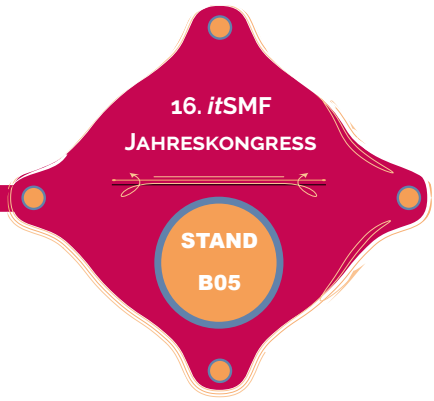

Risikoanalyse bei der Umsetzung der IT-Sicherheitsstandards

TEXT KRZYSZTOF PASCHKE

RISIKOBETRACHTUNG – VON DER SEEFAHRT ZUR ISO-NORM

Die Geschichte der Risikobetrachtung ist genauso spannend wie alt. Die Herkunft des Wortes „**Risiko**" ist nicht eindeutig belegbar. Als noch nicht ersichtlich war ob die Erde eine Scheibe oder kugelförmig ist, bezeichneten die Spanier und Portugiesen ihre Entdeckungsreisen als „**risco**" (=Klippe). Die Schifffahrt war ohne Seekarten ein gewagtes Unternehmen. Seit dem haben viele bekannte Mathematiker und Philosophen wie Fibonacci, Geralamo Cardano, Blaise Pascal, Pierre de Fermat und Abraham de Moivre, um nur einige zu erwähnen, sich mit dem Thema Risiko auseinander gesetzt. Im Jahre 1994 entwickelten die Mitarbeiter der Investmentbank Morgan Stanley das Konzept **„Value at Risk"**, eine der meist verbreiteten statistischen Methoden für die quantitative Bestimmung des Risikos. So viel zu der Geschichte der Risikobetrachtung. Bei der Auseinandersetzung mit den etablierten IT-Sicherheitsstandards, wie z.B. der ISO-Reihe 270xx, ISO/IEC 22301 und der BSI-Standards stellen wir fest, dass die Risikoanalyse eine Grundvoraussetzung für ihre erfolgreiche Planung und Umsetzung darstellt.

RISIKOMANAGEMENT

Unter Unternehmensrisiken sind alle negativen Ereignisse zu verstehen, die die Leistungserstellung (Wertschöpfung) und die Erreichung der Unternehmensziele verhindern sowie die bestehenden Unternehmenswerte reduzieren können. Ein positiver Ausgang eines Ereignisses wird als Chance bezeichnet. Ein (**R**)isiko ist das Produkt der (**E**)intrittswahrscheinlichkeit und der (**A**)uswirkung und kann mit einer einfachen mathematischen Grundformel dargestellt werden: **R = E * A.** Koordinierte Aktivitäten zur Leitung und Kontrolle einer Organisation in Bezug auf Risiken bezeichnet man als Risikomanagement. Die genaue Methodik des Risikomanagements gibt die Norm ISO 31000 vor. Im Bereich IT oder genau gesagt IT-Sicherheitsmanagement wird das Risikomanagement vor allem nach der ISO/IEC 27005 und dem BSI-Standard 100-3 verwendet, wobei die ISO/IEC 27005 von der Norm 31000 abgeleitet ist. Bei dem BSI-Standard 100-3 handelt es sich um eine Risikoanalyse auf der Basis von BSI IT-Grundschutz (nationaler Standard). Bei der Risikoanalyse kann zwischen quantitativen und qualitativen Methoden unterschieden werden. Die quantitative Risikoanalyse wird mit Hilfe von mathematischen Formeln durchgeführt und liefert numerische Werte. Die sogenannten stochastischen Methoden der Risikoanalyse, wie z.B. „**Value at Risk**" oder „**Monte-Carlo Simulation**", die vor allem bei Banken und Versicherungen im Finanzwesen eingesetzt werden, werden hier nicht behandelt. Bei der qualitativen Risikoanalyse wird mit subjektiven Schätzwerten, die auf Erfahrungswerten und anderen Informationen basieren, wie z.B.: Herstellerangaben einer IT-Komponente gearbeitet. Die qualitative Analyse und Bewertung der Risiken ist die meistgenutzte Methode im IT-Sicherheitsmanagement. Der Risikomanagementprozess ist in der ISO-Welt einheitlich und wird in der Regel in zwei Schritten durchgeführt: Risikobeurteilung und Risikobehandlung. Bei einer prozessorientierten Risikobeurteilung können einem Prozess ein oder mehrere Risiken zugeordnet werden, die zu einem Ausfall führen oder ihn negativ beeinträchtigen können. Risiken wie Ausfall der Klimaanlage, Brand, Sabotage, Pandemie etc. sind prozessunabhängig und können zum gleichzeitigen Ausfall mehrerer Prozessen führen. Die Beurteilung der Risiken wird in drei Schritten durchgeführt: Identifikation, Analyse und Bewertung.

