IT-Sicherheit erhöht den Datenschutz entscheidend

Vorkehren ist besser als Brand löschen

Wie lässt sich der Anspruch der Kunden auf die Sicherheit ihrer Daten in der Praxis umsetzen?

Immer wieder sind in den letzten Monaten sensible Kundendaten aus Unternehmen an die Öffentlichkeit gelangt. Richtig publik wird in solchen Fällen meist nur die Spitze des Eisberges, vor allem dann, wenn namhafte Unternehmen betroffen sind.

IT-Sicherheit dreht sich in vielen Unternehmen um die kritischen Unternehmensdaten: im Mittelpunkt der Anstrengungen steht die Sicherheit von Zahlen, Strategien und Projektdokumenten. Kaum einer würde beispielsweise auf die Idee kommen, eine Präsentation mit strategischen Unternehmenszielen über Jahre hinweg auf einem Webserver zu lagern. Aber wie sieht es mit sensiblen Kundendaten aus? Gerade bei Unternehmen, die einen Teil ihres Geschäfts über das Internet betreiben, werden häufig personenbezogene Daten auf Servern mit »Außenverbindung« gelagert. Die Gründe dafür sind vielfältig: Häufig sind die Zuständigkeiten für Datenschutz und IT-Sicherheit in verschiedene Abteilungen verteilt, oder externe Lieferanten wie beispielsweise die Webagentur haben sicherheitskritische Anwendungen aufgesetzt, ohne dass diese vom Unternehmen selbst hinreichend auf Sicherheitsaspekte geprüft wurden. Auch mangelndes Bewusstsein bei einzelnen Mitarbeitern ist eine der wichtigsten Ursachen für derartige Datenlecks.

Den Grundsatz der Datensparsamkeit beachten. Aber wie kann man ein dauerhaft hohes Schutzniveau erreichen? Wie kann der Anspruch auf den Schutz der Kundendaten, der häufig auf dem Papier bereits definiert ist, auch genauso in die Praxis umsetzen?

Zunächst sollten neben den sensiblen Unternehmensdaten auch die Kundendaten explizit in den Schutzbereich einbezogen werden. Das hört sich einfach an, ist aber in der Praxis deutlich schwieriger als bei sensiblen Unternehmensdaten, zu denen im Regelfall nur ein kleiner Personenkreis Zugang hat. Mit Kundendaten hantieren hingegen oftmals eine große Anzahl an Mitarbeitern und externen Partnern.

Viele Unternehmen können ihre Kundendaten alleine dadurch besser schützen, dass sie den Grundsatz der »Datensparsamkeit« konsequent umsetzen. Das bedeutet beispielsweise, Daten von inaktiven Kunden nach zwei Jahren zu archivieren und dem Zugriff auf solche Altdaten auf Administratoren einzuschränken. Auch sollten die internen Zugriffsberechtigungen auf Kundendaten auf das wirklich notwendige Maß beschränkt werden – brauchen alle Mitarbeiter Zugriff auf alle Kundendaten, oder genügt es, dass das Controlling auf Abrechnungsdaten zugreifen kann?

Audits und Risikoanalysen als Basis für ein Sicherheitskonzept. Um zu klären, wer Zugriff auf welche Daten hat, bietet es sich an, eine Ist-Analyse im Unternehmen durchzuführen, beispielsweise durch interne Audits. Dabei sollte darauf geachtet werden, nur den Ist-Zustand zu beschreiben und nicht bereits einen Soll-Zustand. Auch ein externes Audit kann helfen, unvoreingenommen und neutral mögliche Schwachstellen zu identifizieren.

Darauf aufbauend kann im nächsten Schritt ein Sicherheitskonzept formuliert werden, um den Schutzbedarf umfassend und lückenlos zu beschreiben. Als Grundlage hierfür bieten sich beispielsweise die Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) an. Wer besonders gründlich vorgehen möchte, führt als erstes eine Risikoanalyse durch, um Schwachstellen systematisch zu erfassen und zu bewerten, etwa hinsichtlich des möglichen Schadenspotenzials, der Eintrittswahrscheinlichkeit und der Entdeckungswahrscheinlichkeit. Darauf aufbauend können adäquate Sicherheitsmaßnahmen definiert werden, um Unternehmens- und Kundendaten im Unternehmen und bei Partnern möglichst optimal zu schützen.

Derartige Vorgehensweisen zur Erhöhung der IT-Sicherheit tragen durch die explizite Ausweitung auf die im Unternehmen gespeicherten Kundendaten maßgeblich dazu bei, den Datenschutz im Unternehmen entscheidend zu verbessern.

Stefan Spiegel

Stefan Spiegel ist Principal Consultant beim Münchener Internetspezialisten Ray Sono AG und beim TÜV SÜD als externer Auditor akkreditiert.