IT-NOTFALLMANAGEMENT

Wirtschaftliche Risiken erkennen

VON MARIUSZ BUCKI UND THOMAS ALTHAMMER

Mariusz Bucki ist Berater für IT-Sicherheit und Datenschutz bei der Althammer & Kill GmbH & Co. KG. Er verfügt über langjährige Erfahrung als Administrator im IT-Umfeld und berät Unternehmen u.a. beim Aufbau von IT-Notfallmanagementsystemen.
www.althammer-it.de

Thomas Althammer ist Geschäftsführer der Althammer & Kill GmbH & Co. KG. Zusammen mit seinem Team begleitet er bundesweit Einrichtungen in Pflege und Sozialwesen als Datenschutzbeauftragter und berät zu Fragen der Informationssicherheit.
www.althammer-it.de

Der Ausfall der Informationstechnik kann eine Organisation an den Rand der Überlebensfähigkeit bringen. Eine entsprechende Notfallvorsorge mit der Bereitstellung entsprechender Ressourcen gehört deshalb zu den wichtigsten Aufgaben des Managements

Entgegen weitläufiger Annahme fokussiert das IT-Notfallmanagement nicht primär auf die Absicherung der IT-Systeme, sondern vielmehr auf die Entwicklung einer organisierten Vorgehensweise zur Prävention und Behebung von Störungen und IT-Notfällen. Dabei soll die Beeinträchtigung IT-gestützter Arbeitsabläufe (»Geschäftsprozesse«) angemessen und in einem wirtschaftlich vertretbaren Verhältnis auf ein Minimum reduziert werden.

Der Umgang mit IT-Notfällen stellt, wie auch andere qualitätssichernde Abläufe, einen kontinuierlichen Verbesserungsprozess dar. Es ist daher enorm wichtig, dass die Geschäftsführung das IT-Notfallmanagement initiiert und die notwendigen Ressourcen zur Verfügung stellt. Existiert bereits eine allgemeine Notfallstrategie, sollte diese um IT-Notfälle erweitert und innerhalb einer Leitlinie zum Ausdruck gebracht werden. Anschließend können die Ziele durch interne Bestimmungen konkretisiert werden.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat für das IT-Notfallmanagement den Standard 100-4 entwickelt, der eine gute Orientierung für den Aufbau eines entsprechenden Konzepts bietet.

Das Kerngeschäft analysieren

IT-Notfallmanagement setzt dabei nicht bei den IT-Systemen selbst an, sondern verfolgt einen prozessorientierten Ansatz. Dazu müssen zunächst alle kritischen IT-gestützten Geschäftsprozesse identifiziert und einzeln bewertet werden. Im Rahmen einer »Business Impact Analyse« werden wesentliche Kernprozesse analysiert: Welche Folgen drohen, wenn Arbeitsabläufe beeinträchtigt sind oder gar nicht fortgeführt werden können?

Anhand individuell festgelegter Schadensszenarien wird untersucht, welcher Schaden durch die Beeinträchtigung der Arbeitsabläufe entstehen könnte. Die Auswirkung der Schadensszenarien kann durch verschiedene Schadenskategorien genauer bestimmt werden. Je höher die Auswirkung, umso größer ist der zu erwartende Schaden. Eine wichtige Rolle spielt ebenfalls der Schadensverlauf. Die ungewollte Beeinträchtigung könnte einen deutlich höheren Schaden nach vier Tagen oder einem Monat verursachen als innerhalb der ersten 24 Stunden.

Während der Schadensanalyse sind die maximal tolerierbare Ausfallzeit und die angestrebte Wiederanlaufzeit – also der Zeitrahmen für die Beseitigung einer Beeinträchtigung – für jeden Geschäftsprozess festzulegen. Erstere sollte immer höher sein, da ab diesem Zeitpunkt der zu erwartende Schaden in der Regel bereits die Überlebensfähigkeit einer Einrichtung gefährdet.

