Datenleck Mitarbeiter

Outsourcing auf eigene Faust

Wenn Beschäftigte eigenmächtig Outsourcing betreiben, da ihnen die Unternehmens-IT die „wirklich benötigten" Anwendungen nicht oder nur in „unakzeptabler" Qualität zur Verfügung stellt, ist Vorsicht geboten. Über Tools, die die Mitarbeiter sich inoffiziell beschaffen, können Unternehmensinformationen in der Cloud landen. Damit sind auch personenbezogene Daten in Gefahr.

Outsourcing von IT-Dienstleistungen ist in Unternehmen gang und gäbe. Was aber, wenn jeder einzelne Mitarbeiter ohne Absprache anfängt, externe IT-Dienste in Anspruch zu nehmen, also selbst outzusourcen?

Potenzielles Datenleck doodle: Einsicht in geplante Termine

Ein typisches Beispiel: Der von Mitarbeitern sicherlich am häufigsten benutzte externe Dienst ist der Terminfindungs-Dienst doodle. Die Nutzer generieren eine kleine Terminanfrage und schicken einen Link per E-Mail an alle potenziellen Teilnehmer. Gerade unternehmensübergreifende Termine sind so einfach zu verabreden.

Vor unberechtigtem Zugriff soll eine 16 Zeichen lange alphanumerische Zeichenfolge im Link schützen – wer diese kennt, hat jedoch Zugriff auf den Inhalt. Da ein Anlass des Termins, ein Ort und eine Beschreibung eingegeben werden können, besteht die Gefahr, dass Mitarbeiter darüber Unternehmensinterna leichtfertig offenbaren.

Verlockender kostenloser Speicher in der Cloud

Nicht minder beliebt als doodle ist die Datenspeicherung in der Cloud: Dienste wie DropBox (2 GByte), Strato Hidrive sowie Apple iCloud (je 5 GB) oder die Microsoft Skydrive und die Telekom Cloud (je 25 GB) stellen jedermann kostenlosen Online-Speicher zur Verfügung. Das macht den Datenaustausch zwischen verschiedenen Rechnern, z.B. dem Rechner im Büro und dem Gerät daheim, sehr einfach.

Komfortabel und gefährlich: Dropbox

Um bei den Nutzern punkten zu können, müssen Windows, Linux, Mac OS, iOS und Android durch einfach zu bedienende Klienten unterstützt werden. Die Standards für einen solchen Klienten hat die Firma Dropbox vorgegeben.

Eine Verschlüsselung ist nicht vorgesehen

Wird das Protokoll der Vorstandssitzung am Freitag nicht mehr fertig, schiebt der verantwortliche Mitarbeiter es schnell in die Dropbox, um es am Wochenende zu beenden. Dabei macht er sich keine Gedanken darüber, wer Zugriff auf die Daten hat. Die Gefahr dabei: Eine verschlüsselte Speicherung sehen die meisten Dienstleister nicht vor.

US-Behörden können sich bedienen

Und so können Details etwa bei den US-amerikanischen Behörden landen. Im Jahr 2011 wurde z.B. bekannt, dass amerikanische Cloud-Anbieter auf Anforderung staatlicher Stellen die Daten europäischer Unternehmen herausge-

Diese Tools könnten auch Ihre Kollegen einsetzen:

www.doodle.com
www.dropbox.com
www.free-hidrive.com/ger/
www.apple.com/de/icloud/
www.windowslive.de/skydrive/
www.telekom.de/lp/b/telekomcloud
www.teamdrive.com/de/

ben müssen. Der „Patriot Act“ macht es möglich (siehe dazu Datenschutz PRAXIS 12/11, „Konsequenzen aus dem Patriot Act für den Datenaustausch mit den USA“).

Achten Sie auf zertifizierte Sicherheit

Lediglich das Hamburger Unternehmen Teamdrive setzt mit guter Verschlüsselung und einem Zertifikat des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) auf eine datenschutzkonforme Lösung (2 GB kostenlos). Bei den „Personal Outsourcern“, also den Mitarbeitern, die zur Selbsthilfe greifen, gilt diese Lösung allerdings leider nicht als erste Wahl.

Teamviewer: Die Fernsteuerung umgeht interne Sicherheitsregeln

In Unternehmen gelten strenge Regeln, auf welche Ressourcen von außen zugegriffen werden darf. Dies führt dazu, dass Beschäftigte an ihrem Arbeitsplatz mehr tun können als privat: E-Mail-Zugriff ist z.B. auch von zu Hause aus möglich, SAP-Zugriff nur im Unternehmen.

