security zone newsletter
PLATTFORM FÜR INFORMATIONSSICHERHEIT

Zugriffsberechtigungen im IT-Security Compliance Report

Vorgaben zu den Zugriffskontrollen sind in Deutschland in zahlreichen Gesetzen, Normen und Verordnungen enthalten. Dabei bedeutet IT-Compliance, dass alle relevanten regulatorischen Vorgaben nachweislich eingehalten werden. Für die Zugriffskontrollen kann ein solcher Nachweis im Rahmen des Reporting erstellt werden.

Dr. Aleksandra Sowa

Tätig bei der Deutschen Telekom AG. Leitete u.a. das Horst Görtz Institut für Informationstechnik und war als IT-Revisor in der Finanzdienstleistungsbranche tätig.

Umfragen zu Folge haben drei Treiber deutlichste Auswirkung auf die Sicherheitspraktiken in den Unternehmen: Vermeidung von Schäden, die durch Viren, Trojaner etc. entstehen könnten, Erreichung der Geschäftsziele sowie Übereinstimmung mit Regulierung (sog. Compliance). Es ist jedoch unangefochten die Compliance, die aktuell als der Haupttreiber für das Sicherheitsmanagement gilt.

Welche Zielsetzung hat die Compliance? Generell, sollen die regulatorischen Vorgaben von allen Führungskräften und Mitarbeitern eines Unternehmens eingehalten werden. Dabei sollen die zunehmenden Haftungsrisiken für das Unternehmen und die Mitglieder der Unternehmensführung persönlich (vgl. AktG §91 (2), § 93 (1), GmbHG §43 (1)-(2)) kontrollierbar sein.

Daraus abgeleitet, bezeichnet die IT-Compliance im engeren Sinne einen Zustand, in dem alle für die IT des Unternehmens relevanten, allgemein geltenden regulatorischen Vorgaben nachweislich eingehalten werden. Aus dieser, von Prof. Michael Klotz vorgeschlagener Definition folgt: Der Nachweis über die IT-Compliance ist nicht minder wichtig, als die ordnungsmässige Umsetzung der Anforderungen. Dies gilt insbesondere für die Zugriffskotrollen.

Regulatorisches Rahmenwerk für die Zugriffskontrollen

Der aktuelle Standard ISO/IEC 38500 unterstützt das Management dabei, die Compliance-Verpflichtungen bezüglich Einhaltung von Sicherheitsstandards und Datenschutzgesetzgebung zu erfüllen.

In Deutschland finden sich Vorgaben zur Implementierung von Zugriffskontrollen in zahlreichen Gesetzen, Normen, Verordnungen etc. wieder. Dazu zählen u.a.:

- Bundesdatenschutzgesetz (BDSG) - § 9 Technische und organisatorische Massnahmen, bzw. Anlage zu § 9 Satz 1 BDSG (sog. „8 Gebote des Datenschutzes"),
- Grundsätze Ordnungsmässiger Buchführungssysteme (GoBS) - Tz. 5 Datensicherheit.
- Abgabenordnung (AO) - § 147 Abs. 2 Pflichten zur Aufbewahrung von rechnungslegungsrelavanten Daten.
- Kreditwesengesetz (KWG) - § 25 (gilt für Kreditinstitute),
- Mindestanforderungen an das Risikomanagement (Ma-

Risk) der BaFin – Ziffer AT 7.2 (gelten für Kreditinstitute).

In den gesetzlichen Vorgaben wird oft auf die sog. „gängigen Standards" verwiesen, sobald es um die Konkretisierung der im Gesetzestext allgemein gefassten Vorgaben geht. Hierzu zählen für die Zugriffskontrollen hauptsächlich der ISO 27002 "Information technology – Code of practice for information security management" – insbesondere Tz. A.11 Access Control, sowie der Standard des BSI 100-2 und das Grundschutzhandbuch.

