NIFIS e.V.

Meldedaten offen im Internet – NIFIS empfiehlt einfache Maßnahmen zum IT-Grundschutz

Thomas Teichmann

27. Juni 2008

Meldedaten offen im Internet: Die Verantwortung für die Einhaltung des Datenschutzes liegt beim Betreiber

Das Fernsehmagazin ARD Report aus München berichtete am Montag, den 23. Juni 2008 von einem schwerwiegenden Fall der Verletzung des Datenschutzes bei Behörden. Die Journalisten hatten offene Zugänge zu Meldedaten bei den Meldeämtern verschiedener Städte und Gemeinden festgestellt. Der Zugang zu einem Auskunftssystem war nur mit dem Startbenutzer und Startkennwort des Softwarelieferanten geschützt, und der Softwarelieferant hatte diese Angaben zeitweise auf seiner Website unter dem LInk zu den Installationen öffentlich einsehbar gemacht.

Dieser scheinbar offenkundige Fehler des Softwarelieferanten hat viele Bürger aufschreien lassen. Sogar die betroffenen Behörden äußerten sich erbost - über den Lieferanten. Dies lenkt aber vom eigentlichen Problem ab.

Es muss festgestellt werden, dass die Verantwortung für die Einhaltung des Datenschutzes beim Betreiber eines Informationssystems liegt, nicht beim Lieferanten. Wenn eine Behörde oder ein Unternehmen eine Datenbank einrichtet mit personenbezogenen Daten, müssen die Verantwortlichen auf die Einhaltung von Datenschutzbestimmungen achten und bestehen. Wer unsicher ist, kann sich informieren, oder einen Berater hinzuziehen, oder bei NIFIS nachfragen. In diesem spektakulären Fall lag für das installierte System ein Kurzgutachten des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein vor, das dem System eine datenschutzrechtlich einwandfreie Funktionsweise attestiert. Das ist gut, aber es bezieht sich auf das Grundsystem und Konzept, nicht auf die einzelne Installation in einem Meldeamt. Was die Datenschutzprüfer nicht zu prüfen hatten, und nicht ahnen konnten, ist, dass die Installateure das System wohl regelmäßig mit einem Standardbenutzer und Standardstartkennwort installierten, und die Kommunen es dabei beließen, und in vilelen Kommunen weder Datenschutz noch IT-Grundschutz geprüft wurden..

Startkennworte, die bei Lieferung und Installation eines Systems eingesetzt werden, sind generell unsicher. Zu viele Leute, vom Entwickler bis zu Pilotanwendern, kennen diese Zugangsdaten. Es gibt spezialisierte Websites für Standardkennworte. Daher wird ein erfahrener Softwareinstallateur nicht nur empfehlen, diese Zugangsdaten direkt nach der Installation zu ändern, er wird darauf bestehen.

Damit Ihnen das nicht geschieht: Ein paar praktische Empfehlungen

Der Umgang mit Benutzernamen und Kennwörtern muss genauso sorgfältig sein wie der mit Schlüsseln zu Tresorräumen. Dies gilt insbesondere für Informationssysteme, die über das Internet erreichbar sind. Werden personenbezogene Daten bereitgestellt, gelten die rechtlichen Anforderungen des Bundesdatenschutzgesetzes (BDSG). Um wirtschaftlichen Schaden durch unbefugte Nutzung von Diensten oder Datenklau zu vermeiden, sollten die Maßnahmenkataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI) herangezogen werden.

Ein paar grundsätzliche Maßnahmen empfehlen wir aufgrund dieses aktuellen Beispiels.

1. Noch vor der ersten Installation sollte ein Konzept für die Verwaltung der Benutzerrechte, Benutzernamen und Kennworte erstellt werden, etwa als Teil des Pflichtenhefts.

2. Mit der ersten Übernahme "echter" Daten, auch für Tests und Schulungen, sollte im selben Zug nur noch mit Benutzernamen und Kennworten nach dem Rechtekonzept gearbeitet werden.

3. Standardbenutzer sollten ab der Installation geändert werden. Verschiedene Systeme haben dafür verschiedene Vorgehensweisen. Kunden sollten darauf bestehen, dass dies durchgeführt wird.

4. Lieferanten sollten Systeme nur für den Betrieb übergeben, wenn der Kunde seine eigenen Kennungen eingegeben hat, und der Startbenutzer entfernt oder inaktiviert wurde.

5. Zugang zu und Nutzung von Informationssystemen trennen und getrennt verwalten:

   - in den Aufbau der Verbindung zum Informationssystem, etwa durch Zuordnung eines Schlüssel für eine gesicherte Verbindung.

   - in die Benutzerverwaltung des eigentlichen Informationssystems.

   So kann ein Vier-Augen-Prinzip installiert werden. Wenn dann an einer Stelle ein Fehler eintritt, bleibt ein Schutz erhalten.

Dies sind einzelne praktische Maßnahmen, die wir jedem empfehlen. Sie können nicht die IT-Grundschutzkataloge ersetzen, und sie können auch nichts daran ändern, dass die Verantwortung für den Datenschutz oder auch wirtschaftlichen Selbstschutz beim Betreiber liegt. Sie können aber denjenigen, die der Bericht von Report überrascht hat, ermuntern, einen ersten Schritt zur Verbesserung von Datenschutz und IT-Sicherheit zu gehen.

Es ist das Anliegen der NIFIS, durch solche Hinweise die Sicherheit von Internet und Informationssystemen durch eigene Initiative zu verbessern.

Die NIFIS e.V.

Die Nationale Initiative für Informations- und Internet-Sicherheit (NIFIS e.V.) ist die Selbsthilfeorganisation der Wirtschaft, um Unternehmen im Kampf gegen die wachsenden Gefahren aus dem Internet technisch, organisatorisch und rechtlich zu stärken. Als neutrale und unabhängige Organisation verbindet die NIFIS Wirtschaft, Wissenschaft und Politik und fungiert als Plattform für einen branchenübergreifenden und interdisziplinären Erfahrungsaustausch.

In prominent besetzten Beiräten unterstützen verschiedene Bundespolitiker und Professoren die Arbeit der Initiative.

Weitere Informationen: NIFIS e.V., Weismüllerstraße 21, 60314 Frankfurt, Tel.: 069 40 80 93 70, Fax: 069 40 14 71 59, E-Mail: nifis@nifis.de, Web: www.nifis.de

Thomas Teichman

Thomas Teichmann ist Berater für IT-Sicherheit und Organisation und Geschäftsführer der Schmitz & Teichmann Betriebsberatung GmbH - www.schmitzteichmann.de - und Mitglied im Expertenkreis Business Continuity Management der Nationalen Initiative für Informations- und Internetsicherheit (NIFIS e.V.) - www.nifis.de.