**Klausurfragen Folie 9: IT-Sicherheits- und Risikomanagement**

**Welche typischen Versäumnisse gibt es im Unternehmen im Hinblick auf die IT-Sicherheit?**

Typische Versäumnisse sind eine unzureichende IT-Sicherheitsstrategie, schlechte Konfiguration von IT-Systemen, unsicher Vernetzung und Internetanbindung, Nichtbeachtung von Sicherheitserfordernisse (z.B. aus Bequemlichkeit), schlechte Wartung von IT-Systemen, sorgloser Umgang mit Passwörtern, mangelhafter Schutz vor Einbrechern und Elementarschäden und die Nichtnutzung vorhandener Sicherheitsmechanismen.

**Welche personellen, organisatorischen, technischen und baulichen Maßnahmen können ergriffen werden?**

Personelle und organisatorische Sicherheitsmaßnahmen sind Protokollierung, geprüftes und aktuelles Organisationshandbuch, Mehr-Augen-Prinzip, Schulung, Beachtung von Interessens- und Befugniskonflikten. Technische Sicherheitsmaßnahmen sind Zugriffskontrollen, Verschlüsselung, Digitale Unterschriften, Integritätssicherung, Authentisierung, Routingkontrolle. Bauliche Sicherheitsmaßnahmen dagegen sind Zugangskontrolle, Feuer- & Wasserschutz, allgemeine Katastrophenplanung, Ausweichlösungen, Überspannungsschutz, Evakuierungspläne.

**Welche Aufgaben hat das strategische, taktische und operative IT-Management?**

Das strategische IT-Management hat als Aufgaben die Unterstützung durch das Top-Management, Visionen, Ziele, Strategien, Politiken, Kompetenzen und Verantwortlichkeiten, Sicherheitsbewusstsein, Abgleich mit Unternehmenszielen und Abgleich mit Informationspolitik. Zu den Aufgaben des taktischen IT-Managements zählen Risikomanagement, Maßnahmenidentifikation und -aufteilung, Implementierung von Maßnahmen, Notfallplanung, Schulungen, Konfigurationsmanagement und Änderungsmanagement. Zu den Aufgaben des operativen IT-Managements zählen Realisierung der Maßnahmen (Betrieb), Monitoring, Reaktion auf Zwischenfälle, Konfigurationsmanagement und Änderungsmanagement.

**Beschreiben Sie den IT-Sicherheitsprozess.**

Zunächst wird der IT-Sicherheitsprozess initiiert. Dazu gehört die Erstellung einer IT-Sicherheitsrichtlinie sowie die Einrichtung des IT-Sicherheitsmanagements. Danach kommt es zur Erstellung eines IT-Sicherheitskonzepts. Danach erfolgt die Umsetzung. Dazu zählt die Realisierung fehlender Maßnahmen in der Infrastruktur, Organisation, Personal, Technik, Kommunikation und Notfallversorge. Dazu zählen insbesondere Sensibilisierung für IT-Sicherheit und Schulung zur IT-Sicherheit. Als letztes kommt es zur Aufrechterhaltung im laufenden Betrieb. Während des laufenden Betriebs können Anpassungen vollzogen und ein neues bzw. überarbeitetes IT-Sicherheitskonzept erstellt werden.

**Erstellen Sie eine Sicherheitsscheckliste für folgendes IT-Objekt (z.B. PC…)**

**Wie definiert sich ein Risiko/ eine Chance?**

Ein Risiko setzt sich aus den Ursachen (Problemen/Ereignissen), der Wahrscheinlichkeit ihres Auftretens und der positiven oder negativen Auswirkung beim Auftreten der Probleme zusammen. Die Reduzierung von Risiken bedeutet Aufwände, die betrieben werden müssen, um ein Risiko mit negativen Auswirkungen zu mindern.

**Was ist ein Risikobaum?**

**Warum ist Sicherheitsmanagement/Risikomanagement aus Sicht der GF so wichtig?**

Es ist aus Sicht der GF wichtig, da gesetzliche und Corporate Governance Vorschriften eingehalten werden müssen. Dabei müssen Interessen der verschiedenen Gruppen (z.B. Stakeholder) gewahrt werden und dies soll zielgerichtete Zusammenarbeit mit der Geschäftsleitung sichern. Des Weiteren soll Risikomanagement die Fahrlässigkeit im Handeln reduzieren und Sorgfaltspflicht in Produkten und Prozessen erhöhen. Außerdem soll es die Einhaltung von Normen und Regeln (Compliance) sicherstellen, da bei der jährlichen Unternehmensprüfung durch Wirtschaftsprüfer ein großes Augenmerk auf IT gelegt wird. Auch soll Risikomanagement die Leistungen von Service Providern überprüfen. Das IT-Risikomanagement kommt dann zum Tragen, wenn ein Schadensfall eingetroffen ist (meist unerwartet).

