Vorbeugen ist besser als heilen

Workshop Mit der IT Bedrohungs- und Risikoanalyse können sämtliche relevanten Faktoren auf Sicherheitslücken und Schwachstellen überprüft und Gegenmassnahmen erarbeitet werden.

Christoph Baumgartner*

Es existieren verschiedene Vorgehensmodelle für die Durchführung von IT-Bedrohungs- und Risikoanalysen. Eine im deutschsprachigen Raum weit verbreitete Methode ist im «IT Grundschutzhandbuch» des Deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) erläutert. Dieses umfangreiche und in der Downloadversion kostenlose Werk besteht aus diversen Checklisten, Formularen und Empfehlungen, welche bei der Durchführung einer Bedrohungs- und Risikoanalyse sehr hilfreich sein können.

Um die Vorgehensweise zu verdeutlichen, wird ein vom Autor entwickeltes fünfstufiges Vorgehensmodell verwendet. Als Beispiel soll die Server-Komponente des ERP-Systems (Enterprise Ressource Planning) eines fiktiven Produktionsbetriebs dienen. Dabei wird nur ein kleiner Ausschnitt des Outputs der jeweiligen Projektetappen wiedergegeben.

Oft wird der richtigen Projektvorbereitung zu wenig Aufmerksamkeit geschenkt. Dies gilt besonders für Projekte im IT-Risk-Management-Umfeld. IT Risk Management ist Chefsache, weil es für den Fortbestand des Unternehmens von vitalem Interesse und die Verantwortung gemäss den gesetzlichen Anforderungen nicht delegierbar ist. Ein Projekt gilt dann als erfolgreich, wenn alle Projektziele fristgerecht und in der gewünschten Qualität erreicht und der im Voraus bewilligte Projektressourcenrahmen nicht überschritten wurde. Dennoch werden Projekte im IT-Risk-Management-Umfeld oft als Infrastrukturprojekte angesehen, welche erfahrungsgemäss nicht höchste Priorität geniessen und bei Ressourcenkonflikten zu Gunsten eines anderen Projektes unter- oder abgebrochen werden.

Projektdefinition

Um diesem Trend entgegenzuwirken, sollten die Projektziele (inkl. präziser Definition des Untersuchungsobjekts und dessen Abgrenzung) und die benötigten (und gebundenen!) personellen und monetären Ressourcen vorab geklärt werden. Zu diesem Zeitpunkt sollten die Projektverantwortlichen auch die Option prüfen, ob ein externer Coach in das Projektteam integriert werden soll. Coaches bringen einerseits Know-how aus anderen Projekten ein und ermöglichen den Knowledge-Transfer zum Kunden. Andererseits können sie in kritischen Situationen als Externe schlichtend wirken. Ein Projektsponsor in der Geschäftsleitung verschafft dem Projekt auch in schwierigeren Projektphasen oftmals den nötigen Vortrieb. Erst wenn die vorhergehenden Punkte geklärt sind, stehen die Erfolgschancen für die IT Bedrohungs- und Risikoanalyse gut und es kann mit dem eigentlichen Projekt begonnen werden.

*Christoph Baumgartner ist seit 1996 im IT Consulting mit den Schwerpunkten IT Risk Management und IT Strategie tätig. Er ist Head of IT Consulting bei der CDC IT AG und Geschäftsführer der Oneconsult GmbH.

Als erstes muss die Systemarchitektur spezifiziert werden. Es werden alle für die Systemsicherheit relevanten Komponenten des IT Systems und deren Beziehungen untereinander spezifiziert. Dabei müssen auch die IT-relevanten Prozesse dokumentiert und aufgelistet werden. Die nachfolgende, nicht abschliessende Aufzählung soll dies verdeutlichen: Der Betrieb setzt ein ERP-System des Herstellers XY ein, über welches alle Business-relevanten Aktivitäten (Beschaffung, Fertigung, Logistik, usw.) abgewickelt werden. Server-Komponente des ERP-Systems läuft auf einem Vier-Prozessor Server im Aktiv/Passiv-Mode (gleich redundante Motherboards: falls auf einem Motherboard oder den damit verbundenen Komponenten ein Defekt eintritt, übernimmt das andere Motherboard dessen Aufgaben). Netzteile des Servers sind redundant ausgelegt und es existiert eine Notstromversorgung. Serverhaltung erfolgt in frei stehenden Racks in einem schwach frequentierten Gang. Systemadministratoren sind für die täglichen Datenbackups auf Bänder und monatliche Datenwiederherstellungstests verantwortlich.

