

# Gegen langfingrige IT-Mitarbeiter

Unternehmen sollten die Gefahr von Datenmissbrauch durch eigene IT-Fachleute nicht unterschätzen. Verfahren zur Datenverschlüsselung helfen, das Risiko einzuschränken.

VON RETO FANKHAUSER

Viele erinnern sich gut: Im Dezember 2009 erregte ein Vorfall bei einer der weltweit grössten Banken, der HSBC, grosses mediales Aufsehen. Der Informatiker, Hervé Falciani, hatte die Identitäten und Profile tausender Kundenkonten entwendet und anscheinend verschiedentlich versucht, diese zu verkaufen. Bis heute ist unklar, wie er sich die Daten beschafft hat: War es der Coup eines Datenbankexperten oder hat lediglich ein herkömmlicher Informatiker die Gunst der Stunde genutzt und bei einer Datenmigration unverschlüsselte Daten kopiert? Auch ob er für die Daten bezahlt wurde oder nicht, ist bis heute unklar. Offenkundig ist jedoch, dass Datendiebstahl durchaus lukrativ sein kann und der Fall der HSBC kein Einzelfall war, wie die Berichterstattung der letzten Monate zeigt. Die Wahrscheinlichkeit, mit der sich ein solcher Vorfall ereignet, steigt mit dem Marktwert der Daten und wird zusätzlich durch äussere Umstände, wie etwa die Finanzkrise, verstärkt.

Im «Data Loss Barometer» der KPMG wird das Gefahrenpotential des internen Personals wie folgt präzisiert: Die Kombination aus wirtschaftlichem Druck und der Versuchung durch Angebote krimineller Organisationen und Akteure führt dazu, dass gewisse Angestellte den Diebstahl als gangbare Option betrachten. Motivationen für Datendiebstähle sind entweder ein finanzieller Gewinn, ein kompetitiver Vorteil oder aber Sabotage.

## Neue Regularien und Sicherheits-Features

In den letzten Jahren haben europäische und amerikanische Verwaltungen verschiedene Gesetze und Richtlinien erlassen, die von Unternehmen und Organisationen zusätzliche Schutzmassnahmen für personenbezogene Kundendaten verlangen. Daraus resultierend bieten viele Hersteller von Datenbanklösungen in ihren Produkten «onboard» Sicherheits-Features zum verstärkten Schutz der gespeicherten Daten an. Diese Features beinhalten einerseits Mechanismen zur restriktiven Beschränkung des Zugriffs der einzelnen Benutzer auf die Daten, so dass nicht jeder Zugriff auf alle Daten hat. Andererseits wird mit einer (transparenten) Verschlüsselung der gespeicherten Daten gearbeitet. Hacker können eventuell eine Datenbankdatei ergattern, diese ist jedoch wertlos, weil die enthaltenen Daten nicht entschlüsselt werden können. Beide Mechanismen schützen jedoch nicht per se vor dem Missbrauch durch das IT-Personal, das sowohl über die Zugriffsrechte wie auch die Verschlüsselung Kontrolle hat.

## IT-Mitarbeitende als Gefahrenpotential

IT-Mitarbeitende haben, je nach Rolle, privilegierte Zugriffe auf die verschiedenen IT-Systeme. Bei der Beurteilung des Gefahrenpotentials stehen zwei Verantwortungsbereiche im Zentrum:

- Die Datenbank-Administratoren (DBAs): Sie verwalten die Datenbanken im Unternehmen und haben Zugriff auf die Daten, die in den verwalteten Datenbanken abgelegt werden.
- Die Systemadministratoren: Sie können Applikationen installieren (und modifizieren). Sie haben Zugriff auf die Konfigurationsparameter von Applikationen, darunter Zugangsdaten von Datenbankkonten. Weiter können sie oftmals (wie auch Netzwerkadministratoren) die Kommunikation auf dem Netzwerk belauschen.

Wurden früher Kundendaten in physischer Form in sicher verschliessbaren Datenschränken aufbewahrt, stellt heutzutage der Schutz digitalisierter Daten Herausforderungen, denen sehr komplexe, abstrakte und für Nicht-Spezialisten schwer nachvollziehbare Fragestellungen zugrunde liegen. Das von IT-Mitarbeitenden ausgehende Gefahrenpotential kann nie gänzlich eliminiert, sondern nur reduziert werden. Im folgenden werden zwei Verfahren zur Verschlüsselung von strukturiert gespeicherten Daten genauer betrachtet und bezüglich des potentiellen Datenmissbrauchs durch das IT-Personal unter die Lupe genommen.

