IT-Risikomanagement im ÖD

Praxiserprobte Verfahren zur Risikobewertung

(BS/Lothar Goecke*) Auch im öffentlichen Bereich wird es immer wichtiger, die Maßnahmen zur IT-Sicherheit zu begründen. Dies kann im Rahmen eines Risikomanagements stattfinden.

Nicht alle IT-Anwendungen sind für eine Behörde gleich wichtig. Die Aufgabe des IT-Risikomanagements ist es, diejenigen herauszufiltern, die für die Behörde schützenswert sind. Die Einschätzung des Schutzbedarfs darf nicht allein durch die IT-Abteilung, sondern muss unbedingt zusammen mit den Anwendern erfolgen. Nur beide gemeinsam können die beiden Seiten von Risiken, das Schadenspotenzial und die Wahrscheinlichkeit des Schadenseintritts, in angemessener Weise erheben und miteinander in Beziehung setzen. Schließlich müssen sie das so ermittelte Risiko an einer behördenspezifischen Skala dahingehend bewerten, ob es tragbar ist oder nicht. Wenn nicht, sind Maßnahmen zu benennen, die das Risiko reduzieren.

Entscheidend für den Aufwand einer IT-Risikoanalyse ist die Gestaltung der Betrachtungstiefe. Je besser die IT-Anwendungen zusammengefasst werden, desto geringer wird der analytische Aufwand. Maßgeblich ist die Sicht der Anwender. Der Schutzbedarf der IT-Ressourcen kann von den IT-Anwendungen, die sie nutzen, abgeleitet werden. Für eine Basis-Infrastruktur ist der Schutzbedarf aller von ihr unterstützten Anwendungen zu berücksichtigen.

Um das Schadenspotenzial mit möglichst geringem Aufwand zu ermitteln, wird eine quantitativ und qualitativ beschriebene Skala eingesetzt, die z. B. lauten kann: unbedeutend, spürbar, erheblich, existenzbedrohend.

Zusammen mit der Einstufung in die Skala sind jeweils mögliche Schadenskategorien zu erfassen. Typischerweise kommen dabei vor:

- physische oder psychische Schädigung von Menschen,
- direkte finanzielle Auswirkung,
- Verstoß gegen Gesetze oder Vorschriften,
- Beeinträchtigung des Geschäftsablaufs,
- negative Außenwirkung,
- Schädigung der Allgemeinheit,
- Abfluss von vertraulichen Informationen.

Hier ist insbesondere auch auf die Schäden zu achten, die nicht in den Behörden, sondern außerhalb (in der Gesellschaft) auftreten.

Die Wahrscheinlichkeit für den Eintritt eines Schadens hängt von der Bedrohungslage sowie den vorhandenen Schwachstellen und Schutzmaßnahmen ab. Auch hier ist eine mit Erläuterungen versehene qualitative Skala mit vier oder sechs Stufen vollkommen ausreichend, z. B. sehr selten, selten, manchmal und häufig.

Nach der Analyse ist bekannt, welche Risiken für die IT-Anwendungen bestehen. Es ist aber noch nicht klar, wie die Behörde darauf reagieren soll. Um dies zu bestimmen, müssen Maßstäbe für den Umgang mit Risiken festgelegt werden. Diese lassen sich z. B. in einer Matrix mit den Dimensionen Eintrittswahrscheinlichkeit und Schadenspotential darstellen, in der für jede Bedrohung einer IT-Anwendung definiert wird, wie das Risiko zu bewerten ist. Dafür wird oft ein Ampelsystem verwendet.

Alle erfassten Risiken können in eine Matrix eingetragen werden. Das Resultat wird Risikolandkarte genannt. Mit ihr lässt sich das Gesamtrisiko anschaulich darstellen. Nach der Risikobewertung folgt die Konzeption des Umgangs mit den vorhandenen Risiken. Zu diesem Zweck sollte eine allgemeine Schutzstrategie festgelegt werden, die die grobe Richtung von Maßnahmen für abgegrenzte Risikogruppen enthält.

Auf der Basis der Schutzstrategie und der ermittelten Risiken werden die Maßnahmen zu einzelnen Risiken erarbeitet. Sind die Maßnahmen festgelegt, sollte noch einmal eine Bewertung jedes Risikos durchgeführt werden. Diesmal geht es jedoch um die Einschätzung der voraussichtlichen Veränderung durch die Maßnahmen. Das Ergebnis kann später, nachdem die Maßnahmen wirksam geworden sind, zur Erfolgskontrolle herangezogen werden.

**Lothar Goecke ist Geschäftsführer der consequa GmbH. Gemeinsam mit dem Autor wird der Behörden Spiegel am 29. und 30. November 2012 in Berlin das Praxisseminar "Der IT-Risikomanager" veranstalten. Die Teilnehmer erhalten einen kompakten Überblick über die wichtigsten Bausteine und Instrumente des IT-Risikomanagements. Weitere Informationen dazu unter: www.fuehrungskraefte-forum.de*