

Die wertlose Beute

Der Diebstahl und Missbrauch von Daten kostet Firmen Unsummen an Entschädigungen und Strafzahlungen. Um sich davor zu schützen, setzen Unternehmen auf die **Tokenisierung**.

TEXT THOMAS KUHN

Es ist der Albtraum all jener, die in Unternehmen für die IT verantwortlich sind. Und Marty Edelman hat ihn durchlebt: „Hacker waren in unsere Kassensysteme eingedrungen und hatten Millionen von Kundendaten gestohlen“, erzählt der langjährige Chef der Bezahldienste bei der US-Baumarktkette Home Depot. Der digitale Raubzug 2014 von mehr als 50 Millionen Kreditkartendaten und rund 53 Millionen E-Mail-Adressen kostete den Konzern bis heute fast 180 Millionen Dollar, um Kunden zu entschädigen, Strafzahlungen zu begleichen – und die IT zu reparieren. „Es hat Monate gedauert, das Chaos aufzuräumen und die Systeme gegen künftige Datendiebstähle zu schützen“, so Edelman.

Dass Hacker bei seinem einstigen Arbeitgeber mit derlei Attacken keinen Erfolg mehr hatten und Edelman nun als Berater für IT-Sicherheit gefragt ist, liegt am Datenschutzkonzept, das der Informatiker nach dem Cyber-Gau bei Home Depot installiert hat – und das inzwischen immer mehr Firmen nutzen: die Tokenisierung von Daten. Dabei verändert Spezialsoftware sensible Informationen so weit, dass weder ein Rückschluss auf die Originaldaten möglich ist noch ein Missbrauch gestohlener Datensätze. Aus dem Geburtsdatum 24.12.1970 würde etwa 32.12.1970, aus der Kreditkartennummer 6420 6508 7415 1520 die 6420 1234 5678 1520. Im Techjargon heißen die modifizierten Datenbestandteile „Token“.

Firmen, denen derart kaschierte Informationen gestohlen würden, drohen keine Strafen mehr wegen Ver-

Raubzug im Handel

Hacker sorgen bei Firmen wie Home Depot für größere Schäden als Ladendiebe. Die Tokenisierung von Kundendaten kann dies verhindern

stoßen gegen den Datenschutz. Hacker, die versuchen, mit der verfremdeten Kreditkartennummer einzukaufen, fielen sofort auf. Lange setzten vor allem Zahlungsdienstleister auf das Verfahren. Doch das Interesse steige auch für viele andere Anwendungsfälle, heißt es etwa in einer Untersuchung des IT-Marktforschers Gartner. „Innerhalb des vergangenen Jahres haben sich die Kundenanfragen zur Technologie bei uns verdoppelt.“

Das Verfahren ist mathematisch weniger komplex als klassische Kryptografie und bietet doch einen wirksamen Schutz. „Wir verschlüsseln Daten nicht immer als Ganzes, sondern ersetzen bei der Tokenisierung oft nur Teilbereiche der Datensätze durch andere Ziffern, Zeichen oder Werte“, erläutert Michael Deissner, Chef des Technologiespezialisten Comforte. Dabei kaschiere die Software nur so viel, dass ein Rückschluss auf schützenswerte Details nicht mehr möglich sei. „Weil aber das Datenformat, also etwa Text oder Zahlen, unverändert und auch die Länge der Datenfelder gleich bleiben, lassen sich die Datensätze weiter mithilfe regulärer Büroanwendungen verarbeiten“, versichert Deissner, zu dessen Kunden auch MasterCard und Visa gehören.

Im sicheren Safe statt weiträumig verteilt

Bei klassischer Kryptografie hingegen müssen die Schlüssel geteilt werden, damit Nutzer oder Programme innerhalb oder außerhalb des Unternehmens die codierten Informationen wieder entschlüsseln können. Gelingt es Hackern, Schlüssel zu stehlen oder zu knacken, bekommen sie Zugriff auf die sensiblen Originaldaten. Im Fall der Tokenisierung hingegen wandern die Ursprungsdaten in einen speziellen Safe, in dem sie wesentlich besser zu schützen sind als die verteilten Schlüssel. Zumal ein Zugriff auf die Originale nur noch in den seltensten Fällen und für einen eng begrenzten Personenkreis nötig ist – etwa um eine Rechnung zu erstellen oder Buchungen zu überprüfen.

Und doch erfordert auch die Tokenisierung bei den Unternehmen, die sie nutzen wollen, einiges an Aufwand: Die Software müsse, erzählt Comforte-Chef Deissner, „erst einmal alle Ecken und Winkel der Unternehmens-IT durchforsten, um alle potenziell sensiblen Informationen aufzustöbern“. Anschließend werden doppelte oder nicht mehr benötigte Einträge eliminiert und alle verbliebenen Informationen modifiziert. „Nur wenn wirklich alle Datensätze erfasst und alle Token eindeutig sind, funktioniert das System.“

Im Fall eines seiner Kunden, eines großen US-Handelskonzerns, erzählt Berater Edelman, hätten Analyse, Bereinigung und Sicherung von mehr als 1,2 Milliarden Datensätzen sogar mehrere Jahre gedauert und Kosten in einstelliger Millionen-Dollar-Höhe verursacht. Aber Edelman weiß auch: „Ein schwerer Datenraub wie damals bei Home Depot wäre um ein Vielfaches teurer gekommen.“

63

Prozent der deutschen Unternehmen waren laut IT-Verband Bitkom im vergangenen Jahr von Datendiebstählen betroffen