Praxisbericht Zertifizierung – Digitale Nachweise in IT-Grundschutz-Zertifizierungsverfahren

IT-Grundschutztag 13. Juni 2012, Bremen

Dr. Sönke Maseberg

datenschutz cert

"Es gilt auch Handschlagqualität in diesem Bereich, wenn man sich mit einer Bank verständigt."

Christian Wulff am 4.1.2012 im ARD-/ZDF-Interview

datenschutz cert

Agenda

- Begriffe
- Ablauf einer IT-Grundschutz-Zertifizierung
- Schichtenmodell
- Diskussion zu Digitalen Nachweisen in IT-Grundschutz-Zertifizierungsverfahren
- Fazit

datenschutz cert

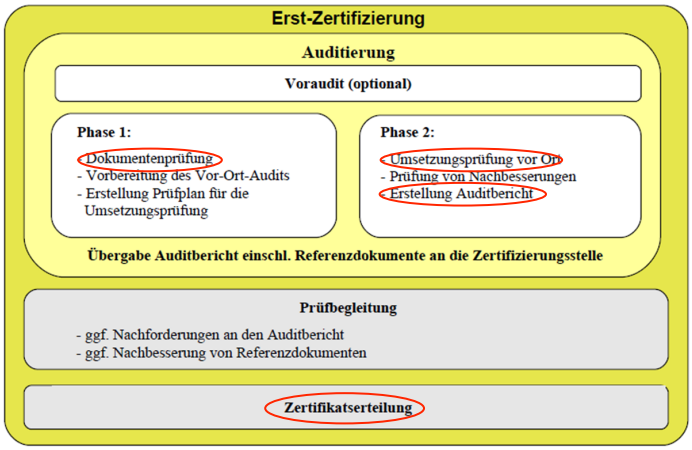
Begriffe

- Integrität (INT)
  - „Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen“
- Authentizität (AUTH)
  - „Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden.“
- Nicht-Abstreitbarkeit/Non-Repudiation (NON)
  - „Hierbei liegt der Schwerpunkt auf der Nachweisbarkeit gegenüber Dritten.“ Stichwort: Willenserklärung.

Quelle: BSI, „IT-Grundschutz-Kataloge, 12. Ergänzungslieferung“, September 2011

datenschutz cert

Ablauf einer IT-Grundschutz-Zertifizierung



datenschutz cert

Quelle: BSI, „Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz, Auditierungsschema“, Version 1.0.

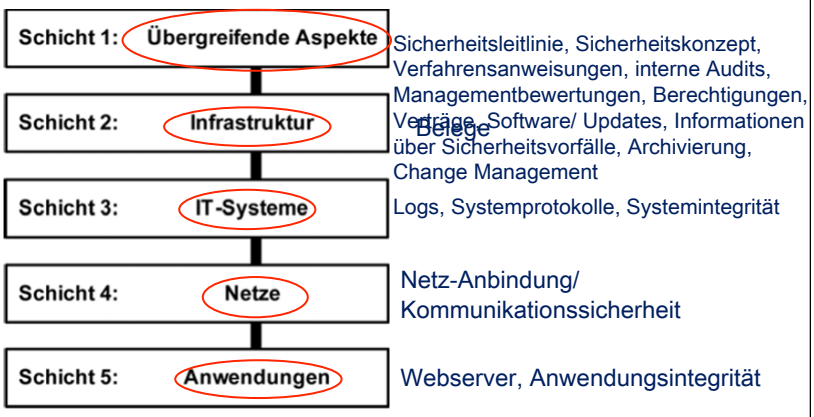
Tätigkeiten eines Auditors

- Prüfmethoden:
  - Dokumentationsprüfung
  - Interviews und Befragungen
  - Inaugenscheinnahme z. B. Begehung, Einsicht in Konfigurationen usw.
  - Durchsicht von Unterlagen, z. B Richtlinien, Anweisungen usw.
  - Analyse und ggf. Verwertung von Unterlagen Dritter, z. B. Protokolle oder Verträge
  - Beobachtung von Aktivitäten und Arbeitsabläufen

