DuD
Datenschutz und Datensicherheit

Incident Management

Wilhelm Dolle

Die Bezeichnung Incident (Vorfall) ist an sich wertneutral. Primäres Anliegen bei der Reaktion auf solche Vorfälle sollte es also sein zu klären, ob ein Sicherheitsverstoß – beispielsweise ein Systemeinbruch – vorliegt oder ob es sich um eine „normale" Betriebsstörung handelt.

Betriebsstörungen

Nach dem recht allgemeinen Verständnis der ITIL (IT Infrastructure Library) ist ein Incident (hier eine Störung) ein Ereignis, das nicht zum standardmäßigen Betrieb eines Services gehört und das tatsächlich oder potentiell eine Unterbrechung oder eine Minderung der Service-Qualität verursacht. Ziel eines Incident Managements ist es in diesem Zusammenhang, die schnellstmöglichste Wiederherstellung des normalen Service-Betriebs bei minimaler Störung des Geschäftsbetriebs zu garantieren sowie das bestmögliche Niveau der Verfügbarkeit und Qualität des Services aufrecht zu erhalten. Teilprozesse innerhalb des Incident Managements sind dabei das Aufspüren und Klassifizieren von Störungen, das Verfassen von Störungsberichten, die Ermittlung der Ursache der Störung sowie deren Behebung und die Wiederherstellung des Services.

Sicherheitsvorfälle

Betrachtet man Incident Management mit der Brille der IT-Sicherheit, so findet man unter anderem bei der Fachgruppe „Security – Intrusion Detection and Response" (SIDAR) [1] der Gesellschaft für Informatik eine brauchbare Definition der Aufgaben: Incident Management beschreibt hier den gesamten organisatorischen und technischen Prozess der Reaktion auf erkannte und vermutete Sicherheitsvorfälle in IT-Bereichen sowie hierzu vorbereitende Maßnahmen und Prozesse. Dabei umfasst das Spektrum möglicher Aufgaben für das Incident Management nicht nur technische Probleme, Schwachstellen und konkrete Angriffe auf die IT-Infrastruktur, sondern ebenso organisatorische und rechtliche Fragestellungen.

Wird ein echter Sicherheitsvorfall diagnostiziert, müssen in der Regel sofort die entsprechenden Reaktionen (Incident Response) eingeleitet werden. Typischerweise bedient man sich dabei Methoden der Computer-Forensik [2], um den angerichteten Schaden, den Angriffsvektor[1] und die mögliche weitere Gefährdung der Organisation zu ermitteln. Ein erfolgreich und ordnungsgemäß durchgeführtes Incident-Response-Verfahren ist zudem die Grundlage für eine eventuelle juristische Verfolgung, aber auch für die Klärung von Streitfällen. Erfolgt das Vorgehen beispielsweise nicht nach gängigen Best-Practice-Verfahren und wird nicht hinreichend sorgfältig dokumentiert, so können bei einer späteren Ermittlung oder bei einem Gerichtsverfahren Zweifel an Herkunft, Besitztum oder Unversehrtheit der gefundenen Beweise bestehen.

Aufgabe des Incident Managements ist es dabei, den Verantwortlichen einer Organisation die Planungswerkzeuge an die Hand zu geben, um die nötigen Vorarbeiten zu erkennen und durchzuführen, damit im Falle des Incidents ohne zeitliche Verzögerung effektive und effiziente Maßnahmen zum Schutz der Organisation ergriffen werden können. Die organisatorischen Vorarbeiten umfassen unter anderem die Erstellung einer Sicherheitsrichtlinie sowie eines Notfallsplans nebst Entscheidungs- und Verantwortlichkeitsstrukturen, Schulungen, um das Sicherheitsbewusstsein der Mitarbeiter zu schärfen, Regeln für das Melden eines Incidents durch die Mitarbeiter, Sicherheitsmonitoring- und Alarmierungskonzepte für das technische Personal und die Bildung eines CSIRTs (Computer Security Incident Response Teams) [3].

Auch wenn Incident-Response-Pläne das Eintreten eines Schadens nicht unbedingt verhindern können, so ermöglichen sie in vielen Krisensituationen, durch schriftlich fixierte Abläufe den Überblick zu behalten, professionell und angemessen zu reagieren und weiteren Schaden von der Organisation abzuwenden. Das Fehlen eines solchen Plans ist ein bei Sicherheits-Audits häufig aufgedeckter Fehler und ein deutlicher Hinweis auf unzureichendes Incident Management.

[1] Weg, den der Eindringling bei seinem Einbruch in den fremden Computer genommen hat, um dessen Sicherungsmaßnahmen zu umgehen.

Datenschutzaspekte

Da das Erkennen eines Sicherheitsvorfalls nicht ohne die Erfassung und Auswertung von protokollierten Daten auskommt, muss man sich beim Planen einer Incident-Response-Strategie auch zwangsläufig mit den geltenden Grundsätzen des Datenschutzes auseinandersetzen. Das Prinzip der Datenvermeidung gebietet es, weitestgehend auf das Verarbeiten von personenbezogenen Daten zu verzichten bzw. – wo ein vollständiger Verzicht nicht zu erreichen ist – den Umfang der gespeicherten Daten möglichst gering zu halten. Sofern sinnvoll realisierbar, sollten personenbezogene Daten, die für das Incident Management erhoben werden, entweder anonymisiert oder pseudonymisiert, also nur durch spezielle Zuordnungsregeln einer Person zuordenbar, abgelegt werden. Das Protokollieren von Daten darf außerdem nur in dem Umfang erfolgen, wie es für die Erkennung von Sicherheitsvorfällen und deren eventuellen Aufklärung erforderlich ist, und ist streng zweckgebunden. Die Kontrolle des Datenschutzes und der Datensicherheit, und damit auch die Auswertung der Protokolldaten, obliegt normalerweise dem betrieblichen oder behördlichen Datenschutzbeauftragten. Er sollte nicht nur bei einer Auswertung im Rahmen eines Incidents informiert, sondern möglichst schon beim Erstellen der Incident-Response-Strategie eingebunden werden.

Literatur

[1] GI-Fachgruppe SIDAR, http://www.gi-fb-sicherheit.de/fg/sidar/
[2] Fox, Kelm, Gateway, DuD 8/2004, S. 491
[3] Handbook for CSIRTs, http://www.sei.cmu.edu/publications/documents/03.reports /03hb002.html

Wilhelm Dolle ist Director Information Technology und Mitglied der Geschäftsleitung, interActive Systems GmbH, Berlin sowie Mitglied der GI-Fachgruppe SIDAR.