ekom21

Die Zukunft der Verwaltung

BSI - Zertifizierung

nach ISO 27001 auf der Basis von IT-Grundschutz

für die ekom21 – KGRZ Hessen

Ziele & Nutzen

Inhalt

1. Ziele
2. Fragen
3. Vorgehensweise
4. Projekt
5. Ergebnisse und Zertifizierung
6. Nutzen für die Kunden
7. Informationssicherheit
8. Folgemaßnahmen und Re-Zertifizierung

Ziele

- Gewährleistung von angemessener IT-Sicherheit unter Beachtung wirtschaftlicher Grundsätze
- Wettbewerbs- und Qualitätsvorteile bei Vergabeverfahren
- hohe Verfügbarkeit der Anwendungsverfahren
- Gewährleistung der Integrität der Kundendaten
- Gewährleistung der Vertraulichkeit im Umgang mit Kundendaten und den zugehörigen Verfahren

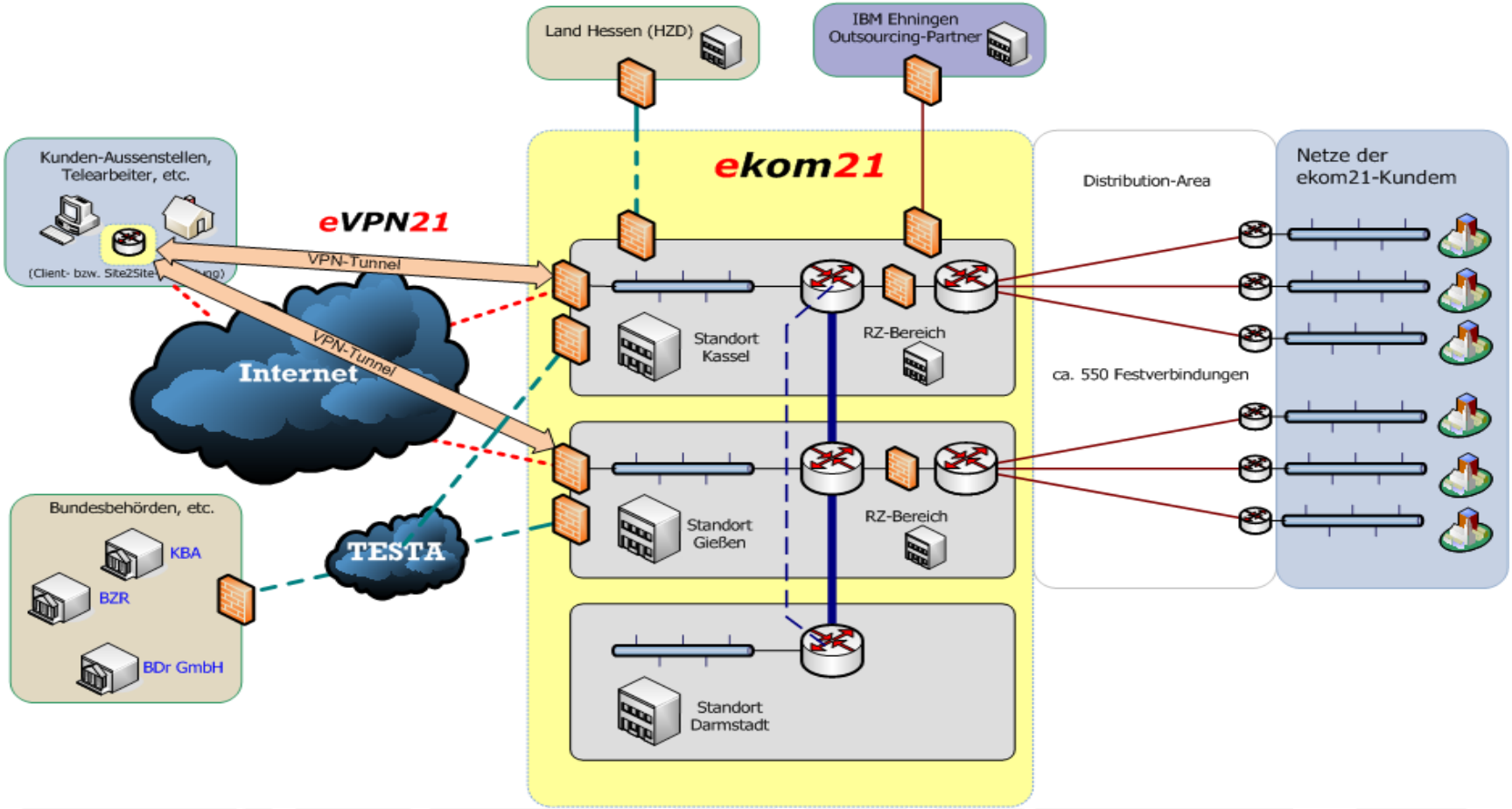
Fragen, die wir uns stellten

- Wie sicher ist die IT der ekom21?
- Welche Gefährdungen und Risiken bestehen?
- Welche Sicherheitsmaßnahmen wurden bereits ergriffen?
