IT-Sicherheitsstandards im kommunalen Bereich

Das Sicherheitskonzept des LWL-Bau- und Liegenschaftsbetriebes

„IT-Systeme sind mittlerweile ein wesentlicher Bestandteil unseres privaten und geschäftlichen Lebens. Ebenso, wie sich dieses private und geschäftliche Tun verändert, wachsen und verändern sich die Anforderungen an die IT-Anwendungen. Daher müssen die IT-Systeme regelmäßig auf den Prüfstand gestellt und bei Bedarf den neuen Gegebenheiten angepasst oder sogar ausgetauscht werden", sagt Prof. Dr. Bertil Haack im gemeinsamen IT&I Interview mit Georg Fehlauer.

IT&I: Wie kam es zur Einführung von PROMOS.CITY beim LWL-BLB?

Georg Fehlauer: Der Landschaftsverband Westfalen-Lippe - Bau- und Liegenschaftsbetrieb (LWL-BLB) stand vor der Aufgabe, innerhalb von drei Monaten Liegenschaften mit rund 250 Gebäuden (Bürogebäude, Schulen, Museen) verteilt in Westfalen-Lippe in sein Sondervermögen zu übernehmen, im Rahmen eines Vermieter/Mietermodells zu bewirtschaften und ein kaufmännisches Rechnungswesen zu implementieren. Zur Unterstützung wurde mit **PROMOS.CITY** – der Musterlösung für das Management kommunaler Immobilien und Liegenschaften – eine Software zur Immobilienbewirtschaftung eingeführt.

IT&I: Welche Bedeutung hatten dabei Sicherheitsüberlegungen?

Herr Fehlauer: Im Zuge derartiger Anpassungs- oder Migrationsvorgänge muss den IT-Sicherheitsstandards höchste Priorität eingeräumt werden: Jeder Kunde, jedes Unternehmen, jeder Betrieb fordert zu Recht, dass die entsprechenden Anwendungen ordnungsgemäß laufen und arbeiten. Dies gilt insbesondere dort, wo es um Geld geht. Hier sind entsprechende Sicherheitsstandards für die Abwicklung datentechnisch gestützter zahlungs- und betriebsrelevanter Vorgänge notwendig und einzuhalten – und zwar in jeder Implementierungsphase der Software. Kommt dieser Betrieb so wie der LWL-BLB aus dem Bereich des öffentlichen Dienstleistungssektors, sind zudem spezielle haushalts- und kassenrechtliche Vorschriften mit zu berücksichtigen.

IT&I: Wie sind Sie mit diesen Überlegungen umgegangen? Welche Schlussfolgerungen haben Sie gezogen?

Herr Fehlauer: All diese Forderungen in einem Paket zu bewältigen, wäre in der Kürze der Zeit nicht möglich gewesen, zumal die Umsetzung aus eigener Kraft, ohne Aufstockung des eigenen Personals, zu bewältigen war und neben der täglich laufenden Arbeit erledigt werden musste. Deswegen waren Prioritäten zu setzen. Einerseits war in jedem Moment des Projektes für die Einhaltung von Mindeststandards hinsichtlich der IT-Sicherheit zu sorgen, um das geforderte Maß an Sicherheit gegen Manipulationen und kriminelle Handlungen zu realisieren. Andererseits ging es darum, die jeweiligen Verfahrensabläufe und Systemeinstellungen Schritt für Schritt zu optimieren und so auch die erforderliche Effizienz der eingeführten Regelungen zu erreichen. Auf eine einfache Formel gebracht: Zum Stichtag der Systemumstellung mit einem Höchstmaß an IT-Sicherheit nur das einzuführen, was unbedingt betriebsnotwendig ist; alles, was sukzessive einzuführen oder zu verbessern war, wurde konsequent nach dem Stichtag datiert.

Buchcover

IT&I: Können Sie dies konkretisieren?

Herr Fehlauer: Mit der Implementierung eines neuen IT-Systems gehen im hier betrachteten Kontext immer wenigstens zwei Fragen einher:

a) Wie soll mit diesem System gearbeitet werden, d. h. bleiben die Geschäftsprozesse und Zuständigkeiten wie bisher oder sind Änderungen erforderlich? Welche sind das? Wie sehen die Ergebnisse aus?

b) Wie muss die Software auf diese Festlegungen ausgerichtet werden, d. h. welche sicherheitsrelevanten Einstellungsmöglichkeiten bietet sie, welche Einstellungen sind vorzunehmen?

