Ohne Transparenz kein Schutz

Durchführung von IT-Risikoanalysen auf der Basis von ISO/IEC 27005

Der hohe Stellenwert der IT erfordert heute eine umfassende Identifikation und Bewertung der zugehörigen Risiken. ISO/IEC 27005 liefert eine strukturierte Vorgehensweise, die es aber in einen umfassenden Gesamtprozess einzubetten gilt.

Von Jakob Pietzka, Ulm, und Reinhard Suhre, Hamburg

Unternehmen stehen heute vor der Herausforderung, in der Fülle allgegenwärtiger IT-Risiken frühzeitig kritische Punkte zu identifizieren und diesen gezielt mit Maßnahmen zu begegnen. Hierbei hilft ein ganzheitlicher Ansatz: IT-Risikoanalysen müssen die Rahmenbedingungen des Unternehmens sowie Anforderungen der Geschäftsprozesse berücksichtigen. Bereits aus Unternehmensgröße, Branche, wirtschaftlicher Stellung et cetera ergibt sich eine spezifische Bedrohungs-Lage – die Anforderungen der Geschäftsprozesse an die IT verfeinern anschließend dieses Bild und unterstützen dadurch die Ableitung spezifischer Bedrohungs-Szenarien.

Konzentriert sich die IT-Risikoanalyse auf diese Bedrohungsszenarien, ermöglicht das ein gezieltes und erfolgversprechendes Vorgehen. Daraus ergibt sich neben dem Schutz vor IT-Angriffen ein weiterer wesentlicher Vorteil: die „wirtschaftliche Betrachtung von Maßnahmen“. Die Zuordnung möglicher Maßnahmen zu einem identifizierten Restrisiko macht ihre Auswirkung nachvollziehbar – beispielsweise die Herunterstufung eines hohen Restrisikos auf ein akzeptables Niveau. Dadurch lässt sich der Nutzen einer Maßnahme auch hinsichtlich ihrer Wirtschaftlichkeit bewerten.

Die Norm ISO/IEC 27005 beschreibt eine strukturierte Vorgehensweise zur Durchführung einer IT-Risikoanalyse anhand von drei Hauptschritten:

- Erfassung des Kontexts,
- Risiko-Assessment und
- Risikobehandlung.

In der Praxis empfiehlt sich die Einbindung der IT-Risikoanalyse in einen Gesamtprozess, der Unternehmen bei der Entscheidung hilft, wann eine IT-Risikoanalyse notwendig ist, und zudem die nachvollziehbare Verwertung der Ergebnisse (Maßnahmentracking) unterstützt:

- Feststellung und Abnahme des Schutzbedarfs
- Vorbereitung der IT-Risikoanalyse
- Durchführung der IT-Risikoanalyse (anhand der drei Hauptschritte)
- Ergebnisbehandlung

Vorgehen nach ISO/IEC 27005

ISO/IEC 27005:2011 steht zurzeit in der zweiten Version zur Verfügung und liefert Handlungsanweisungen für das Risikomanagement in der IT-Sicherheit. Sie unterstützt die Konzepte der ISO/IEC 27001 und ist integraler Bestandteil eines Informationssicherheitsmanagementsystems (ISMS) – die IT-Risikoanalyse spiegelt die prozessorientierte Ausführung der darin beschriebenen Handlungsanweisungen wider. Abbildung 1 verdeutlicht die drei Hauptschritte mit Ergänzungen durch projektrelevante Koordinations- und Managementaufgaben.

Erfassung des Kontexts

Um eine fundierte IT-Risikoanalyse durchführen zu können, ist zunächst ihr Kontext zu definieren: Entsprechende Grundlagen und Informationen ergeben sich sowohl aus dem IT-Risikomanagement als auch aus dem Informationssicherheitsmanagementsystem. Der Kontext liefert detaillierte Informationen über die Struktur des Unternehmens, organisatorische und rechtliche Rahmenbedingungen, Schutzbedarfsklassifizierungen und spezifische Rahmenbedingungen. Bei der anschließenden Bewertung der IT-Risiken spielen diese Punkte eine wesentliche Rolle.

