Der Gesetzgeber will hohe Ansprüche erfüllt sehen

ITSM-Tools unterstützen das Sicherheits-Management

Die Verabschiedung des IT-Sicherheitsgesetzes stellt viele Institutionen vor hohe **Anforderungen an ihre IT-Systeme** und ihre Sicherheit. Die Grundlagen, den Vorgaben zu entsprechen, lassen sich bereits jetzt legen.

Mitte Juni 2015 hat der Bundestag das IT-Sicherheitsgesetz verabschiedet. Es geht weit über die Vorschriften des Bundesdatenschutzgesetzes hinaus.

So benennt es unter dem Kürzel KRITIS kritische Infrastrukturen, zu denen nicht nur Behörden und Sicherheitsorgane zählen. Vielmehr erstreckt es sich auch auf Energieversorgung, Transport und Verkehr, das Finanzwesen, das Gesundheitswesen, Wasserversorgung, Ernährung und nicht zuletzt die Informations- und Telekommunikationstechnik. In allen diesen Bereichen ist künftig sicherzustellen, dass es nicht zu schweren Beeinträchtigungen ihrer Funktion kommen kann.

Auf Seiten der Informationstechnik haben die angepeilten Maßnahmen vordergründig den Fokus: Für das Sicherheitsmanagement sollen geeignete Systeme und Maßnahmen nicht nur Angriffen von außen vorbeugen, sondern auch interne Schwachpunkte identifizieren. Hierzu zählen beispielsweise die Zugangssicherung, eine Notstromversorgung oder der Zugriffsschutz, um Manipulationen durch Unberechtigte vorzubeugen.

Zwei Rahmenwerke beschreiben diese Anforderungen: BSI Grundschutz ist ein Katalog von verschiedenen Methoden und Maßnahmen, der mit einem Umfang von 4600 Seiten die Orientierung schwer macht. Die Norm ISO 27001 enthält hingegen weniger konkrete Vorgaben, sondern ist ergebnisorientiert, wodurch sie organisationsspezifische Handlungsspielräume lässt.

Mit der Software „verinice“ vom Göttinger Hersteller Sernet gibt es ein Tool, das es deutlich erleichtert, den Maßnahmenkatalog nach BSI Grundschutz in der Praxis umzusetzen.

Bild: GISA GmbH

Höchste Anforderungen an die Sicherheit im Betrieb

Neben diesen Rahmen tritt die Sicherung dessen, was in der IT geschieht. Es geht also um ihre eigentliche Funktion, um die Prozesse in Rechenzentren. Tools für das IT Service Management (ITSM) beschreiben diese.

Zugleich ermöglichen sie es, Schwachstellen und sich abzeichnende Schwierigkeiten frühzeitig zu erkennen und zu beheben. Diese Service Management Systeme lassen sich weit über die unmittelbare IT hinaus für das Sicherheitsmanagement verwenden.

Das Zentrum von ITSM-Lösungen ist die Configuration Management Database (CMDB), in der alle – auch für die Sicherheit – relevanten Elemente fortlaufend dokumentiert und klassifiziert sind. Das können Gebäude und Räume sein, Sicherungssysteme, Rechner, Software, Netzwerk-Infrastruktur etc. Zusätzlich ist in ihnen festgehalten, in welchem Zusammenhang sie stehen, welche Rolle sie also in den IT-Prozessen spielen.

Beispiel: Der Ausfall eines Netzwerksystems für eine zentrale Fachanwendung löst bei der ITSM-Software einen Alarm aus, in dessen Folge unter anderem auch die sicherheitsseitigen Auswirkungen auf den zentralen Fachservice bewertet werden können. Gleichermaßen bietet es mit der CMDB die Basis für die Modellierung der Sicherheitskonzeption und die sich daraus ergebenden Sicherheitsmaßnahmen.

Ein ITSM-System erfüllt also mehrere Ansprüche, die sich aus dem IT-Sicherheitsgesetz ergeben werden: Es dokumentiert die vorhandene Situation und stellt damit sicher, dass die zahllosen technischen und organisatorischen Grundlagen überhaupt erfüllt sind. Es vollzieht Änderungen mit und lässt erkennen, ob die vorgesehenen Maßnahmen überhaupt umgesetzt sind und noch greifen. Es automatisiert die Prozesse bei Verletzung des Soll-Zustands und leitet Gegenmaßnahmen ein.

Schließlich ist all das dokumentiert und damit beweiskräftig nachprüfbar. Als zügig in spezifischen Sicherheitsanforderungen einsetzbares Produkt bietet c.a.p.e. IT das in der IT und in der Überwachung industrieller Anlagen bewährte ITSM-System „KIX4OTRS“ an. Für die Anforderungen des IT-Sicherheitsgesetzes integriert es „verinice“ und hilft somit u.a. die Vorgaben nach dem BSI Grundschutz zu erfüllen. GISA ist ein auf diese Umgebung spezialisierter IT-Dienstleister, der durch individuelle Beratung bei der sachgerechten Sicherheitskonzeption und deren Implementierung unterstützt.

Die Autoren:

Rico Barth, Mitbegründer und Geschäftsführer der auf IT Service Management spezialisierten c.a.p.e. IT GmbH, Chemnitz

Stefan Planert, Berater für IT-Prozesse und IT-Sicherheit im Bereich eGovernment der GISA GmbH, Halle.

GISA und c.a.p.e. sind Partner im Bereich IT-Service- sowie -Sicherheitsmanagement.