RISIKOIDENTIFIKATION

Während der Identifikation werden die Risiken aufgedeckt und geprüft. Sie können zur strukturierten Analyse, Bewertung und Zuordnung nach individuellen Kriterien in Risikogruppen zusammengefasst werden. Die Aufdeckung der Risiken kann durch den Einsatz unterschiedlicher Techniken durchgeführt werden, u.a.:

- Walkthroughs
- Workshops
- Interviews/Fragebögen/Checklisten
- Self-Assessment
- Auswertung der vorhandenen IT-Dokumentation

In der Praxis werden oft mehrere der genannten Techniken miteinander kombiniert. Bei der Risikoidentifikation und –bewertung sollten generell folgende Fragen beantwortet werden:

- Was kann schief gehen?
- Wie kann es passieren?
- Wann kann es passieren?
- Was ist die Ursache?
- Wie hoch ist der potentielle Schaden?
- Wie kann dem vorgebeugt werden?
- Wie können bereits eingetretene Risiken in Zukunft verhindert werden?

RISIKOANALYSE UND BEWERTUNG

Ergebnisse der Analyse und Bewertung sind qualitative und quantitative Aussagen zur Eintrittswahrscheinlichkeit, Auswirkung, Gewichtung und möglichen Höhe eines Schadens. Ein Risiko ist das Produkt der Eintrittswahrscheinlichkeit und der Auswirkung. Die Eintrittswahrscheinlichkeit ist die geschätzte Wahrscheinlichkeit, in der ein Ereignis in einem bestimmten Zeitraum in Zukunft auftreten kann. Sie kann mit Hilfe von statistischen Werten ermittelt werden. Voraussetzung dafür ist die Verfügbarkeit von entsprechenden Daten (quantitative Datengrundlage). Da genannte Daten nicht immer zur Verfügung stehen, kann eine qualitative Einschätzung der Eintrittswahrscheinlichkeit bestimmt werden. Sie kann prozentual oder in Form einer Bewertung dargestellt werden (z.B. Notendarstellung oder Scoring-System). Die Auswirkung ist der Wertverlust oder Schaden, der beim Eintritt eines Risikos vermutet wird. Bei der Bewertung der Auswirkung werden in der Regel folgende Schadensszenarien explizit betrachtet: Finanzielle Auswirkung, Imageschaden, Beeinträchtigung der Aufgabenerfüllung, Beeinträchtigung der persönlichen Unversehrtheit und Beeinträchtigung des informationellen Selbstbestimmungsrechts. Einige Branchen haben strikte Vorgaben bestimmte Schadensszenarien zu berücksichtigen.

Die Netzbetreiber sind verpflichtet gemäß dem IT-Sicherheitskatalog bei der Risikoanalyse folgende Kriterien zu bewerten: Beeinträchtigung der Versorgungssicherheit, Einschränkung des Energieflusses, betroffener Bevölkerungsanteil, Gefährdung für Leib und Leben, Auswirkung auf weitere Infrastrukturen, Gefährdung für Datensicherheit und Datenschutz und finanzielle Auswirkung. Die Ergebnisse werden in der Regel in einer Risiko-Bewertungs-Matrix dargestellt. Die einzelnen Zahlen in der Matrix positionieren die erfassten Risiken und geben einen Hinweis auf ihre Gewichtung:

- Mäßige Risiken (Grün) – Die hier klassifizierten Risiken werden im Tagesgeschäft gelöst. Es sind keine besonderen Maßnahmen notwendig.
- Wichtige Risiken (Gelb) – Sie gefährden nicht direkt den Fortbestand des Unternehmens. Die hier klassifizierten Risiken können die Aufgabenerfüllung signifikant beeinträchtigen und sollten u.U. durch geeignete Maßnahmen ausgeschlossen oder minimiert werden.
- Kritische Risiken (Rot) – Sie können für das Unternehmen existentiell bedrohlich sein. Die hier klassifizierten Risiken müssen durch geeignete Maßnahmen behandelt werden.