datenschutz cert

Quelle: BSI, „Muster Auditreport“. Version 1.0

Schichtenmodell



datenschutz cert

Übersicht Digitale Nachweise in IT-Grundschutz-Zertifizierungsverfahren

- Dokumentenprüfung: Referenzdokumente
- Auditreport
- Zertifikat
- Sicherheitsleitlinie, Sicherheitskonzept, Verfahrensanweisungen, interne Audits, Managementbewertungen, Berechtigungen, Verträge, Software/ Updates, Informationen über Sicherheitsvorfälle, Archivierung, Change Management
- Belege
- Logs, Systemprotokolle, Systemintegrität
- Netz-Anbindung/ Kommunikationssicherheit
- Webserver, Anwendungsintegrität

datenschutz cert

Referenzdokumente

Richtlinien für Informationssicherheit (A.0)
Strukturanalyse (A.1)
Schutzbedarfsfeststellung (A.2)
Modellierung des Informationsverbundes (A.3)
Ergebnis des Basis-Sicherheitschecks (A.4)
Ergänzende Sicherheitsanalyse (A. 5)
Risikoanalyse (A.6)
Risikobehandlungsplan (A.7)

- eindeutige Identifizierbarkeit: Autor/Firma, Name, Versionsnummer, Datum
- sicherer Transport: Chiasmus, PGP, S/MIME, kryptographische Verfahren, Schlüssellänge, Key-Management, richtiger Empfänger

- INT AUTH ~~NON~~

datenschutz cert

Dokumente zum ISMS-Prozess

Sicherheitsleitlinie
Sicherheitskonzept
Verfahrensanweisung
interne Audits
Managementbewertung

- INT AUTH NON

- Papier vs. digital: Versionskontroll-, Dokumenten-Management-Systeme
- Freigabe durch autorisierte Person
- Konsolidieren von Änderungen
- eindeutige Identifizierbarkeit: Unterscheidbarkeit, Änderungsanzeige
- Verfügbarkeit: zweifelsfrei und aktuell
- Urheberschaft: Nachweis der Durchführung

datenschutz cert

Dokumente des ISMS

Berechtigungen
Change Management
Logs/ Systemprotokolle

- INT AUTH NON

- Autorisierung: (sichere) Mail, Fax, Telefon, Bestätigung, Bekanntgabe der autorisierten Personen
- Berechtigungen: Need-to-know, Passwort-Hinterlegen

datenschutz cert

Kommunikationssicherheit

Netz-Anbindung/ Kommunikationssicherheit (Externe, Telearbeiter, Standorte)
Webserver
Informationen über Sicherheitsvorfälle
Software/ Updates
System- und Anwendungsintegrität

- INT AUTH ~~NON~~

- Autorisierung: (sichere) Mail, Fax, Telefon, Bestätigung, Bekanntgabe der autorisierten PersonenZertifikate/ PKI: kryptographische Verfahren, Schlüssellänge, CA, Root CA
- Authentizität: Sicherheitsanker, Abgleich Fingerprint (out-of-band)
- SSL-Zertifikate: CA/Browser-Forum
- Checksummen: Authentizität der Checksumme, unabhängige Berechnung, vertrauenswürdiger Referenzwert (out-of-band)
- Berechtigungen: Need-to-know, Passwort-Hinterlegen

datenschutz cert

Verträge

Belege
Verträge
Archivierung

- INT AUTH NON

- Signaturgesetz/-verordnung: qualifizierte elektronische Signaturen, Anscheinsbeweis, qualifizierte Zeitstempel, Vergänglichkeit: Archivierungskonzepte
- fortgeschrittene Signaturen, e-Mail: „Handschlagqualität“ grundsätzlich zulässig, Nachweis u.U. fraglich, kein Anscheinsbeweis, freie Beweiswürdigung
- eID/nPA: sichere Identifizierung/ Authentisierung, Willenserklärung über qualifizierte elektronische Signatur
- DE-Mail/ePost-Brief: sichere Identifizierung/ Authentisierung, keine qualifizierte elektronische Signatur, freie Beweiswürdigung

datenschutz cert

Dokumente zum Audit-/ Zertifizierungs-verfahren

Auditreport
Zertifikat

- INT AUTH NON

- qualifizierte elektronische Signatur
- IT-Grundschutz-Zertifikat: Graphik, Verifikation über https://www.bsi.bund.de

datenschutz cert

Fazit

- Digitale Nachweise sind wichtige Bestandteile
  - eines ISMS
  - eines Auditierungs- und Zertifizierungsprozesses
- Einblick in Anforderungen von IT-Grundschutz
- Ausblick in Verbesserung der Informationssicherheit

datenschutz cert

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Sönke Maseberg
0421 – 69 66 32 52
smaseberg@datenschutz-cert.de

datenschutz cert