Zudem erfolgen innerhalb des ersten Schritts die genaue Definition und Abgrenzung des Untersuchungsobjekts – ein gemeinsames Verständnis des Untersuchungsobjekts ist entscheidend für den Erfolg der IT-Risikoanalyse. Dazu ist ihr „Scope“ zu definieren: sprich das Untersuchungsobjekt selbst, relevante Schnittstellen, unterstützende IT-Prozesse et cetera. Die Schwerpunkte der nachfolgenden Analyse werden erst im zweiten Hauptschritt festgelegt.

Risiko-Assessment

Das Risiko-Assessment ist der wichtigste Schritt einer IT-Risikoanalyse – sie lässt sich in drei Teilschritte unterteilen: in Identifikation, Abschätzung und Bewertung der Risiken.

Die Risikoidentifikation ist dabei nicht nur der wichtigste, sondern auch der arbeitsintensivste Schritt. Hierzu gehört die Identifikation der Assets, Bedrohungen, bereits umgesetzten Maßnahmen (Controls) sowie vorliegenden Schwachstellen. Um den genauen Stellenwert des jeweiligen Untersuchungsobjekts innerhalb einer Organsisation bewerten zu können, muss zu Beginn eine entsprechende Zuordnung der Abhängigkeiten erfolgen. Das beginnt mit einer Zuordnung des Untersuchungsobjekts bezüglich der „Primary Assets“:

_____ Welche unternehmenskritischen Geschäftsprozesse werden durch das Untersuchungsobjekt (IT-Anwendung) tangiert?

_____ Sind rechtliche Rahmenbedingungen im Bereich des Untersuchungsobjekts zu beachten (behördliche Auflagen, Datenschutz etc.)?

Darüber hinaus gilt es, die unterstützenden Assets mit Bezug zum Untersuchungsobjekt zu ermitteln:

_____ eingesetzte Soft- und Hardware,

_____ Netzwerkkomponenten und -verbindungen,

_____ Mitarbeiter,

_____ Standortfaktoren (Gebäude, Räume, Umgebung) sowie

_____ Organisationsstrukturen (übergeordnet).

Anschließend erfolgt die Identifikation der Bedrohungen, deren Ergebnisse den Schwerpunkt der weiteren (technischen) Analysen festlegen. ISO/IEC 27005 liefert hierzu eine generische Liste verschiedener Bedrohungen und Bedrohungsherkünfte – beispielsweise physische Bedrohungen wie Feuer oder Wasserschaden sowie von Personen ausgehende Bedrohungen wie Hacking oder Social Engineering.

Unter Berücksichtigung der Rahmenbedingungen (Kontext) ermittelt und dokumentiert man die für das Untersuchungsobjekt individuellen Szenarien. Ein vereinfachtes Beispiel: Bei einem Untersuchungsobjekt mit extern erreichbaren, jedoch geschützten Webseiten könnte ein spezifisches Bedrohungsszenario für die Bedrohung „Hacking“ wie folgt lauten: „Umgehung der Authentifizierung durch technische Manipulation“.

Die gefundenen Szenarien werden dann hinsichtlich ihrer Eintrittswahrscheinlichkeit und dem möglichen Schaden (Business Impact) eingeschätzt – bei der Eintrittswahrscheinlichkeit kann man ferner noch zwischen verschiedenen Verursachern unterscheiden. ISO/IEC 27005 liefert auch dafür eine Reihe von Vorgaben, zum Beispiel „Hacker/Cracker“, „Computerkriminelle“ oder „Insider“.