Ergänzend zu Einschätzung und Bewertung der Kernprozesse sind erforderliches Personal, IT-Equipment sowie weitere Ressourcen zu klären. Eine Herausforderung stellt dabei häufig die Berücksichtigung von Abhängigkeiten zwischen Arbeitsabläufen dar. Unterschieden werden sollte zwischen einem Normalbetrieb und einem Notbetrieb.

DOI: 10.5771/1613-0707-2017-1-28

Beispielsweise muss eine EDV-Pflegedokumentation nicht zwingend 24 Stunden am Tag verfügbar sein und kann im Notbetrieb zunächst auf Papier erfolgen.

Im nächsten Schritt gilt es relevante Ursachen und Gefährdungen für IT-Ausfälle und ihre bereits ermittelten Folgen zu identifizieren und die damit verbundenen Risiken zu bewerten. Grundlage der Untersuchung sind nun nicht mehr die Geschäftsprozesse allein, sondern auch die für die Arbeitsabläufe benötigten IT-Systeme (Ressourcen). Wird ein Ausfall der EDV-Pflegedokumentation als Risiko des Arbeitsablaufs eingestuft, müssen die möglichen Ursachen dafür gefunden werden.

Zur Unterstützung der Risikoidentifikation bieten sich die Gefährdungskataloge des BSI-IT-Grundschutzes an. Diese Sammlung enthält eine große Auswahl an möglichen Ursachen für eine Reihe von verschiedenen Gefährdungsklassen, wie höhere Gewalt (Feuer, Diebstahl, Personalausfall usw.) oder technisches Versagen (Datenverlust, Ausfall Active Directory usw.).

Grundsätzlich können nicht alle Risiken identifiziert werden, sodass der Umfang dieser Analyse auf ein gesundes Maß beschränkt werden sollte. Auch die Entwicklung von Szenarien, wie dem Ausfall der EDV-Pflegedokumentation, welchem verschiedene Risiken (Ausfall Hardware, Datenbankfehler usw.) zugeordnet werden können, erleichtert das gesamte Handling und reduziert die Anzahl der notwendigen IT-Notfallpläne. Hierbei kann vor allem auf den internen Erfahrungsschatz zurückgegriffen werden.

Im Rahmen der Bewertung von Risiken wird die Wahrscheinlichkeit des Eintretens in Bezug zu den erwartenden Schäden gesetzt, welche zuvor im Rahmen der Schadensanalyse untersucht worden sind. Die Wahrscheinlichkeit sollte, wie schon die Schadensszenarien, in mehrere Kategorien unterteilt werden, da Gefährdungen durchaus täglich oder nur einmal in zehn Jahren eintreten können.

Notfälle meistern

Auf Grundlage der erfolgten Untersuchungen lassen sich jedem Risikoszenario bereits bekannte Schwachstellen zuordnen und somit Maßnahmen zur Vorsorge und Behebung von IT-Notfällen ableiten. Für alle kritischen Beeinträchtigungen sind IT-Notfallpläne das richtige Werkzeug. Konzentrieren sollte man sich vor allem auf die sogenannten »Single-Point-of-Failure«. Mit zunehmender Virtualisierung lässt sich die Hochverfügbarkeit von IT-Diensten zwar immer leichter realisieren, was passiert allerdings, wenn die Klimatisierung der Serverräume oder zentrale Netzwerkverteiler ausfallen? Solche Störungen beeinträchtigen womöglich die gesamte Organisation aber zumindest die abhängigen Arbeitsabläufe und Ressourcen.