Hier gibt es sicher eine Vielzahl von Antworten. Die Arbeitsprozesse können in verschiedener Weise modelliert und angepasst und die „Stellschrauben" von **PROMOS.CITY** entsprechend „angezogen" werden. Dabei müssen die Sicherheitsvorgaben restriktiv ausgelegt werden. In der Praxis ergeben sich vielfältige Fragen. Werden optimierte betriebliche Abläufe durch überhöhte Sicherheitsvorgaben gehemmt, wie viel Sicherheit ist nötig, wie sinnvoll sind die getroffenen Maßnahmen, wie sieht es mit dem Kosten-Nutzen-Verhältnis aus? Hier hat der LWL-BLB einen auf den Betrieb abgestimmten Weg gesucht und gefunden!

IT&I: Warum das Buch?

Prof. Dr. Bertil Haack: Zahlreiche Kommunen stehen vor ähnlichen Aufgaben wie sie der LWL-BLB in den letzten Wochen und Monaten gemeinsam mit seinen Partnern gelöst hat. Bei den geführten Gesprächen wurde deutlich, die Probleme sind gleichlautend. ▶

IT&I: Welches Ziel verfolgt das Buch also? Wem nutzt es und was ist neu?

Prof. Dr. Bertil Haack: Auf Vorschlag des LWL sollen mit diesem Buch Antworten aus der Praxis für die Praxis vorgestellt werden. Es sollen Anregungen insbesondere für Unternehmen im kommunalen Umfeld gegeben werden, wie sie auch und gerade in einem durch mannigfache Anforderungen geprägten Umfeld zu einem passenden – und damit auch praktikablen – Sicherheitskonzept im Bereich der IT-gestützten zahlungs- und betriebsrelevanten Vorgänge kommen können.

Dabei geht es nicht primär darum, einen einheitlichen Sicherheitsstandard zu definieren. Dies ist schwierig, weil z. B. für einen kaufmännisch orientierten Betrieb, wo der monetäre Zahlvorgang im Vordergrund steht, ein zu erarbeitendes Sicherheitskonzept anders ausgerichtet sein muss als z. B. für ein Unternehmen aus dem Gesundheitsbereich, wo es um schutzwürdige Patientendaten geht. Entsprechende Sicherheitsanforderungen und auch die dafür notwendigen Kontrollen und Prüfungen sind daran anzupassen. Zudem ist die Eigenart des Betriebes mit zu berücksichtigen. Aufgaben, Organisation und das eingesetzte Personal sind zusätzliche Faktoren, die ein Sicherheitskonzept beeinflussen.

An Stelle einer allgemein gültigen Lösung sollen hier viel mehr ein gangbarer Weg und dessen Ergebnisse vorgestellt werden, wie sie beim LWL-BLB gemeinsam mit dessen Partnern entwickelt und eingeführt wurden und sich zwischenzeitlich in der Praxis bewährt haben.

Den Lesern und Leserinnen dieses Buches sollen hiermit Empfehlungen, Orientierungshilfen und Materialien an die Hand gegeben werden, mit denen sie den in der Nutzung ihrer IT-Systeme immanenten Risikopotenzialen begegnen können. Im besten Fall – und das ist das Neue und zugleich die Hoffnung, die wir mit diesem Buch verbinden – sollen die vorliegenden Materialien als Muster dienen, die die Leser und Leserinnen ohne übermäßigen Aufwand modifizieren können, um so zu einem angemessenen IT-Sicherheits-konzept für ihr eigenes Unternehmen zu kommen.

Das Buch ist für 14,90 € über den deutschen Buchhandel zu bestellen.
ISBN 3-938663-00-6
50 Seiten

Georg Fehlauer
Projektverantwortlicher beim LWL-BLB
Landschaftsverband Westfalen-Lippe
LWL-Bau- und Liegenschaftsbetrieb
Georg.Fehlauer@lwl.org

Prof. Dr. Bertil Haack
Koordinator des Sicherheitskonzeptes
G&S Goals & Strategies GmbH, Berlin
info@goals-strategies.com

IMPRESSUM

Herausgeber
Jens Kramer
j.kramer@openpromos.com

Redaktion und Anzeigen
Manuela Lange
m.lange@openpromos.com

Layout und Produktion
Gabriele Keller
g.keller@openpromos.com

Anschrift
PROMOS PRESS
Rungestraße 19
10179 Berlin-Mitte
redaktion@openpromos.com
www.openpromos.com

Repro und Druck
DMP
Digital Media Production

IT&I erscheint halbjährlich im Frühjahr und im Herbst.

Die Zeitschrift erscheint als Beilage zu Fachzeitschriften bzw. wird direkt versandt. Darüber hinaus können Sie IT&I auch im Abonnenten-Service direkt beziehen. Die Porto- und Abwicklungsgebühr beträgt pro Ausgabe 4,50 Euro bzw. 8,50 Euro im Ausland.

ISSN 1610-6644