Themen: Datenzugriff
Berufe: IT-Abteilung
Datentypen: Geschäftliche Daten

Wie müssen Datenbanken geschützt werden?

Ein Datenbankadministrator verwaltet eine Datenbank auf einem Enterprise-Resource-Planning-System.
Er möchte Daten, auf die er den Zugriff hat, kopieren, um sie entweder direkt in Tabellenform lesen oder sich interaktiv mit dem System verbinden zu können.
Er ist sich mit seinem Vorgesetzten uneinig und beschliesst, selbst zur Tat zu schreiten. Er ändert vorübergehend das Passwort, deaktiviert das Auditprotokoll und nimmt Änderungen in den Dokumenten vor.
Um diesem Katastrophenszenario, dem Datenraub, vorzubeugen, hätte die IT-Abteilung folgende Massnahmen ergreifen können: Verschlüsselungen des Datenflusses, sichere Konfigurierung des Servers und des Betriebssystems, Regelung der Zugriffsrechte, Zutrittskontrolle für die Gebäude und Schulungen der Mitarbeiter.
Man kann nie vorsichtig genug sein, vor allem bei der Benutzung von komplexen Enterprise-Resource-Planning-Systemen, bei denen der Datenschutz zum Zeitpunkt der Projektkonzeption nicht vorgesehen ist!

Empfehlungen
Der Inhaber der Datensammlung ist für die Sicherheit der von ihm verarbeiteten Daten verantwortlich. Er muss konkrete Risiken einschätzen können und die angemessenen Massnahmen ergreifen. Er muss gegebenenfalls sogar so weit gehen, befugten Personen die Benutzung ihres Mobiltelefons oder eines USB-Sticks zu verbieten.

Grundprinzipien
StGB 143, 179ss et 321ter ; OR 328 et 328*b*

Datensicherheit.

Praxisbeispiel
cf. Leitfaden des EDÖB:

https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden/technische-und-organisatorische-massnahmen-des-datenschutzes.html