Im weiteren Verlauf konzentriert sich die Analyse auf die relevanten Bedrohungsszenarien aus dem vorangegangenen Schritt: Im Umfeld des jeweiligen Untersuchungsobjekts werden zunächst alle bereits getroffenen Maßnahmen ermittelt und hinsichtlich Vollständigkeit sowie Angemessenheit bewertet – dabei bilden die entsprechenden Vorgaben aus ISO/IEC 27001 und IT-Grundschutz eine wesentliche Grundlage. Konkret bieten sich die folgenden Methoden an:

_____ Interviews mit den IT-verantwortlichen Mitarbeitern im Umfeld des Untersuchungsobjekts (insbesondere auch zur Ermittlung der getroffenen Maßnahmen),

_____ Prüfung der Konzept- und Prozessdokumentationen (sowie weiterer relevanter Dokumente, z. B. Verträge)

_____ technische Prüfung der Maßnahmen aus Perspektive potenzieller Angreifer (z. B. Penetrationstest, Web-Application-Security-Audit), wobei sich die zu simulierenden Szenarien aus dem Schritt „Identifikation der Bedrohungen“ ableiten, sowie

_____ Ortsbegehungen in den für den Betrieb des Untersuchungsobjekts relevanten Räumlichkeiten.

Zu den bisherigen Ergebnissen sind nun deren Auswirkungen zu ergründen: Vergleichbar zum einleitenden Schritt „Identifikation von Bedrohungen“ werden die möglichen Auswirkungsszenarien identifiziert und dokumentiert, wobei man den theoretischen Bedrohungsszenarien nun auch konkrete Schwachstellen zuordnen kann. Diese Szenarien lassen sich, mit direktem Bezug auf das Untersuchungsobjekt, wie folgt gliedern:

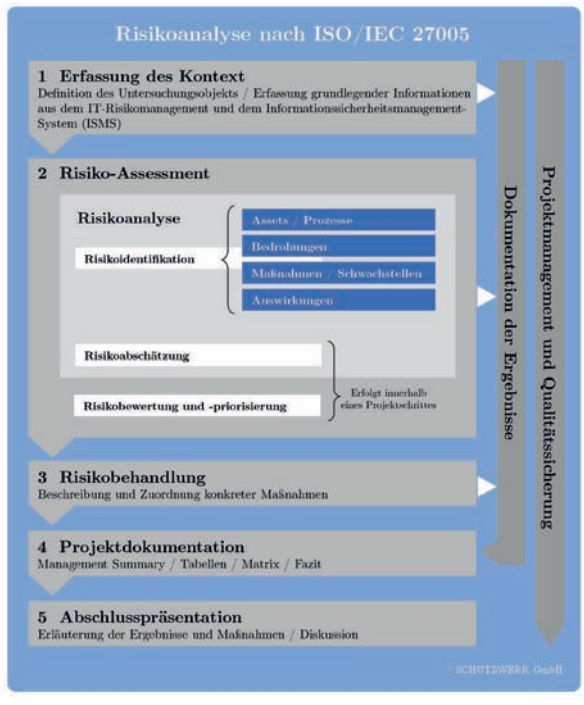

Abbildung 1: Überblick der Hauptschritte einer IT-Risikoanalyse nach ISO/IEC 27005

_____ Beeinträchtigung unternehmenskritischer Geschäftsprozesse,
_____ finanzielle Schäden sowie
_____ Imageschäden und Vertrauensverlust.

Zum Abschluss gilt es alle Ergebnisse zusammenzuführen, um die Restrisiken zu ermitteln – für die Risikoabschätzung ist sowohl der Einsatz quantitativer als auch qualitativer Techniken möglich. Quantitative Techniken bedingen das Vorhandensein konkreter Zahlen mit möglichst direktem Bezug zum Untersuchungsobjekt (konkrete Eintrittswahrscheinlichkeit einer Bedrohung auf Basis einer Schadensereignisdatenbank, entstehender finanzieller Schaden in Euro etc.) – in der Praxis sind jedoch oft keine fundierten Zahlen vorhanden, zudem kann die individuelle Ermittlung einen erheblichen Aufwand bedeuten. Eine qualitative Bewertung der Restrisiken, beispielsweise auf einer Skala von „niedrig" bis „sehr hoch", erweist sich in der Praxis als gangbare Alternative.