## Verschlüsselung in der Datenbank

Praktisch alle populären Speicher- bzw. Datenbanklösungen bieten die Möglichkeit, in der Datenbank abgelegte Daten zu verschlüsseln. Die Hersteller betonen, dass bei der Einführung der Verschlüsselung bestehende Applikationen nicht angepasst werden müssen. Das Datenmodell kann beibehalten werden, die Verschlüsselung sei für Umsysteme transparent. Solche Lösungen versprechen per Knopfdruck Konformität mit den geltenden Gesetzen und Richtlinien zum Schutz von Daten. Wie oben beschrieben, schützt dieser Ansatz vor dem Diebstahl der «rohen» Datenbankdateien, da der Dieb mit den verschlüsselten Daten nichts anfangen kann.

Der Schutz der Daten vor IT-Administratoren ist jedoch nicht gewährleistet. Ein DBA verfügt über die Berechtigungen und Werkzeuge, die notwendig sind, um sämtliche Daten zu entschlüsseln.

Auch die System-Administratoren stellen eine Gefahr dar, denn sie dürfen oft beliebige Applikationen installieren, auch einen Client zur Datenbankabfrage. Dem arglistigen Mitarbeiter fehlen nun lediglich noch Zugangsdaten eines legitimen

### IN KÜRZE

- Datendiebstähle durch internes Personal haben in den letzten Monaten stark zugenommen.
- IT-Mitarbeitende stehen dabei besonders im Fokus, da sie oft privilegierte Zugriffe haben.
- Das Gefahrenpotential kann nie ganz eliminiert, sondern nur reduziert werden. Dabei helfen Verfahren zur Verschlüsselung von strukturierten Daten.

Datenbankkontos. Diese sind für einen System\_Administrator in der Regel leicht zu beschaffen; er bedient sich aus Konfigurationsdateien von Serverapplikationen, die auf die Datenbank zugreifen müssen und zu diesem Zweck diese Login-Informationen abgelegt haben.

Eine weitere Analyse zeigt auch die technischen Grenzen einer solchen «transparenten» Verschlüsselung. Je nach Produkt steht nur eine beschränkte Auswahl an Verschlüsselungsalgorithmen zur Verfügung. Datenfelder, die zur eindeutigen Identifikation eines Datensatzes verwendet werden, können prinzipbedingt nicht verschlüsselt werden. Je nach Produkt ist die wahlweise Verschlüsselung einzelner Tabellen oder Spalten nicht möglich; entweder wird alles oder nichts verschlüsselt. Wird alles verschlüsselt, müssen beim Suchen auf Tabellenfeldern zuerst alle zu durchsuchenden Felder datenbankintern entschlüsselt werden. Da die Verschlüsselung zusätzliche Ressourcen erfordert, ist es nicht zweckmässig, einfach «blind» alle Daten zu verschlüsseln. Eine wahlweise Verschlüsselung der einzelnen Datenfelder muss in der Praxis möglich sein. Zudem sind die Daten, sobald sie die Datenbank verlassen, nicht mehr verschlüsselt. Für den Transport über ein Netzwerk oder auf Datenträgern müssen die Daten erneut verschlüsselt werden.

Vor diesem Hintergrund wird eine «Compliance auf Knopfdruck» zur Utopie. Die Notwendigkeit, sich mit den Eigenheiten der Daten und Applikationen auseinanderzusetzen, kann nicht umgangen werden.

**Verschlüsselung auf Applikationsebene**

Ein alternativer Lösungsansatz verschlüsselt die Daten auf Applikationsebene, bevor die Applikation diese in der Datenbank ablegt und sie werden entschlüsselt, nachdem die Applikation diese aus der Datenbank geladen hat. Dabei kann das Verschlüsseln direkt in der Applikation stattfinden oder die Applikation delegiert die Aufgabe an einen «zentralen Verschlüsselungsdienst». Ein zentraler Dienst hat unter anderem den Vorteil, dass er von mehreren Applikationen gemeinsam genutzt werden kann.

Da die Daten erst in der Applikation entschlüsselt werden, ist es nicht notwendig, den Transport der Daten zwischen Datenbank und Applikation zusätzlich zu sichern, da die Daten bereits verschlüsselt übertragen werden. Somit sind bei einem Mitschnitt des Datenverkehrs auf dem Netzwerk keine sensiblen Daten sichtbar. Weiter können Daten einfach migriert und portiert werden, ohne dass dabei eine Ent- und anschlies-

sende Neuverschlüsselung notwendig ist. Anders als beim Datenbankansatz bleiben die Daten während der Migration verschlüsselt.