- Wie verbessert die ekom21 das bereits erreichte Sicherheitsniveau?
- Wie sicher ist die IT anderer Institutionen, mit denen kooperiert wird?

Vorgehensweise

- Aufbauend auf 4 Jahrzehnten IT-Erfahrung unterzog sich die ekom21 einer grundlegenden Auffrischung zum Thema „Informationssicherheit".
- Stärkung des IT-Sicherheitsbewusstseins aller MitarbeiterInnen durch gezielte Schulungsmaßnahmen.
- Spezielle Trainingseinheiten für besondere Funktionen und Personengruppen.
- Alle bestehenden Schutzeinrichtungen und -vorkehrungen wurden überprüft und nach Bedarf ausgebaut bzw. erweitert.
  - Gebäude und Räume
  - IT-Systeme und Netze
  - Anwendungen
  - Spezifische Funktionen / Personal

Überprüfungsbereich



Maßnahmen

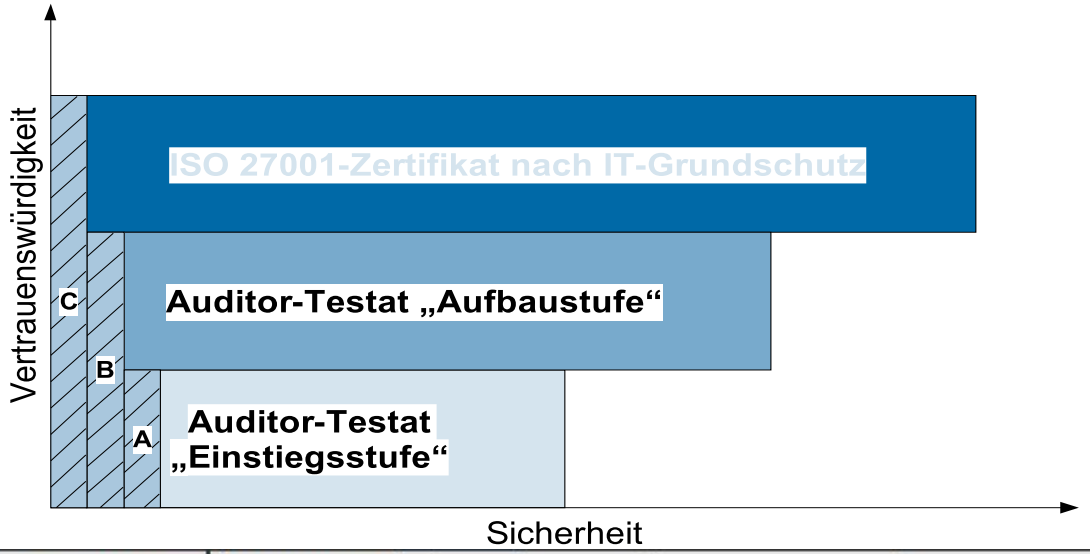
Anpassung der Betriebsorganisation mit Einrichtung eines IT-Sicherheits-Managementteams (ISMT) und eines IT-Sicherheitsbeauftragten.