Risikobehandlung

Ziel der Risikobehandlung ist die Beschreibung und Zuordnung konkreter Maßnahmen im Hinblick auf den Umgang mit den ermittelten Restrisiken. ISO/IEC 27005 nennt hierzu vier grundlegende Strategien: Reduktion, Übernahme, Vermeidung und Transfer. In der Praxis liegt der Schwerpunkt der Maßnahmen hauptsächlich im Bereich der Strategien „Reduktion" und „Vermeidung", wobei folgende Ausprägungen zum Tragen kommen:
_____ Umsetzung oder Optimierung betriebstechnischer Maßnahmen (Konfigurationsänderungen / Softwareaktualisierung am Untersuchungsobjekt etc.),
_____ Umsetzung oder Optimierung physischer Maßnahmen im Umfeld des Untersuchungsobjekts (Zutrittsschutz etc.) sowie
_____ Umsetzung oder Optimierung konzept- und prozessbezogener Maßnahmen (Patchmanagement, Dokumentationsrichtlinien etc.).

Mit dem Hauptschritt der Risikobehandlung endet die IT-Risikoanalyse nach ISO/IEC 27005 – der Umgang mit den ermittelten Maßnahmen unterscheidet sich von Unternehmen zu Unternehmen und ist abhängig vom jeweiligen IT-Risikomanagement.

Gesamtprozess

In der Praxis hat es sich bewährt, die Vorgehensweise der Norm in einen Gesamtprozess einzubinden, um einen nachhaltigen Nutzen zu garantieren. Die ergänzenden Prozessschritte entscheiden über Notwendigkeit der IT-Risikoanalyse und unterstützen Unternehmen bei der Verwertung der Ergebnisse. In der Regel besteht dieser Gesamtprozess aus vier Phasen.

Feststellung und Abnahme des Schutzbedarfs

Die erste Phase dient der Feststellung, ob und in welchem Umfang überhaupt eine Analyse durchzuführen ist. Hierzu sind Kriterien vorzugeben, zum Beispiel die Einstufung des Schutzbedarfs hinsichtlich der IT-Grundwerte: So kann man etwa bei Anwendungen mit niedrigem oder mittlerem Schutzbedarf vereinbaren, auf eine Analyse zu verzichten – bei Anwendungen mit hohem und sehr hohem Schutzbedarf oder anderen, besonderen Anforderungen wäre die Durchführung einer IT-Risikoanalyse hingegen Pflicht. Die Durchführung der Schutzbedarfsklassifizierung ist durch Richtlinien vorzuschreiben – die offizielle Freigabe der Klassifizierung durch eine zentrale Stelle sorgt für die notwendige Verbindlichkeit.

Vorbereitung der IT-Risikoanalyse

Hierzu gehört eine Beschreibung des Untersuchungsobjekts in einer Form, die eine Schätzung des Aufwands der Analyse ermöglicht. Die Festlegung des Scopes stellt dar, in welchem Umfang die Untersuchungen durchzuführen sind: Wird ausschließlich interview- und dokumentenbasiert geprüft? Sind technische Tests erforderlich? Ortsbegehungen? Bereits zu diesem Zeitpunkt sollten auch die zu prüfenden Dokumente zur Verfügung stehen.

Durchführung der IT-Risikoanalyse

Phase drei umfasst die bereits erörterten Hauptschritte von Erfassung des Kontexts bis zur Risikobehandlung. In der Praxis werden meist alle Abhängigkeiten und damit auch genutzten Komponenten in die Analyse einbezogen: beginnend mit dem Rechenzentrum über Infrastrukturkomponenten und IT-Systeme bis hin zu relevanten IT-Prozessen, wie Incident- oder Patchmanagement. Das Ergebnis der IT-Risikoanalyse zeigt eine Aufstellung aller identifizierten und bewerteten Restrisiken – es muss durch die Projektbeteiligten abgenommen werden.