IT-Compliance bezeichnet einen Zustand, in dem alle für die IT des Unternehmens relevanten, allgemein geltenden regulatorischen Vorgaben nachweislich eingehalten werden.

Doch die o.g. Standards haben eine Schwäche: es fehlen darin die Vorgaben zum Monitoring, zur Messung und zu den Metriken für die IT-Kontrollen. (vgl. Bejtlich 2004).

Die Messbarkeit-Defizite in den aktuellen Standards wurden bereits erkannt und werden voraussichtlich durch den angekündigten ISO-Standard 27004 ausgeräumt. Ebenfalls kündige das IT Governance Institut (ITGI) eine "Information Security Program Metrics" an, deren Zielsetzung wird es sein „[to] guide security managers to develop business focused information security program measures and reports" (ITGI 2009).

Metriken für die Zugriffskontrollen – ein Beispiel

Regulatorische Vorgaben, aktuelle Standards und verfügbare Werke zum Thema Sicherheit machen es allerdings jetzt schon möglich, mit Hilfe von Metriken und regelmässigen Bewertungs- und Beurteilungsrunden, einen Nachweis über die IT-Compliance zu erstellen.

Im ersten Schritt werden Metriken für die relevanten (quantitativ messbaren) Aspekte der Zugriffskontrollen definiert. Im Folgenden wurden einige, von Herrmann (2007) adaptierten, Beispiele für die Metriken aufgeführt, die der Beurteilung und Bewertung von Ordnungsmässigkeit und Compliance von Zugriffsberechtigungen dienen können.

1. Anteil von inaktiven Benutzerkonten, die in der Berichtsperiode gemäss Vorgaben der Security Policy deaktiviert wurden
2. Anteil der Benutzer, die aus der Organisation ausgeschieden sind und dessen Benutzerkonten nicht mehr benötigt werden, und in der Berichtsperiode gemäss Vorgaben der Security Policy deaktiviert wurden.
3. Anteil der Arbeitsplätze, die mit einer automatischen Log-out bzw. Session Time-out Funktionalität ausgestattet sind **
4. Anteil der Benutzerkonten, die in der Berichtsperiode im Hinblick auf die Richtigkeit der aktuellen Zugriffsrechte und Privilegien überprüft wurden.**
5. Anteil der Systeme und Applikationen, die Zugriffsrechte und Privilegien nach dem Prinzip der rollenbasierten Zugriffskontrollen umgesetzt haben.*
6. Anteil der mobilen und privaten Geräte, die einer Prüfung und Konfiguration unterzogen wurden, um Zugriff zur IT und zu bestimmten Informationen zu erhalten.*
7. Anzahl der Versuche, bei denen ein - erfolgreicher oder erfolgloser - administrativer Zugriff von ausserhalb des gültigen Wartungsfenster (gültige Wartungsumgebung) erfolgte.*

[...]

(*) Für kritische, wesentliche und normale Bestände.

(**) Gegliedert nach Informationsklassen, z.B. streng vertraulich, vertraulich, intern, öffentlich.

Vollständige Metriken-Liste kann den folgenden Quellen entnommen werden: Hermann (2007); Sowa (2010).

Die o.g. Metriken adressieren aktuelle regulatorische Vorgaben. Sie beziehen sich zugleich auf verschiedene Aspekte der Zugriffskontrollen. So umfasst beispielsweise die Metrik Nr. 6 die Themen tragbare PCs, mobile Arbeitsplätze, Telearbeit und adressiert - in Abhängigkeit von den zu verarbeitenden Daten - u.a. in dem BDSG, KWG und den MaRisk, GoBS etc.