Sicherheitsanforderungen

Im nächsten Schritt werden alle Sicherheitsanforderungen explizit definiert. Als Vorlage dienen die klassischen Sicherheitskriterien: Verfügbarkeit, Vertraulichkeit und Integrität. Bei elektronischen Dokumenten mit vertraglichem Charakter (zum Beispiel Bestellungen in Web-Shops) kommt noch ein weiteres Sicherheitskriterium hinzu: die Verbindlichkeit. Sicherheitsanforderungen bezüglich der Verfügbarkeit könne lauten: Das ERP-System muss zu mindestens 95 Prozent verfügbar sein. Systemausfälle des ERP-Systems dürfen maximal einen Tag dauern. Die vom ERP-System generierten Daten müssen täglich gesichert werden. Auf die Vertraulichkeit bezieht sich beispielsweise die Forderung: Forschungsergebnisse, Kundeninformationen, Personal- und Finanzdaten müssen vor dem Zugriff Unberechtigter geschützt werden. Und für die Sicherstellung der Integrität gilt: Es existiert eine Masterdatenbank im Betrieb, welche gepflegt wird. Andere Datenhaltungen beziehen ihre Daten aus der Masterdatenbank.

Qualifikation der Risiken

Nachdem die Sicherheitsanforderungen fest stehen, gilt es nun mit Hilfe eines allgemeinen Bedrohungskatalogs – kann im «IT Grundschutzhandbuch» nachgeschlagen werden – die individuellen IT-Risiken des Unternehmens abzuleiten. Eine auf das Unternehmen zutreffende Bedrohung wird ab dieser Projektetappe als Risiko bezeichnet. Beispiele für die Qualifikation der Risiken sind: Bedrohung «Gefahr durch Wasserschaden» wird als Risiko angesehen, weil die Sicherheitsanforderung «Verfügbarkeit des ERP-Systems» definiert wurde. Die Bedrohung «Gefahr durch Stromausfall» wird als Risiko angesehen, weil die Sicherheitsanforderung «Verfügbarkeit des ERP-Systems» definiert wurde. Die Bedrohung «Gefahr durch Hacker» wird als Risiko angesehen, weil die Sicherheitsanforderung «Vertraulichkeit von sensitiven Daten» definiert wurde.

Quantifikation der Risiken

Um die Auswirkungen von Risiken zu erkennen, behelfen wir uns in dieser Projektetappe mit einem Szenarienkonzept, welches auf hypothetisch eintretenden Ereignissen basiert und dennoch Rechenwerte liefert, deren Ergebnisse sich miteinander vergleichen lassen. So ist ein Server üblicherweise weit mehr wert, als die Summe seiner Einzelteile und der Softwarelizenzen. Um den wahren Wert eines (Teil-) Systems zu beziffern, muss es als Ressource in den richtigen Kontext gestellt werden. Was passiert, wenn eine Sicherheitsanforderung nicht mehr gewährleistet ist, wenn ein System nicht mehr verfügbar ist, oder die vertraulichen Daten im LAN/WAN nicht mehr sicher durch Verschlüsselung sind (und somit Mitbewerber sensitive Marketingpläne lesen könnten)? Die Beantwortung solcher Fragen hilft, den wahren Wert eines funktionierenden (Teil-)Systems zu erkennen.

Bei dieser Projektetappe ist die Mitwirkung des Managements unumgänglich, weil der Projektnutzen direkt von glaubwürdigen Schätzungen abhängt. Es muss für jede Komponente des Untersuchungsobjekts berechnet werden, welcher Schaden im Falle der Verletzung einer Sicherheitsanforderung – Verfügbarkeit, Integrität, Vertraulichkeit oder Verbindlichkeit – entsteht. Dabei kommt folgende Formel zum Einsatz: Die geschätzte Schadenshöhe im Eintrittsfall multipliziert mit der Eintrittwahrscheinlichkeit pro Jahr ergibt den Rechenwert oder den Maximalbetrag, welcher aus ökonomischer Sicht in Gegenmassnahmen investiert werden könnte.

Ausfälle erfassen

Mitunter ist es ziemlich schwierig, brauchbare Schätzungen anzustellen. Sinnvoll ist es oftmals, die Mitarbeiter der IT-Abteilung zu bitten, aufzuschreiben, wie viel Zeit sie für welche Arbeiten aufwenden und wie oft es zu bestimmten Systemausfällen kommt. Wichtig ist dabei, den Betroffenen klar zu machen, dass es bei dieser Umfrage nicht um eine persönliche Beurteilung der Qualität ihrer Arbeit geht, sondern dass sie als Spezialisten einen bedeutenden Beitrag zum Projekterfolg leisten können. Ansonsten werden die Resultate nur bedingt brauchbar sein. Auf Grund der Angaben kann so die Variable «Eintrittswahrscheinlichkeit» ermittelt werden. Der Erfahrungswert «Eintrittswahrscheinlichkeit» beinhaltet den sicherheitstechnischen Status Quo.

