen in Schleswig-Holstein– Zentrale Komponenten“**“ wurde festgestellt, dass

- das Finanzministerium in vertraglichen Vereinbarungen mit den kommunalen Nutzern eine nach § 17 LDSG i.V.m. §§ 4-7 DSVO ordnungsgemäße Datenverarbeitung im Auftrag korrekt und umfassend regelt.
- der Auftragnehmer Dataport die gemäß §§ 5 und 6 LDSG erforderlichen technischen und organisatorischen Maßnahmen nach dem Stand der Technik getroffen hat, die der Schutzbedürftigkeit der verarbeiteten personenbezogenen Daten angemessen sind.
- das Finanzministerium, KomFIT und Dataport ein geeignetes Datenschutzmanagementsystem für kits.system eingerichtet haben, welches die Umsetzung der Datenschutzziele dokumentiert und bei zukünftigen Entwicklungen für das geforderte Datenschutzniveau sorgt.

Darüber hinaus wurden bei der Durchführung des Audits folgende „**datenschutzfreundliche**“ Aspekte als besonders erwähnenswert festgestellt:

- Nutzer von kits.system werden durch eine mustergültige Dokumentation des zentralen Systems und eine aussagekräftige Sicherheitskonzeption in der Erstellung der eigenen Sicherheitskonzepte unterstützt.

- Nutzer von kits.system können durch eine aussagekräftige Protokollierung und ein umfassendes Berichtswesen einfach und effektiv Ihrer Verantwortung im Rahmen der Auftragsdatenverarbeitung gemäß § 17 LDSG nachkommen.
- In ihrem Zusammenwirken stellen die technischen und organisatorischen Maßnahmen in kits.system sicher, dass die festgelegten Datenschutz- und -Sicherheitsziele in der gegebenen räumlich verteilten Infrastruktur und bei der Vielzahl der Beteiligten erreicht werden können.

Die Prüfung hat ergeben, dass die Konzeption und der Betrieb der zentralen Komponenten des kommunalen IT-Standards für Kommunen in Schleswig-Holstein sowie das Konzept des eingerichteten Datenschutz- und Sicherheitsmanagementsystem keinen Anlass zu datenschutzrechtlichen Beanstandungen geben. Ferner hat die Prüfung ergeben, dass die notwendigen technischen und organisatorischen Sicherheitsmaßnahmen korrekt implementiert sind.

Kiel, 03. September 2007

(Gutachter: Dr. Martin Meints)