**Welche Möglichkeiten des Umgangs mit IT-Risiken gibt es im Unternehmen?**

Bei dem Umgang mit Risiken kann es zu 4 Strategien kommen: Vermeidung, Minderung, Übertragung und Risikoakzeptanz. Bei der Vermeidung versucht man, durch die Änderung der IT-Prozesse bzw. der eingesetzten IT-Produkte und IT-Ressourcen das Risiko überhaupt auszuschließen, z. B. die mit dem Risiko behafteten Aktivitäten/Personen durch andere Aktivitäten/Personen ohne Risiko zu ersetzen. Bei der Minderung wird in erster Linie durch geeignete Gegenmaßnahmen versucht, die Eintrittswahrscheinlichkeit des Risikos auf ein akzeptables Maß zu reduzieren, z. B. durch Anpassungen der IT-Prozesse, Veränderungen der Projektaktivitäten, mehr Ressourcen und ähnliche Optionen. Als Prinzip gilt: Wenn die Eintrittswahrscheinlichkeit nicht gemindert werden kann, muss man versuchen, die Auswirkungen zu reduzieren. Bei der Risikoübertragung wird das Risiko durch Abschluss einer entsprechenden Versicherung, durch Vertragsklauseln (SLAs für IT-Systeme) oder durch ein Kompensationsgeschäft abgewälzt oder ausgeglichen. Damit wird allerdings das Risiko selbst nicht beseitigt. Vielmehr werden die Folgen des Risikos und somit die Verantwortung für die Risikobewältigung an einen Dritten übertragen. Bei der Risikoakzeptanz geht es darum, dass IT-Risiken, deren Schadensausmaß und Eintrittswahrscheinlichkeit gering sind, akzeptiert werden können.

**Welche Bedeutung hat IS027001 bzw. BSI-Sicherheitsstandard?**

Die internationale Norm ISO/IEC 27001 spezifiziert die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung des Kontexts einer Organisation. Darüber hinaus beinhaltet die Norm Anforderungen für die Beurteilung und Behandlung von Informationssicherheitsrisiken entsprechend den individuellen Bedürfnissen der Organisation. (wikipedia.org). BSI-Standards enthalten Empfehlungen des BSI zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen mit Bezug zur Informationssicherheit. Das BSI greift dabei Themenbereiche auf, die von grundsätzlicher Bedeutung für die Informationssicherheit in Behörden oder Unternehmen sind und für die sich national oder international sinnvolle und zweckmäßige Herangehensweisen etabliert haben (bsi.bund.de)

**Ist IT-Sicherheit kostenlos zu haben?**

**Nennen Sie vier typische IT-Risikoklassen und erläutern Sie diese kurz?**

Vier typische Risikoklassen sind Hardwarerisiken, Lizenzrisiken, Sicherheitsrisiken und IT-Prozessrisiken. Zu den Hardwarerisiken zählen beispielsweise Hardwaredefekte oder Diebstahl von Datenträgern. Zu den Lizenzrisiken zählen u.a. die Überlizenzierung und die Unterlizenzierung (führt zu Strafzahlungen). Zu Sicherheitsrisiken zählen u.a. Datenverlust, Datendiebstahl oder Virenbefall. Zu den IT-Prozessrisiken gehören u.a. fehlende Prozessdokumentation oder Risiken im Umfeld des Outsourcings von IT.

**Welche Ziele werden durch ein geplantes, organisiertes IT-Risikomanagement verfolgt?**

Ziele sind Vorbeugender Schutz gegen drohende Risiken, Minimierung der Auswirkungen von Schadens-, Notfalls- oder Krisenfällen, Schutz vor Schadensersatz und Vermeidung von persönlichen zivil- und strafrechtlichen Haftungen, Erhöhung der Wettbewerbsvorteile und Vermeidung von Imageverlusten, zielgerichtete und intensive Nutzung der Potenziale und Chancen des Unternehmens und Sicherheit bei externen Prüfungen durch die Aufsichtsbehörde und andere Organisationen.

**Zeigen Sie mit IT-Objekte die IT-Risiken auf.**

**Gegeben ist folgende IT-Risikomatrix. Interpretieren Sie die Inhalte.**

**Wie kann der Umgang mit Risiken erfolgen?**

Bei dem Umgang mit Risiken kann es zu 4 Strategien kommen: Vermeidung, Minderung, Übertragung und Risikoakzeptanz. Bei der Vermeidung versucht man, durch die Änderung der IT-Prozesse bzw. der eingesetzten IT-Produkte und IT-Ressourcen das Risiko überhaupt auszuschließen, z. B. die mit dem Risiko behafteten Aktivitäten/Personen durch andere Aktivitäten/Personen ohne Risiko zu ersetzen. Bei der Minderung wird in erster Linie durch geeignete Gegenmaßnahmen versucht, die Eintrittswahrscheinlichkeit des Risikos auf ein akzeptables Maß zu reduzieren, z. B. durch Anpassungen der IT-Prozesse, Veränderungen der Projektaktivitäten, mehr Ressourcen und ähnliche Optionen. Als Prinzip gilt: Wenn die Eintrittswahrscheinlichkeit nicht gemindert werden kann, muss man versuchen, die Auswirkungen zu reduzieren. Bei der Risikoübertragung wird das Risiko durch Abschluss einer entsprechenden Versicherung, durch Vertragsklauseln (SLAs für IT-Systeme) oder durch ein Kompensationsgeschäft abgewälzt oder ausgeglichen. Damit wird allerdings das Risiko selbst nicht beseitigt. Vielmehr werden die Folgen des Risikos und somit die Verantwortung für die Risikobewältigung an einen Dritten übertragen. Bei der Risikoakzeptanz geht es darum, dass IT-Risiken, deren Schadensausmaß und Eintrittswahrscheinlichkeit gering sind, akzeptiert werden können.