Projektstart „BSI-Zertifizierung" Anfang 2008. Erreichung der Grundschutz-Zertifizierung im Jahre 2009.

Überarbeitung und z.T. Erneuerung verschiedener organisatorischer Regelwerke, wie z.B.

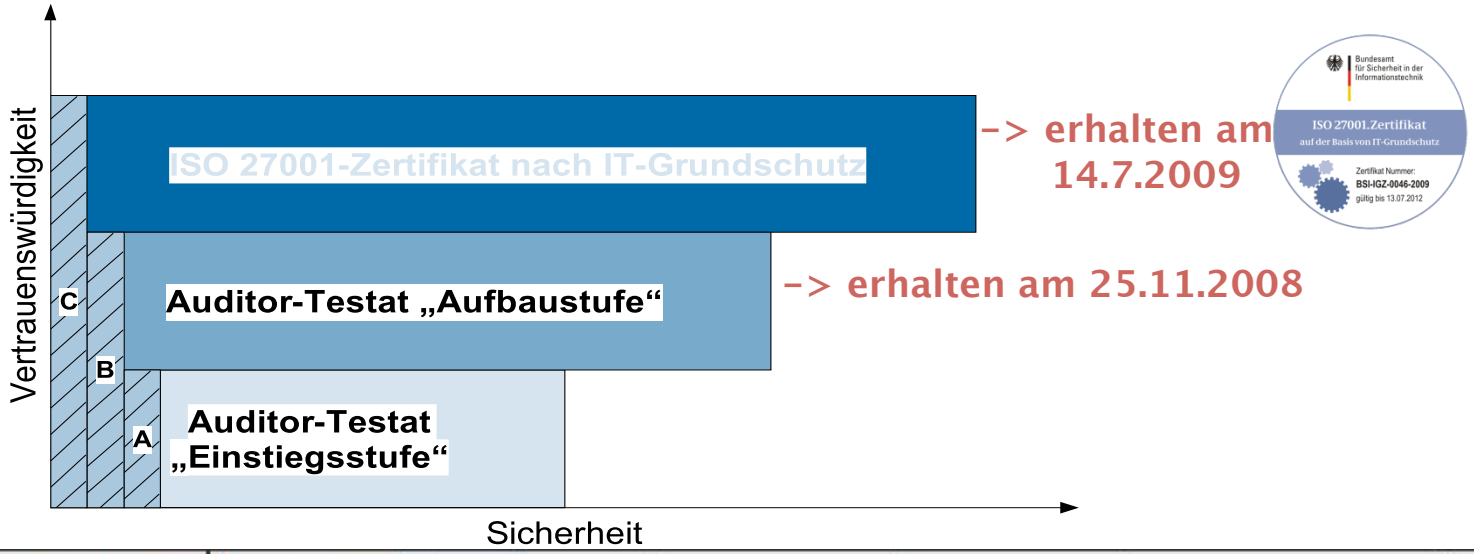
- IT-Sicherheitsleitlinie und
- weiterer Richtlinien für IT-Systeme und Netze sowie zugehöriger
- Handlungsanleitungen (Betriebsorganisation, Datenträgerentsorgung, Durchführung von Bedrohungsanalysen und Schutzbedarfsfeststellungen, Datensicherung, Change-Management, Behandlung von Sicherheitsvorfällen, etc.)

