Notfallkonzept

Vorbereitet auf die IT-Panne

Montagmorgen, 5 Uhr. Der wichtigste Server der Firma steht still. In wenigen Stunden beginnen die ersten Mitarbeiter an zu arbeiten. Nun gilt es, genau und schrittweise vorzugehen. Ein Notfallkonzept kann hier die notwendige Unterstützung liefern.

Autor: Andreas Wisler

Um grössere Schäden zu begrenzen oder diesen vorzubeugen, ist eine zügige und effiziente Behandlung von Sicherheitsvorfällen notwendig. Ein Notfallplan hat zum Ziel, die Geschäftstätigkeit während eines Ausfalls eines IT-Systems oder einer IT-Anwendung aufrechtzuerhalten und sicherzustellen (Business Continuity) sowie die Betriebsfähigkeit innerhalb einer tolerierbaren Zeitspanne wiederherzustellen (Business Recovery).

Dabei sind nicht nur die technischen Massnahmen zum Wiederanlauf zu beachten. Besonders wichtig ist die Planung im Vorfeld: Im Notfall muss es Verantwortliche mit klaren Kompetenzen geben. Zu einer guten Vorbereitung gehören ebenso Notfallschulungen und -übungen sowie eine stetige Pflege und Aktualisierung des Notfallplanes.

Definition

Der Ausfall eines IT-Systems in Folge eines Sicherheitsvorfalls kann zu einem Ausfall des gesamten IT-Betriebs führen. Auch der Ausfall von Komponenten der technischen Infrastruktur, beispielsweise Klimaanlage oder Stromversorgung, kann zu Störungen des IT-Betriebs führen. Technisches Versagen muss nicht zwingend die Ursache für den Ausfall von IT-Systemen sein. Ausfälle werden oft durch menschliches Fehlverhalten oder vorsätzliche Handlungen (z.B. Diebstahl, Sabotage, Viren-Angriff) verursacht. Auch durch höhere Gewalt können hohe Schäden eintreten.

Ein Sicherheitsvorfall stellt jedoch nicht zwangsläufig einen Notfall dar. Für einen Notfall gilt die folgende Definition: Ein Notfall tritt ein, wenn ein Zustand erreicht wird, bei dem innerhalb der geforderten Zeit eine Wiederherstellung der Verfügbarkeit nicht möglich ist und sich daraus ein Schaden ergibt (siehe dazu auch Blickpunkt KMU 4/06, Die drei «V» im IT-Sicherheitskonzept).

Wichtig ist, dass ein Notfall-Verantwortlicher ernannt wird. Dieser hat die folgenden Aufgaben:

- Erstellung und Pflege des Notfallvorsorgekonzepts
- Bewertung von Sicherheitsvorfällen
- formale Ausrufung und Beendigung des Notfalls
- Koordination der Notfallmassnahmen
- Dokumentation des Notfalls, Erstellung eines Abschlussberichts
- Unterrichtung der betroffenen Abteilungen sowie bei Bedarf der Geschäftsleitung
- Zusammenstellung und Einberufung eines Notfall-Teams
- Organisation und Vorbereitung von Notfallschulungen und Übungen
- Erhält im Notfall die nötigen Kompetenzen zur Wiederinbetriebnahme der IT (inkl. dem dazu notwendigen Budget)

Da schnelle Entscheidungen getroffen und Mitarbeiter vielleicht ausserhalb der normalen Arbeitszeit verständigt werden müssen, könnten Massnahmen notwendig werden, die vom normalen Arbeitsablauf abweichen und Sonderberechtigungen erfordern. In Notfällen müssen unter Umständen Beschränkungen und Sicherheitsvorkehrungen ausser Kraft gesetzt werden, um ein Problem schneller lösen zu können.

Die Folgen eines Ausfalls können verschiedene Stufen betreffen. Bei der ganzheitlichen Betrachtungsweise ist erkennbar, dass Geschäftskontinuität mehr umfasst als nur technisch bedingte Ausfälle von Ressourcen, nämlich auch den Schutz vor Angriffen, internen und externen kriminellen Handlungen, Fehlverhalten oder menschlichem Versagen. Alle diese Bedrohungen können letztlich zu einer Einschränkung oder Störung einzelner oder mehrerer Geschäftsprozesse und des regulären Geschäftsbetriebs bis hin zur Handlungsunfähigkeit führen.