Gegenüber der Datenbankverschlüsselung hat die Verschlüsselung auf Applikationsebene den Vorteil, dass sie die eigentliche «Angriffsfläche» für Datendiebstahl reduziert, insbesondere wenn es sich bei den möglichen Tätern um Mitarbeiter handelt. Es ist weder den DBAs noch den System\_Administratoren möglich, die Daten im Klartext zu sehen. Selbst wenn sie über die Zugangsdaten eines legitimen Datenbankkontos verfügen und mittels Datenbank-Client Abfragen ausführen, werden sie nur die verschlüsselten Daten zu Gesicht bekommen.

Dieser Ansatz der Datenverschlüsselung benötigt gegenüber dem ersten Verfahren einen höheren Aufwand bei der Einführung und er nimmt Einfluss auf das Datenmodell. Heute gebräuchliche Verschlüsselungsalgorithmen bewahren bei der Verschlüsselung den Datentyp des Eingangswerts nicht. Das Datenmodell muss also für verschlüsselte Spalten den resultierenden Datentyp anstelle des originären Datentyps verwenden. Die Applikation selbst muss um die Ver- und Entschlüsselung erweitert werden. Und auch dieser Ansatz benötigt zusätzliche Ressourcen zur Ver- und Entschlüsselung, jedoch nicht in der Datenbank, sondern in der Applikation selbst beziehungsweise auf den zusätzlichen Verschlüsselungsservern.

**Es existiert kein Königsweg**

Eine Patentlösung, welche die Unternehmensdaten gegen die Gefahr eines internen und externen Datendiebstahls schützt und die auf Knopfdruck zugeschaltet werden kann, existiert heute nicht. Unter den angesprochenen Gesichtspunkten haben die beiden Ansätze jeweils ihre eigenen Vor- und Nachteile (siehe Tabelle). Unabhängig davon, welches Verfahren man bevorzugt, der Entscheidung sollte eine Analysephase vorausgehen, in der das am besten geeignete Verfahren für die individuelle Sachlage identifiziert und die Details zur Umsetzung festgelegt werden. Dies minimiert das Risiko von unangenehmen Überraschungen bezüglich Performance, Kosten und erlangter Datensicherheit.

RETO FANKHAUSER IST SENIOR ARCHITECT UND SECURITY-EXPERTE BEI DER ELCA INFORMATIK AG IN ZÜRICH

**VERFAHREN ZUR VERSCHLÜSSELUNG VON STRUKTURIERTEN DATEN**

	Verschlüsselung in Datenbank	Verschlüsselung in Applikation
<b>Vorteile</b>	<ul style="list-style-type: none"> <li>Die Applikationen müssen nicht angepasst werden</li> <li>Datenmodell muss nicht angepasst werden</li> <li>«Out of the box»-Funktionalität vieler Datenbanken</li> </ul>	<ul style="list-style-type: none"> <li>Ermöglicht bessere Trennung der Administratorrollen</li> <li>Verschlüsselte Daten und Schlüssel sind getrennt abgelegt</li> <li>Daten sind auch ausserhalb der Datenbank verschlüsselt, dadurch werden Transport, Migration und Archivierung einfacher</li> <li>Datenbank ist vom Verschlüsselungsaufwand befreit</li> <li>Skalierbarkeit: Verschlüsselungsinfrastruktur kann die Arbeit für mehrere Applikationen/Datenbanken übernehmen</li> <li>Beliebige Verschlüsselungsalgorithmen können verwendet werden</li> <li>Kein Vendor-Lock-in: Daten können einfach von einem Datenbankprodukt auf ein anderes migriert werden, unabhängig davon, ob Verschlüsselung von der Datenbank unterstützt wird</li> </ul>
<b>Nachteile</b>	<ul style="list-style-type: none"> <li>Daten sind ausserhalb der Datenbank nicht geschützt</li> <li>Standard: Keine Trennung der Daten und Schlüssel ohne zusätzliches Hardware-Security-Modul (Schlüssel in Datenbank)</li> <li>Zusätzliche Arbeit in der Datenbank (Performanceverminderung)</li> <li>Limitierte Unterstützung von Verschlüsselungsalgorithmen</li> </ul>	<ul style="list-style-type: none"> <li>Zusätzliche Kommunikation zwischen den Systemen</li> <li>Verschlüsselungsserver muss zusätzlich administriert werden</li> <li>Datenmodelle und Applikationen müssen angepasst werden</li> </ul>

Quelle: Elca Informatik AG