Zertifizierungsstufen nach BSI



Kennzeichnung	Bedeutung
A	Unabdingbare Standardsicherheitsmaßnahmen; die Umsetzung ist für alle drei Stufen der IT-Grundschutz-Qualifizierung erforderlich.
B	Wichtigste Standardsicherheitsmaßnahmen; die Umsetzung ist für die Aufbaustufe und für das Zertifikat erforderlich.
C	Für ein Zertifikat darüber hinaus erforderliche Maßnahmen.
Z	Die Umsetzung dieser zusätzlichen IT-Sicherheitsmaßnahmen sollte zur Steigerung der IT-Sicherheit erfolgen, ist jedoch zur Qualifizierung nach IT-Grundschutz nicht erforderlich.

Zertifizierungsstufen nach BSI



-> erhalten am 14.7.2009

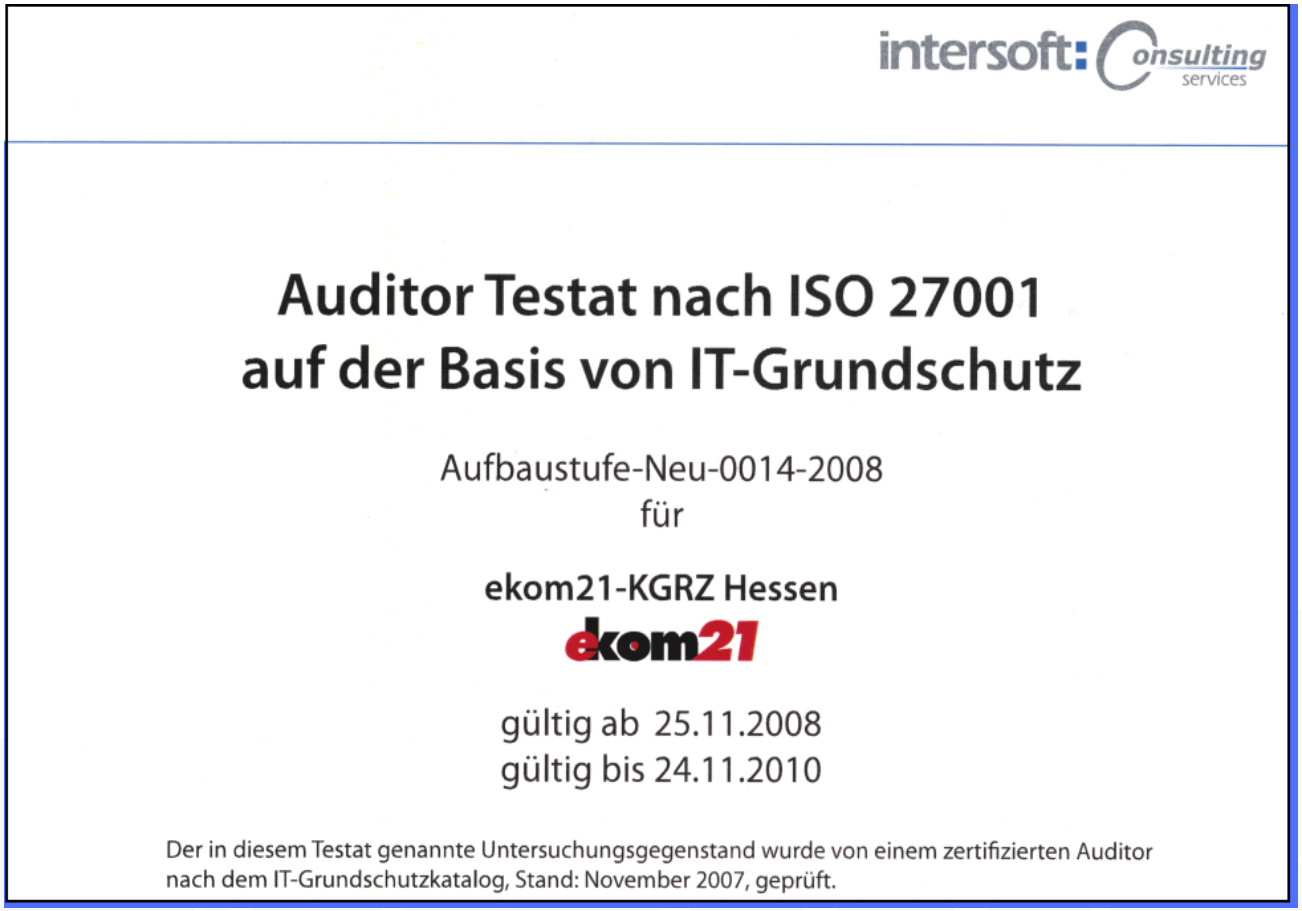
-> erhalten am 25.11.2008

Kennzeichnung	Bedeutung
A	Unabdingbare Standardsicherheitsmaßnahmen; die Umsetzung ist für alle drei Stufen der IT-Grundschutz-Qualifizierung erforderlich.
B	Wichtigste Standardsicherheitsmaßnahmen; die Umsetzung ist für die Aufbaustufe und für das Zertifikat erforderlich.
C	Für ein Zertifikat darüber hinaus erforderliche Maßnahmen.
Z	Die Umsetzung dieser zusätzlichen IT-Sicherheitsmaßnahmen sollte zur Steigerung der IT-Sicherheit erfolgen, ist jedoch zur Qualifizierung nach IT-Grundschutz nicht erforderlich.

Ergebnisse

- Auditorentestat (Aufbaustufe) nach ISO 27001 erreicht am 25.11.2008
- ISO 27001-Zertifikat auf der Basis von IT-Grundschutz erreicht am 14.07.2009

