DuD
Datenschutz und Datensicherheit

# Kontrolle und Datensicherheit

Martin Meints

Kontrolle über IT-Systeme ist eine zwingende Voraussetzung, um Datensicherheit erfolgreich umsetzen zu können. Die Umsetzung von Datensicherheit lässt sich aus internationalen Standards zur IT-Sicherheit wie z.B. ISO/IEC 27001 (Information Security Management Systems) und ISO/IEC 17799 ('Code of Practice' der British Standards) ableiten. Grundlage für die erfolgreiche Anwendung dieser Standards ist in jedem Fall die Wahl eines geeigneten Kontroll-Modells bei der Errichtung der IT-Systeme. Um das benötigte Niveau an IT-Sicherheit erreichen zu können, muss es eine geregelte **organisatorische Kontrolle** über alle am System teilnehmenden Personen, wie Nutzer, Administratoren etc. und die **administrative Kontrolle** über die eingesetzte Technik geben. Die administrative Kontrolle soll die Umsetzung festgelegter technischer Sicherheitsmaßnahmen ermöglichen.

Grundsätzlich kann diese Kontrolle **direkt** (z.B. per Weisung innerhalb einer Organisation) oder **indirekt** über Verträge mit geeigneten Security Service Level Agreements (SSLAs) ausgeübt werden.

In der Praxis spielen vor allem vier typische Kontroll-Modelle eine Rolle:

1. Kontrolle über ein System durch seinen Besitzer und alleinigen Nutzer. Dies ist häufig bei Computereinsatz im Privatbereich gegeben. Die in der Einleitung genannten ISO-Normen können mit Einschränkungen zum Management der benötigten IT-Sicherheit verwendet werden. Einschränkungen treten z.B. bezogen auf die Qualität des IT-Sicherheitsmanagements auf, da hier Management, Maßnahmenumsetzung und Kontrolle bei einer Person zusammenlaufen.
2. Zentrale Kontrolle über ein organisationseigenes System durch die Organisation selbst. Technik und Nutzer des Systems (z.B. Mitarbeiter) stehen unter unmittelbarer Kontrolle der Organisation. Die genannten ISO-Normen können angewandt werden.
3. Verteilte Kontrolle über mehrere Beteiligte. In diesem Fall basiert die Sicherheit des Gesamtsystems auf Vertrauen zwischen den Beteiligten.
   In dieser Kategorie können die beteiligten Betreiber unterschiedlich zueinander stehen. Sie können in einem hierarchischen Unterstellungsverhältnis zueinander stehen, z.B. im Fall der Auftragsdatenverarbeitung, oder gleichrangig sein. Beispiele hierfür sind unterschiedliche Betreiberkonstellationen bei Public Key Infrastructure (PKI), wie hierarchische PKI-Systeme oder mittels Gateway verbundene gleichrangige Certificate Authorities (CAs). Die folgenden Abbildungen stellen schematisch diese Verhältnisse dar.

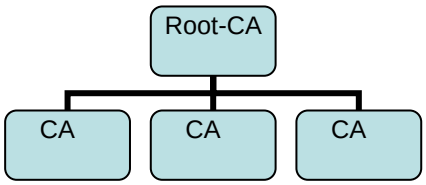


Abb. 1: Hierarchisches PKI-System

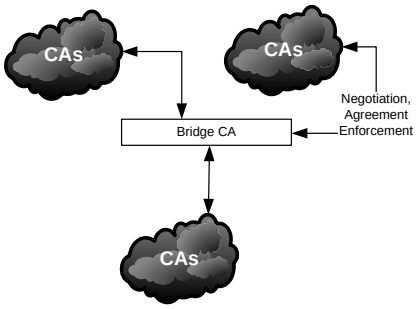


Abb. 2: PKI-System mit gleichrangigen Partnern

   Auch Mischformen sind möglich. Ein Beispiel ist ein automatisiertes Abrufverfahren, bei dem die Stelle, die personenbezogene Daten speichert, besondere Pflichten hat. Noch deutlicher wird diese Mischform, wenn sich diese speichernde Stelle auch noch auf einen externen Dienstleister stützt (Auftragsdatenverarbeitung).
   In all diesen Fällen können die genannten ISO-Normen angewandt werden. Dabei gründet sich das Vertrauen in „Outsourcer“ oder Partner (Mitbetreiber) auf SSLAs, geeignete Auditschemata und bei Bedarf zusätzlich auf vertragliche Sanktionen. Die Sicherheitsanforderungen an und -maßnahmen für das Gesamtsystem sind typischerweise in einem gemeinsamen, für alle Betreiber gültigen Sicherheitskonzept beschrieben. Auch das Sicherheitsmanagement findet koordiniert statt.
4. Verteilte Kontrolle bei allen an dem System Beteiligten (Betreiber und Nutzer) mit unterschiedlichen, unter Umständen widersprüchlichen Sicherheitszielen. Dies wird auch als ein System mit mehrseitigen Sicherheitsanforderungen bezeichnet.
   Für die Umsetzung dieses vierten Modells gibt es bislang nur Forschungsansätze. Bei einem Datenaustausch, z.B. im Zuge von Transaktionen, werden Sicherheitsanforderungen dynamisch und möglicherweise automatisiert ausgehandelt und technisch durchgesetzt. Implementierungen existieren bislang nicht, aber unter anderem mit auf Trusted Computing basierendem Digitalem Rechtemanagement (DRM) gibt es konkrete Ansatzpunkte, wie solche Systeme in Zukunft implementiert werden könnten.

Typischerweise vermeiden Systembetreiber derzeit das vierte Modell, in dem sie die Komplexität durch Vereinheitlichung von Sicherheitsanforderungen, insbesondere auf Nutzerseite, und ein geeignetes technisches Design reduzieren. So erhält man ein System mit verteilter Kontrolle über mehrere Betreiber (Modell 3). Dies kann mit den dazu vorliegenden Erfahrungen und unter Verwendung der oben beschrieben Standards betrieben werden.