Bei der Schätzung der Variable «Schadenshöhe im Eintrittsfall» ist das Management gefordert. Zu berücksichtigen sind dabei direkte und indirekte Schäden in Abhängigkeit zur Dauer der Verletzung einer Sicherheitsanforderung. Zu den direkten Schäden zählen unter anderem Umsatzeinbussen, Produktivitätsverlust, Umstellung auf manuelle Prozessabwicklung, Wiederbeschaffungs-/Reparaturkosten der defekten Hardware oder Wiederanlaufkosten der automatisierten Fertigung. Indirekte Schäden können sein: Imageverlust oder Opportunitätskosten. Dabei ist es den Projektleitern frei gestellt, ob sie nur den Maximalschaden berücksichtigen – Verletzung der Sicherheitsanforderung während eines betriebskritischen Zeitraums – oder feiner untergliedern wollen. Ein Raster von einer, zwei, vier, acht und zwölf Stunden, beziehungsweise einem und mehr Tagen hat sich in der Praxis bewährt. Selbstverständlich können auch individuelle Zeiteinheiten verwendet werden. Die Erfahrung zeigt, dass die eigentlichen Hard- und Softwarewarekosten bei zentralen Systemen nur noch eine untergeordnete Rolle spielen.

Grundlage für Massnahmen

Das Resultat der Quantifikation und Monetarisierung von Risiken sind Rechenwerte, die einen Massstab liefern, wie weit aus ökonomischer Sicht sinnvoll in Gegenmassnahmen zur Bekämpfung der entsprechenden Risiken investiert werden könnte.

Beispiel für die Quantifikation und Monetarisierung von Risiken wie «Gefahr durch Wasserschaden» und «Gefahr durch Stromausfall»: Sowohl ein Wasserschaden als auch ein Stromausfall können zur temporären Nicht-Verfügbarkeit des ERP-Systems führen. Im Falle eines Wasserschadens am Systemstandort ist die Serverkomponente voraussichtlich irreparabel beschädigt, während sie nach einem Stromausfall oftmals wieder hochgefahren werden kann und problemlos weiter arbeitet. Somit unterscheiden sich die beiden Risiken einerseits in Bezug auf die Dauer der Verletzung der Sicherheitsanforderung an die Systemressource ERP-System, andererseits spielt die allenfalls nötige Reparatur oder Neuanschaffung einer Systemkomponente eine Rolle.

Rechenbeispiel: Bei einem Wasserschaden wird mit einer Schadenshöhe von 250 000 Franken gerechnet – aufgeteilt in direkte Kosten von 200 000 Franken und indirekte von 50 000 Franken. Multipliziert mit der Eintrittswahrscheinlichkeit von fünf Prozent (0,05) ergibt sich ein Rechenwert von 12 500 Franken. Die gleiche Rechnung bei einem Stromausfall: Die Schadenshöhe beträgt 140 000 Franken (100 000 Franken direkte und 40 000 Franken indirekte Kosten) und wird mit der Eintrittwahrscheinlichkeit von zehn Prozent (0,1) multipliziert. Das Produkt ergibt einen Rechenwert von 14 000 Franken.

Demnach würden sich in diesen Beispielen aus ökonomischer Sicht Investitionen bis zu 12 500 Franken pro Jahr zum Schutz vor Wasserschäden dieser ERP-Serverkomponente lohnen. Zum Schutz vor Stromausfällen wären gar Investitionen bis zur Höhe von 14 000 Franken pro Jahr ökonomisch noch sinnvoll.

Risikomanagement

Dank der vorherigen Projektetappe liegen nun Rechenwerte zu den einzelnen Risiken vor. Es kann jetzt bestimmt werden, wie mit den einzelnen Risiken umgegangen werden soll. Grundsätzlich hat man dabei vier Möglichkeiten: Man kann Risiken verhindern, vermindern, abwälzen (z. B. Versicherung abschliessen), oder bewusst tragen.

Die Möglichkeit, ein bekanntes Risiko zu ignorieren, existiert nicht. Aus ökonomischen Gründen ist es meistens nicht sinnvoll, alle Risiken zu verhindern. Um Kosten einzusparen, werden bestimmte Risiken vermindert, abgewälzt oder bewusst getragen. Dabei kann von den jeweiligen Rechenwerten ausgegangen werden: Je höher die Summe der Rechenwerte einer bestimmten Systemkomponente, desto eher sollten deren Risiken verhindert oder vermindert werden. Das Risiko «Gefahr durch grossen Asteroideneinschlag» ergibt beispielsweise einen niedrigen Rechenwert. Die im Eintrittsfall sehr hohe Schadenssumme wird durch die äusserst geringe Eintrittswahrscheinlichkeit relativiert. Solche Risiken werden üblicherweise auf eine Versicherung abgewälzt oder bewusst getragen.