Messen, Bewerten, Dokumentieren – in drei Schritten zum IT-Compliance Report

Ein weiterer Schritt besteht darin, die für das Unternehmen relevanten Metriken auszuwählen, für diese Auswahl angemessene Zielwerte festzulegen (in Prozent oder als Punktezahl), die Messungen zu veranlassen und die Messergebnisse zu dokumentieren, wie im Beispiel für Metrik Nr. 2 dargestellt:

Definition der Metrik: Anteil der Benutzer, die aus der Organisation ausgeschieden sind und dessen Benutzerkonten nicht mehr benötigt werden, sowie in der Berichtsperiode gemäss Vorgaben der Security Policy deaktiviert wurden.

Zielwert: 100% (aller ausgeschiedenen Benutzer)

Beobachteter Wert: 75%

GAP: 25 Prozentpunkte

Analyse der Ursachen: Veraltete HR-Systeme- und Rechtevergabe–Prozesse erschweren und verlangsamen die Kommunikation der Deaktivierungsaufträge an die Benutzerverwaltung.

Ergebnis: 5 Punkte (von max. 10)

Um eine quantitatives Ergebnis für jede Metrik zu erhalten, muss vorab eine Bewertungsformel erstellt werden, wie z.B. die folgende:

Ordnungsmässigkeit und Wirksamkeit von Zugriffskontrollen wird regelmässig beurteilt und bewertet.

Abweichung <0; 15> Prozentpunkte = 10 Punkte

Abweichung (15;35) Prozentpunkte = 5 Punkte

Abweichung <35;100> Prozentpunkte = 0 Punkte

Summiert über alle relevanten Metriken, ergibt die Bewertung ein Gesamtergebnis für die Zugriffskontrollen – eine Punktezahl – die im Report veröffentlicht werden kann (vgl. Abbildung).

Regelmässige Prüfung von Verbesserungen

Eine regelmässige Beurteilung der Messergebnisse soll nicht nur die Feststellung und Dokumentation des Status Quo ermöglichen. Ebenfalls eine Definition des Verbesserungspotentials, der Massnahmen zur Schliessung der „GAP" zwischen dem Status Quo und dem angestrebten Zustand, sowie eine Dokumentation der Verbesserungen selbst, sind wichtige Ergebnisse der Metrik-Auswertung.

Die Bewertungsergebnisse sind erst dann für das IT-Security Compliance Report von Nutzen, wenn sie eine bestimmte Kontinuität bzw. Regelmässigkeit aufweisen, also z.B. in einem Quartals-Rythmus erstellt werden, wie in der Graphik dargestellt.

Fazit

Vergleichbare Metriken lassen sich auch für die anderen Teilaspekte der Informationssicherheit bzw. andere IT-Kontrollen aus den gesetzlichen und regulatorischen Vorgaben ableiten. So hat Herrmann (2007) ca. 300 Metriken vorgeschlagen, die u.a. für logical access controls, data authentication, non-repudiation, encryption, cryptographic support, Identification and authentication oder privacy verwendet werden können. Die Metriken können sowohl für die Bewertung einzelner Komponenten als auch des gesamten Informationssicherheitssystems eingesetzt werden.

Empfehlenswert ist eine Ergänzung des Reports um eine Übersicht der geplanten und umgesetzten Massnahmen, mit welchen die identifizierten Lücken geschlossen werden sollen bzw. worden sind.

Quellen

Bejtlich, R. (20044: *The Tao of Network Security Monitoring. Beyond Intrusion Detection.* Amsterdam: Addison-Wesley.

Herrmann, D. S. (2007): *Complete Guide to Security and Privacy Metrics. Measuring Regulatory Compliance, Operational Resilience, and ROI*. New York: Auerbach Publications.

IT Governance Insitute (ITGI 2009): Current Projects - Information Security Program Metrics. (http://www.isaca.org/Content/Content-Groups/Research1/Projects/Research_Current_Projects.htm#Project16)

Sowa, A. (2010): "Access Control Controls. Metrik für den IT-Security-Compliance-Report am Beispiel von Zugriffsberechtigungen". In: <*kes*> 1/2010, 12-7.