Ergebnisbehandlung

Für die berechtigte Frage „Und was geschieht jetzt mit den Ergebnissen?" ist die vierte Phase zuständig. Dabei hat es sich als sinnvoll erwiesen, die Ergebnisbehandlung eigenständig zu sehen – die Individualität der Restrisiken und identifizierten Schwachstellen bestätigt diesen Weg. Die folgende Aufzählung nennt Beispiele möglicher Arten von Schwachstellen – ohne natürlich den Anspruch auf Vollständigkeit zu erheben. Schwachstellen können...
_____ sich ausschließlich auf das Untersuchungsobjekt beziehen (Maßnahmen lassen sich direkt initiieren, die Entscheidungsträger sind i.d.R. an der Analyse beteiligt),
_____ andere Systeme, Objekte oder Schnittstellen betreffen (der Personenkreis der Entscheidungsträger erweitert sich),

_____ komplexe Infrastruktur oder Örtlichkeiten betreffen,
_____ gegen Verträge oder Compliance-Anforderungen verstoßen,
_____ in unzureichenden Kenntnissen der Mitarbeiter bestehen,
_____ lokale oder globale Auswirkungen haben.

Je Schwachstelle ist zu entscheiden, ob man das bestehende Restrisiko akzeptiert oder ob und in welchem Umfang Maßnahmen mit welcher Dringlichkeit von wem bis wann durchzuführen sind. Zu berücksichtigen ist hier, dass Maßnahmen längere Zeiträume benötigen können – auch darin liegt ein wichtiger Grund, die Ergebnisbehandlung als eigene Phase anzusehen und hierfür sauber strukturierte Prozesse und Rollen zu definieren.

Systematik und Hilfsmittel

Erfolgen IT-Risikoanalysen immer nach der gleichen Vorgehensweise, sind ihre Ergebnisse vergleichbar und auditierbar. Dies schafft die Möglichkeit, auf bereits durchgeführte IT-Risikoanalysen referenzieren zu können – ändern sich Voraussetzungen eines Untersuchungsobjekts, reicht häufig eine kleine, ergänzende Prüfung. Die ständige Kontrolle der Vorgehensweise führt ferner zu einer stetigen Optimierung und somit zu effektiverer Ermittlung der Restrisiken.

Zur optimalen Unterstützung einer IT-Risikoanalyse hat es sich bewährt, in der Praxis einige „Templates" zu entwerfen, die der Vergleichbarkeit Rechnung tragen:

_____ *Task-Description:* legt die Rahmenbedingungen für die durchzuführende Analyse fest. Dazu gehören eine kurze Beschreibung und die wichtigsten Eckpunkte des Untersuchungsobjekts. Ebenso wird der Schutzbedarf dargestellt, der besondere Ausprägungen der Analyse vorgeben kann. Ein grober Zeitplan, eventuell einzuhaltende Fristen und zu berücksichtigende Standorte sind ebenfalls wichtige Informationen in diesem Dokument.

_____ *Risk-Assessment-Report:* ist eine textorientierte Zusammenfassung der Ergebnisse und richtet sich an die organisatorisch verantwortlichen Personen des Untersuchungsobjekts – eine Kapitelstruktur mit entsprechenden Hinweisen gibt vor, welche Inhalte erwartet werden. Der Report beschreibt neben dem Untersuchungsobjekt die verwendeten Methoden zur Identifikation der Maßnahmen und Schwachstellen, Ergebnisse in managementgerechter Darstellung und die Ergebnisse im Detail.

_____ *Risk-Assessment-/Schwachstellenanalyse-Formular:* Dieses tabellenorientierte Dokument entsteht während der Durchführung der IT-Risikoanalyse und unterstützt das dargestellte Vorgehen der Analyse nach ISO/IEC 27005 – jede Tabellenzeile enthält spezifische Bedrohungsszenarien. Das Formular unterstützt zudem die sys-tematische Bewertung des initialen Risikos, erfasst bereits getroffene Maßnahmen und bewertet diese. Abschließend wird das resultierende Risiko berechnet: Erreicht es hohe oder sehr hohe Werte, so wurde eine Schwachstelle identifiziert. Für alle solchen Schwachstellen fordert das Formular eine Maßnahmenempfehlung, die das Restrisiko auf ein akzeptables Maß reduziert.