Clevere Kollegen wissen sich jedoch zu helfen: Ein sehr beliebtes Werkzeug für den Fernzugriff auf den Rechner im Büro ist der Teamviewer, da sich das Programm ohne Administratorrechte nutzen lässt. Im Büro kurz vor Arbeitsende gestartet, ermöglicht es den Zugriff von daheim und die Fernsteuerung des PC im Büro. Dazu muss man nur den Rechner angeschaltet lassen und die Zugriffscodes mitnehmen.

Die Unternehmensfirewall hat keine Chance gegen das Hintertürchen

Die Unternehmens-Firewall kann die Fernsteuerung des Arbeitsplatz-PCs nicht ohne Weiteres unterbinden, da sie „nur“ eine unverdächtige ausgehende https-Verbindung sieht. Lediglich mit einem detaillierten Blick in die Daten der Verbindung wäre eine Blockade möglich.

Meist steckt keine böse Absicht der Mitarbeiter dahinter

Jedes Unternehmen sollte sich also intensiv mit der Problematik beschäftigen. Tatsächlich benötigen viele Beschäftigte diese Dienste und haben nichts Böses im Sinn. Vielmehr wollen sie einfach ihre Arbeit effizient erledigen und wissen sich oftmals nicht anders zu helfen.

Eigene Lösungen und Sensibilisierung schaffen Sicherheit

Um also die Sicherheit zu verbessern, ist die Alternative nicht, alles zu verbieten. Vielmehr sollten die Verantwortlichen prüfen, welche Dienste zu einer Verbesserung der Arbeitsabläufe beitragen können, und sie den Beschäftigten unter eigener Regie anbieten. Eine private Cloud im Unternehmen erfüllt ja gegebenenfalls auch den Bedarf der Kollegen. Und einen Remote-Zugriff, etwa über Terminalserver, kann das Unternehmen selbst regelkonform anbieten.

Schließlich ist wichtig, dass das Unternehmen seine Beschäftigten ausdrücklich auf die Gefahren des eigenmächtigen Outsourcens von IT-Diensten hinweist. Unser Muster finden Sie zum Download unter *www.datenschutz-praxis.de/fachwissen/vorlagen/muster* oder *kurzlink.de/muster_bsi*.

Prof. Dr. Rainer W. Gerling

Rainer W. Gerling ist Datenschutz- und IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft und Honorarprofessor für IT-Sicherheit an der Hochschule München.

Mitarbeiterinformation
Unberechtigte Nutzung externer IT-Dienstleistungen

In unserem Unternehmen nutzen Beschäftigte und sonstige dort tätige Personen ohne Genehmigung und Beteiligung der eigenen IT-Abteilung oder sonstiger administrativer Abteilungen Dienstleistungen externer Diensteanbieter. Diese scheinen ihnen vermeintlich besser, effizienter oder einfacher zu bedienen. Insbesondere sind die diversen Dienste von Google, Microsoft Live und anderen zu nennen. Allen diesen Diensten ist gemeinsam, dass der Nutzer – und damit letztendlich auch unser Unternehmen – aufgrund bestehender Bedingungen der Nutzung, eines unklaren Speicherorts der Daten und der Übertragung von Nutzungsrechten an die Diensteanbieter die Kontrolle über die Daten verliert.

Da es sowohl arbeitsvertragliche Verschwiegenheitspflichten als auch gesetzliche Vorgaben bezüglich der Verarbeitung personenbezogener Daten, Verkehrsdaten im Telekommunikationsbereich und Nutzungsdaten im Telemedienbereich – um nur einige Datenarten zu nennen – gibt, kann ein solcher externer Dienstleister nur genutzt werden, wenn den gesetzlichen und sonstigen Belangen durch angemessene Verträge zwischen unserem Unternehmen und dem Dienstleister Rechnung getragen wird.

Kriterien für die Auswahl von IT-Dienstleistern sind Datensicherheit, Datenschutz und der Schutz der Unternehmensdaten vor Missbrauch. Dies ist durch die zuständigen administrativen Stellen unseres Unternehmens sicherzustellen!

Eine eigenmächtige, ungeprüfte und damit unberechtigte Nutzung externer Dienstleistungen durch Beschäftigte und sonstige im Unternehmen tätige Personen ist sowohl aus datenschutzrechtlichen als auch aus IT-sicherheitstechnischen Gründen abzulehnen und gefährdet das Unternehmen!