Der Notfallprozess wird durch eine Störung ausgelöst. Diejenige Person, welche die Störung entdeckt, meldet dies an die verantwortliche Person (Hinweis: es ist notwendig, eine stets aktuelle Adressliste zu führen. Darin

Zum Autor

Andreas Wisler (Tel.: 052 320 91 20), Dipl. Ing. FH, CISSP, ISO 27001 Lead Auditor, ist Geschäftsführer der GO OUT Production GmbH, welche sich mit ganzheitlichen und produktneutralen IT-Sicherheitsüberprüfungen und -beratungen auseinandersetzt. Regelmässig veröffentlicht er einen informativen Newsletter zu aktuellen Sicherheitsthemen, der kostenlos und unverbindlich auf www.gosecurity.ch (Infonews) heruntergeladen werden kann. Im Rahmen des Swiss Security Days ist er für die Schulungen an der Klubschule Winterthur zuständig.

enthalten sind alle internen und externen Stellen, die in einen Notfall involviert sein können. Die verantwortliche Person entscheidet, ob es sich um einen Bagatellfall handelt oder ob die Störung eskaliert werden muss. Fall zwei tritt dann ein, wenn Geschäftsprozesse nicht mehr eingehalten werden können. Die verantwortlichen Stellen, die aktiv handeln oder Verantwortung übernehmen müssen, sind zu alarmieren (z.B. Feuerwehr, Hauswart, Administrator, IT-Sicherheitsmanagement).

Je nach Ausmass der Störung wird ab diesem Zeitpunkt das komplette Sicherheitsmanagement einbezogen. In einem ersten Schritt muss eine Beweissicherung aller Systeme durchgeführt werden. Die Lagebeurteilung definiert die nun folgenden Sofortmassnahmen. Alle Massnahmen, die selber und sofort getroffen werden können, sind auszuführen (Checklisten erstellen). Gleichzeitig mit den Sofortmassnahmen wird ein Zeitplan erstellt, in welchem die folgenden Schritte definiert werden. Die notwendigen Ressourcen sind sofort aufzubieten. Nachdem die Sofortmassnahmen ergriffen wurden sowie alle betroffenen Personen informiert sind, gilt es, eine zweite Lagebeurteilung durchzuführen. Das Ziel ist es, die getroffenen Sofortmassnahmen zu verfeinern und den Weg in den Normalbetrieb in die Wege zu leiten. Mit Hilfe der zweiten Lagebeurteilung wird entschieden, welche Massnahmen bis zur Lösung der Störung durchgeführt werden. Die getroffenen Massnahmen sind zu überwachen. Abweichungen oder neue Erkenntnisse fliessen in die nachfolgenden Massnahmen ein. Nach Behebung der Störung gilt es, die getroffenen Massnahmen schriftlich festzuhalten sowie Erkenntnisse in die vorhandenen Checklisten einfliessen zu lassen.

Für die Notfallbehebung wird zwischen zwei unterschiedlichen Methoden unterschieden:

Incident Management

Im laufenden Betrieb treten in der Regel immer wieder Fragen, Störungen und Probleme auf. Um Beeinträchtigungen des Geschäftsbetriebs zu minimieren und die Geschäftskontinuität aufrecht zu erhalten, muss der Umgang mit derartigen Ereignissen definiert und umgesetzt sein. Ziel muss es sein, das jeweilige Ereignis kurzfristig zu lösen, und sei es auch nur durch einen Reset oder in Form eines Workarounds. Es geht also nicht um Ursachenforschung und -behebung, sondern um Schnelligkeit.

Problem Management

Probleme gehören zum Lebenszyklus von Prozessen und Ressourcen. Regelmässige Reviews sollen diese frühzeitig erkennen und Massnahmen definieren, bevor es im Betrieb zu Problemen oder Beeinträchtigungen kommt. Probleme zu erfassen, zu untersuchen und eine langfristige Lösung zu suchen ist die Aufgabe des Problem-Managements. Wichtig dabei ist, bei Problemen und Notfällen eine schnelle und akzeptable Lösung zu finden und diese in einem zweiten Schritt genau zu untersuchen sowie Massnahmen zu deren Behebung zu definieren und umzusetzen. ◆