Zertifizierung



intersoft: consulting services

Auditor Testat nach ISO 27001 auf der Basis von IT-Grundschutz

Aufbaustufe-Neu-0014-2008
für

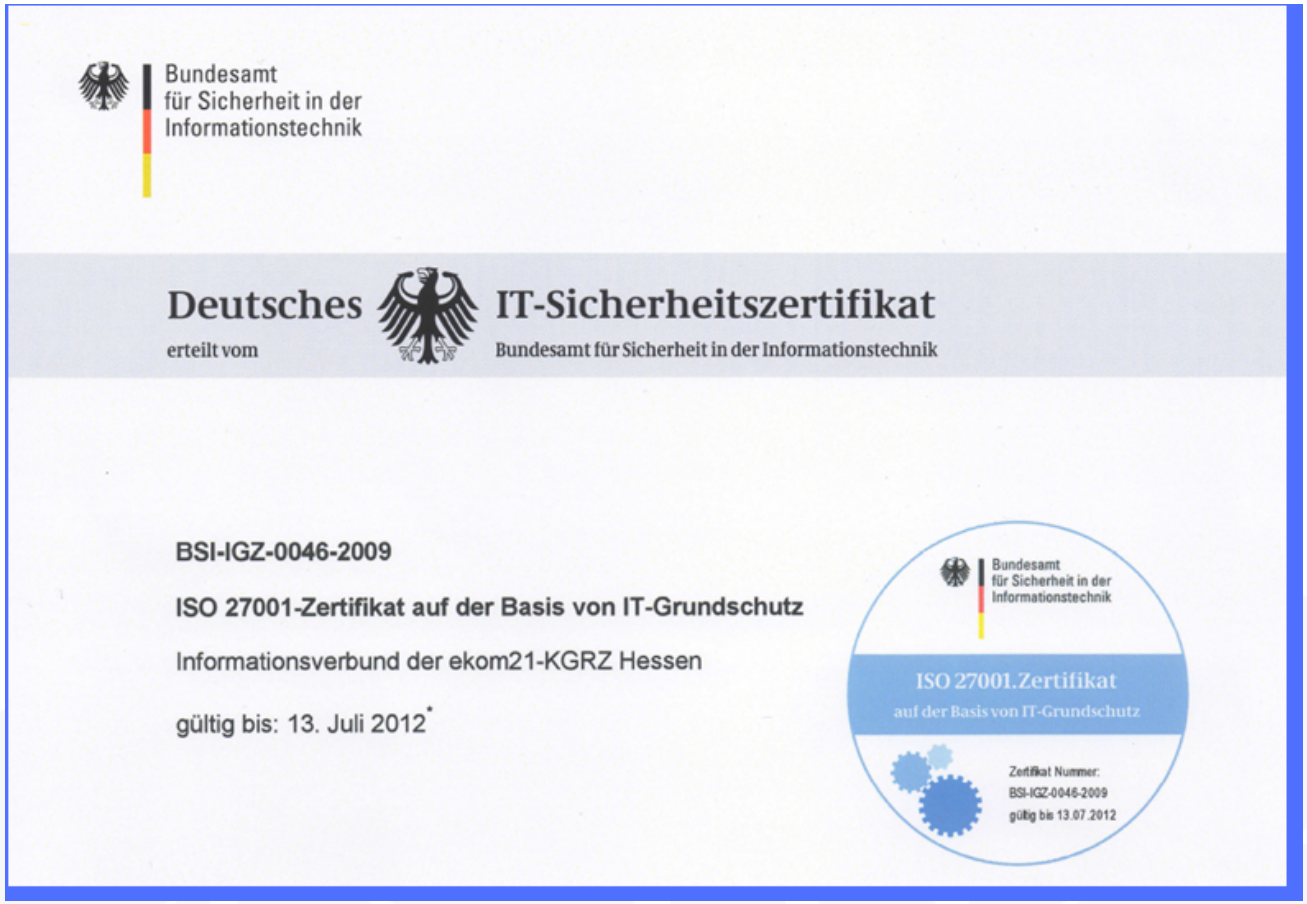
ekom21-KGRZ Hessen

ekom21

gültig ab 25.11.2008
gültig bis 24.11.2010

Der in diesem Testat genannte Untersuchungsgegenstand wurde von einem zertifizierten Auditor nach dem IT-Grundschutzkatalog, Stand: November 2007, geprüft.

Zertifizierung



Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-IGZ-0046-2009

ISO 27001-Zertifikat auf der Basis von IT-Grundschutz

Informationsverbund der ekom21-KGRZ Hessen

gültig bis: 13. Juli 2012*

Bundesamt
für Sicherheit in der
Informationstechnik

ISO 27001.Zertifikat
auf der Basis von IT-Grundschutz

Zertifikat Nummer:
BSI-IGZ-0046-2009
gültig bis 13.07.2012

Nutzen für die Kunden

Ein Höchstmaß an Informationssicherheit
unter besonderer Beachtung der Verfügbarkeit von Verfahren und IT-Systemen und des Schutzes von Vertraulichkeit und Integrität der Kundendaten.

Wirtschaftlich vertretbarer Mehraufwand,
weil hohe Nutzlasten mit großen Stückzahlen bedient werden.

Höhere Dienstleistungsqualität,
da alle Systemkomponenten, Netze und Anwendungen sowie Räume ablauftechnisch und im Hinblick auf Betriebsdokumentation einer Überprüfung unterzogen werden.

Informationssicherheit

- Ein IT-Sicherheitsmanagementteam (ISMT) gewährleistet die Erhaltung und kontinuierliche Verbesserung der Informationssicherheit.
- Aufgaben, Steuerungs- und Kontrollfunktionen des ISMT sind in einer Geschäftsordnung klar geregelt.
- Der IT-Sicherheitsbeauftragte führt mit dem ISMT regelmäßig interne Schwerpunktüberprüfungen durch und berichtet unverzüglich an die Geschäftsführung.
- Im Rahmen des Schulungs- und Awareness-Programms finden jährliche Nachschulungen sowie gezielte Sondermaßnahmen statt,
- um einen hohen Standard in der Informationssicherheit zu festigen.

Folgemaßnahmen und Re-Zertifizierung

Der BSI - Zertifizierungs-Zyklus

Vielen Dank für Ihre Aufmerksamkeit!