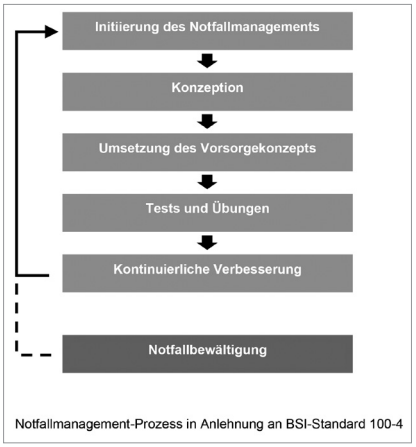
Ein möglichst unterbrechungsfreier Produktivbetrieb lässt sich nur mit einem hohen Aufwand und Budget gewährleisten, sodass für bestimmte Komponenten bevorzugt ausreichend Ersatzteile vorgehalten werden sollten. Die Durchführung einer Kosten-Nutzen-Analyse kann bei der Priorisierung von Risiken zur Entscheidungsfindung beitragen. Nicht zu unterschätzen ist auch das Know-how des zuständigen Personals. In die IT-Notfallpläne sind Kontaktdaten aller zuständigen Ansprechpartner, auch der externen Dienstleister, sowie Verweise auf relevante Informationen, wie Herstellerangaben, Konfigurationsdaten oder notwendige Zutrittsberechtigungen aufzunehmen.

IT-Notfallpläne sollten zudem so gestaltet werden, dass nicht nur ausgewiesene Wissensträger ihre Umsetzung einleiten und durchführen können – sie stehen nicht immer zur Verfügung. Die Dokumentation ist bei vielen Einrichtungen und Trägern nur sehr lückenhaft oder teils gar nicht vorhanden.

Wirksamkeit prüfen

Eine stets fehlerfrei durchgeführte Datensicherung hilft nicht, wenn die Informationen anschließend nicht wiederhergestellt werden können. Konfigurationsfehler und Lücken in der Datensicherung stellen sich meist erst dann heraus, wenn eine Wiederherstellung der Daten erforderlich wird. Wir empfehlen daher, eine vollständige Rücksicherung mit Wirksamkeitskontrolle regelmäßig durchzuführen, um für den Fall der Fälle gewappnet zu sein.

Ebenso wenig hilft eine unterbrechungsfreie Stromversorgung der IT-Systeme, wenn die Batterien bereits ihre maximale Lebensdauer erreicht haben oder kritische Komponenten gar nicht angeschlossen sind. Alle präventiven



Risikobasierte Gesamtkonzeption von Datenschutz und IT-Notfallmanagement.

Maßnahmen sollten regelmäßig überwacht und geprüft werden. Übungen zum Wiederanlauf von Arbeitsabläufen sind nicht trivial, kosten Zeit und somit auch Geld, dennoch stellen sie eine solide Möglichkeit zur Überprüfung der Wirksamkeit der Notfallvorsorge dar. Möglich ist es auch, mit einem simulierten Totalausfall, die gesamte Konzeption des IT-Notfallmanagement zu beginnen.

Das IT-Notfallmanagement erfordert keine gänzlich neue Herangehensweise. Geschickt mit anderen Dokumentationspflichten kombiniert, kann eine wirksame Organisation auch im Rahmen des Datenschutzes mit aufgebaut werden. Die Abbildung veranschaulicht eine entsprechende Herangehensweise.

Fazit

Steht die Geschäftsführung hinter dem IT-Notfallmanagement, ist bereits eine große Hürde überwunden. Wird das eigene Know-how unterschiedlicher Bereiche gebündelt, sind Schadensszenarien schnell identifiziert und die entsprechenden Risiken bewertet. Die Betrachtung einzelner Geschäftsprozesse sollte dabei möglichst subjektiv auf die tatsächlichen Vorgänge der eigenen Organisation ausgerichtet werden, denn Vorlagen oder allgemeine Empfehlungen könnten schnell an individuellen Arbeitsabläufen vorbeigehen.

Nicht vernachlässigt werden sollte die Nachsorge von Beeinträchtigungen. Eine genaue Untersuchung solcher Vorfälle führt unmittelbar zur Optimierung der eigenen Sicherheitsmaßnahmen. Schläft der kontinuierliche Verbesserungsprozess ein, ist das böse Erwachen vorprogrammiert. ■