Mehrere Möglichkeiten

Nachdem man beschlossen hat, wie mit den einzelnen Risiken umgegangen werden soll, können geeignete Massnahmen evaluiert werden. Es gibt Massnahmen, welche verschiedenen Risiken gleichzeitig entgegenwirken. So kann ein Computersafe sowohl vor Wasser als auch vor Feuer schützen. Eine solche Massnahme müsste über die Rechenwerte «Schutz der Server vor Feuer» und «Schutz der Server vor Wasser» finanziert werden. Falls der Safe zusätzlich über einen sicheren Schliessmechanismus verfügt, käme auch noch der Rechenwert «Schutz der Server vor Diebstahl» in Frage.

Zum Schluss wird ein Massnahmenkatalog ausgearbeitet und die daraus resultierenden Massnahmen umgesetzt. Dabei ist zwischen organisatorischen und technischen Massnahmen zu unterscheiden. Beispiele für Massnahmendefinitionen sind: Risiko «Gefahr durch Wasserschaden» soll durch die Verlegung der Serverracks in das vierte Obergeschoss vermindert werden. Risiko «Gefahr durch Stromausfall» soll mittels des Einbaus und der regelmässigen Funktionskontrolle von Notstromaggregaten verhindert werden. Risiko «Gefahr durch Hacker» soll durch den Einsatz einer Firewall und eines Intrusion Detection Systems vermindert werden. Risiko «Gefahr durch Hacker» soll durch regelmässige IT-Verwundbarkeitstests und Sicherheitsaudits vermindert werden. Das Risiko «Gefahr durch Hacker» (unlautere Informationsbeschaffung durch Telefonate) soll durch gezielte Mitarbeiterschulung und Aufklärung möglichst klein gehalten werden.

Fazit

Es lohnt sich in jedem Fall, eine IT-Bedrohungs- und Risikoanalyse durchzuführen. Die Komplexität des Projekts zwingt die Unternehmen dazu, sich intensiv und kritisch mit ihrer IT und allen damit vernetzten Faktoren (Menschen, Organisation und Technik) auseinander zu setzen. Leider wird in der Praxis oft vergessen, dass IT Risk Management ein Prozess ist und nicht bloss eine Momentaufnahme bleiben darf. Es reicht nicht, Massnahmen umzusetzen, wenn deren Wirksamkeit nicht von Zeit zu Zeit wieder überprüfen werden.

Info/http://www.cdcit.ch, http://www.oneconsult.com,http://www.bsi.de

IT-Bedrohungs- und Risikoanalyse

1. Spezifizierung der Systemarchitektur

- ERP-System des Herstellers XY für Beschaffung, Fertigung, Logistik usw.,
- Vier-Prozessoren-Server im Aktiv/Passiv-Mode,
- Redundant ausgelegte Netzteile,
- Notstromversorgung
- Frei stehendes Serverrack an schwach frequentiertem Ort,
- Tägliche Datenbackups auf Bänder,
- usw.

2. Definition der Sicherheitsanforderungen

Verfügbarkeit:
- Verfügbarkeit des ERP-Systems mindestens 95 Prozent,
- Ausfall des ERP-Systems maximal ein Tag,
- Daten des ERP-Systems müssen täglich gesichert werden,
- usw.

Vertraulichkeit:
- Forschungsergebnisse vor dem Zugriff Unberechtigter schützen, ebenso
- Kundeninformationen,
- Personaldaten,
- Finanzdaten,
- usw.

Integrität:
- Existenz einer Masterdatenbank,
- Datenbezug von Masterdatenbank,
- usw.

3. Qualifikation der Risiken

- Gefahr durch Wasserschaden beeinflusst Verfügbarkeit, ebenso
- Gefahr durch Stromausfall,
- Gefahr durch Hacker beinflusst Vertraulichkeit von sensitiven Daten,
- usw.

4. Quantifizierung und Monetarisierung der Risiken

Formel: Schadenshöhe im Eintrittsfall mal Eintrittswahrscheinlichkeit pro Jahr = Rechenwert

Direkte Schäden:
- Umsatzeinbussen,
- Produktivitätsverlust,
- Umstellung auf manuelle Prozesse,
- Wiederbeschaffung/Reparatur von Hardware,
- usw.

Indirekte Schäden
- Imageverlust,
- Opportunitätskosten,
- usw.

5. Risikomanagement und Massnahmendefinition

- Verlegung des Serverracks in den vierten Stock, um Wasserschäden vorzubeugen,
- Einbau und regelmässige Kontrolle von Notstromaggregaten, um Stromausfällen entgegenzuwirken,
- Einsatz einer Firewall und eines Intrusion Detection Systems, um Hackerangriffe abzuwehren,
- Regelmässige IT-Verwundbarkeitstests und Sicherheitsaudits, um Hackerangriffe abzuwehren,
- Mitarbeiterschulung, um Social Engineering vorzubeugen,
- usw.