IT-Sicherheit & Notfallmanagement – Ein Integriertes Managementsystem

- IT-Grundschutz (BSI 100-2)
- (IT-)Notfallmanagement (BSI 100-4)
- IT-Risikoanalyse (BSI 100-3)
- ISMS (ISO 27001)
- IT-Risikoanalyse (ISO 27005)
- TR-RESISCAN (BSI-TR 03138)
- Datenschutz (BDSG, LDSG)
- Verfahrensdokumentation und IKS
- ISO (9001, 14001, 50001, …)

GRC Partner ▪ Schauenburgerstraße 116 ▪ 24118 Kiel ▪ Tel.: 0431 53033 990 ▪ info@grc-partner.de ▪ **grc-partner.de**

RISIKOBEHANDLUNG

Auf die identifizierten und bewerteten Risiken sollte ein Unternehmen oder eine Behörde angemessen mit Maßnahmen reagieren. Dabei spielen die sogenannte Risikobereitschaft (Risikoappetit) und die Risikotoleranz eine entscheidende Rolle. Beide Begriffe beschreiben eine Grenze, ab der die festgestellten Risiken aus Sicht einer Organisation nicht mehr tolerierbar sind und auf jeden Fall behandelt werden müssen. Für die Risikobehandlung stehen vier Optionen zur Verfügung:

- **Risikoakzeptanz** – Das Risiko und seine Folgen werden ohne Einleitung von irgendwelchen vorbeugenden Maßnahmen akzeptiert.
- **Risikovermeidung** – Durch eine gezielte Änderung der Rahmenbedingungen, wie z.B.: Aktivitäten, Abläufe etc., eines kritischen Prozesses oder einer Ressource kann das Risiko nicht mehr auftreten.
- **Risikotransfer** – Durch eine geplante Übertragung des Risikos auf externe Dienstleister oder Versicherer wird das Risiko bzw. die Risikofolgen minimiert. Mit dem Abschluss einer Versicherung können direkte finanzielle Folgen ganz oder teilweise kompensiert werden. Indirekte Schäden, wie z.B. aufgrund von Nichteinhaltung der Verträge und damit verbundenem Imageverlust können u.U. nicht wieder gut gemacht werden.
- **Risikoreduktion** – Durch gezielte organisatorische und technische Maßnahmen wird die Eintrittswahrscheinlichkeit und Auswirkung eines Risikos weitgehend reduziert.

Welche der genannten Risikobehandlungsmethoden angewendet werden sollen, entscheidet, prüft und genehmigt eine verantwortliche Person, z.B. der Abteilungsleiter, der Prozessverantwortliche oder ein Mitglied der Geschäftsleitung. Empfehlenswert ist die Entwicklung von klaren Kriterien für die Risikoakzeptanz. Eines der Kriterien können die möglichen Folgekosten des Risikos sein. Bei der Wahl einer der genannten Optionen müssen unterschiedliche Aspekte berücksichtigt werden, u.a.:

- Unternehmensweit geltende Gesetze und Regelungen
- Risikoappetit und -toleranz
- Verträge mit Geschäftspartnern
- Kosten-Nutzen-Analyse
- Organisatorische und technische Gegebenheiten
- Politische Gegebenheiten
- Kompetenzen und Verfügbarkeit der Mitarbeiter
- Wirtschaftliche Lage des Unternehmens

Gemäß dem P-D-C-A-Zyklus sollte die Risikoanalyse periodisch, z.B. jährlich wiederholt werden. Falls wesentliche organisatorische oder technische Änderungen im Unternehmen stattgefunden haben, sollte die Risikoanalyse für betroffene Bereiche und Prozesse außerhalb des P-D-C-A-Zyklus durchgeführt werden.

In beiden Fällen ist die Überprüfung des Geltungsbereiches (Scopes) des Informationssicherheitsmanagementsystems (ISMS) zu berücksichtigen.

LITERATUR:
[Quelle: ISO] ISO 31000
[Quelle: ISO] ISO/IEC 27001
[Quelle: ISO] ISO/IEC 27005
[Quelle: K.Paschke] „IT Notfallmanagement im Unternehmen und in der Behörde“
ISBN: 978-3-7322-7418-5 Seite 304
[Quelle: BSI] www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html
[Quelle: IT-Sicherheitskatalog] vgl. Seite 13

KRZYSZTOF PASCHKE

Leiter *it*SMF-Fachforum
„**Cyber Defense und Resilienz**“

Geschäftsführer und Berater
GRC Partner GmbH, Kiel.

KPASCHKE@GRC-PARTNER.DE

WWW.GRC-PARTNER.DE