Die zuletzt genannte Tabelle sollte für die Berechnungen ein Formelwerk verwenden, das sich ebenfalls an den Vorgaben der ISO/IEC 27005 orientiert. Zudem kann das Formular auch die Ergebnisbehandlung unterstützen – die Grenzen sind hier fließend. Denn oft kommt es bereits zum Ende der dritten Phase, sprich der eigentlichen IT-Risikoanalyse, schon zu Diskussionen, ob sich bestehende Risiken reduzieren lassen, welche Maßnahmen sich eignen und welche Zuständigkeiten zu erwarten sind. Während der Ergebnisbehandlung wird das konkretisiert: Durchführung und genaue Art von Maßnahmen werden vereinbart, Zuständigkeiten und Zeiträume der Umsetzung festgehalten. Die Analyse endet mit diesem Ergebnis – das Tracking der Maßnahmenumsetzung wird jedoch im Gesamtprozess periodisch weiterverfolgt.

Fazit

IT-Risikoanalysen sind ein geeignetes Mittel, um innerhalb von komplexen IT-Umgebungen kritische IT-Risiken gezielt zu identifizieren und zu behandeln. Die ISO/IEC 27005 bietet Unternehmen hierfür eine strukturierte Vorgehensweise und liefert generische Vorgaben. In der Praxis lässt sich dies effektiv in einen Gesamtprozess integrieren, um eine nachhaltige Verwertung der Ergebnisse zu garantieren.

Die strukturierte Vorgehensweise und der Einsatz von Templates ermöglichen es Unternehmen, die Ergebnisse einzelner IT-Risikoanalysen zu vergleichen und wiederzuverwenden. So reduziert sich mittelfristig der Aufwand einer IT-Risikoanalyse – bei zusätzlich deutlich steigender Qualität der Bewertungen.

Die Transparenz über IT-Risiken führt in der Konsequenz zu weniger Ausfällen und Störungen des IT-Betriebs. Gleichzeitig kann man die Auswirkung von Maßnahmen auf ein IT-Risiko anhand der Ergebnisse einfach nachvollziehen. Dies ermöglicht es Unternehmen, Maßnahmen zielgerichtet umzusetzen und ihren Nutzen wirtschaftlich zu bewerten. ■

Jakob Pietzka ist Geschäftsführer der Schutzwerk GmbH. Reinhard Suhre ist Senior Business Consultant bei der direkt gruppe GmbH.

Sind Sie verantwortlich für die IT-Sicherheit?

<kes> liefert alle relevanten Informationen zum Thema IT-Sicherheit – sorgfältig recherchiert von Fachredakteuren und Autoren aus der Praxis.

In jeder Ausgabe finden Sie wichtiges Know-how, Hinweise zu Risiken und Strategien, Lösungsvorschläge und Anwenderberichte zu den Themen:

Internet/Intranet-Sicherheit
Zutrittskontrolle
Virenabwehr
Verschlüsselung
Risikomanagement
Abhör- und Manipulationsschutz
Sicherheitsplanung
Elektronische Signatur und PKI

<kes> ist seit 20 Jahren *die* Fachzeitschrift zum Thema Informations-Sicherheit - eine Garantie für Zuverlässigkeit.

Jetzt Probeheft anfordern!

<kes>-online

<kes>-Leser können neben der Print-Ausgabe auch <kes>-online unter www.kes.info nutzen. Hier finden Sie ohne Zugangsbeschränkung aktuelle Kurzmeldungen zum Probelesen.

PROBEHEFT-ANFORDERUNG

☐ **ja,** bitte schicken Sie mir gratis und unverbindlich ein Exemplar der <kes> - **Die Zeitschrift für Informations-Sicherheit** zum Probelesen zu.

☐ **ja,** bitte schicken Sie mir aktuelle **<kes> Specials** gratis zu.

Es kommt nur dann ein Abonnement zustande, wenn ich es ausdrücklich wünsche.

Das Abonnement beinhaltet ein Passwort zur Nutzung des Abo-Bereichs auf www.kes.info sowie den Bezug des SecuPedia-Newsletters.

Datum | Zeichen | Unterschrift

FAX an +49 6725 5994

SecuMedia Verlags-GmbH
Leser-Service
Postfach 12 34
55205 Ingelheim

Lieferung bitte an

Telefon Durchwahl