Postbrief für Berufsgeheimnisträger" gibt Ärzten, Anwälten oder Amtsträgern die Möglichkeit, elektronische Kommunikationsmittel geschäftlich zu nutzen, ohne dabei gegen ihre Verschwiegenheitspflicht nach Paragraph 203 des Strafgesetzbuchs (StGB) zu verstoßen. Der erweiterte E-Postbrief eignet sich beispielsweise für die Abrechnung privatärztlicher Leistungen oder die Kommunikation zwischen Steuerberatern beziehungsweise Anwälten und ihren Mandanten. Die Lösung ist ab Sommer verfügbar.

Mit der Integration einer durchgängigen Verschlüsselung in den E-Postbrief kommt die Post einer langjährigen Forderung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) im Rahmen der DE-Mail-Diskussion nach. Dieser hatte sich im Gesetzgebungsverfahren dafür ausgesprochen, dass die Ende-zu-Ende-Verschlüsselung verpflichtend für De-Mail eingeführt wird. Diese Anregung wurde aber nicht aufgegriffen. Aus seiner Sicht ist eine durchgängige Verschlüsselung der Nachrichten von zentraler Bedeutung.

Durch die Lösung des E-Postbriefs für Berufsgeheimnisträger ist die bequeme Einbindung von Privatkunden, also beispielsweise von Patienten oder Mandanten, in den Kommunikationsablauf gesichert. Durch die Ende-zu-Ende-Verschlüsselung bietet der E-Postbrief nun eine bequeme Möglichkeit für eine rechtskonforme Kommunikation. Ohne weitere Hardware oder zusätzliche Dienstleister kann der Empfänger die Nachrichten automatisch in seinem Browser entschlüsseln.

Bestimmte Berufsgruppen unterliegen in Deutschland einer besonderen Verschwiegenheitspflicht. Dazu gehören – neben Ärzten, Anwälten und Amtsträgern – auch Angehörige von Heilberufen, Sozialarbeiter sowie Notare oder Mitarbeiter privater Krankenversicherungen. Anvertraute personenbezogene Informationen dürfen von ihnen nur unter sehr eingeschränkten Voraussetzungen weitergegeben werden, um zu verhindern, dass unbefugte Dritte Zugang zu sensiblen Daten erhalten. Träger von Berufsgeheimnissen konnten daher elektronische Kommunikationsformen bislang nur mit erheblichem Aufwand nutzen. Die Folge waren kostenträchtige manuelle Arbeitsabläufe über verschiedene Medien hinweg, beispielsweise bei der Leistungsabrechnung dieser Berufsgruppen.

Sealed Cloud schließt IT-Sicherheitslücke „Mensch"

Das Fraunhofer AISEC in München gehört zu den Gewinnern des Technologiepreises »Trusted Cloud«. Gemeinsam mit dem Münchner Startup Uniscon universal identity control GmbH und der SecureNet GmbH erhielt Fraunhofer AISEC auf der CeBIT 2013 in Hannover von Bundesminister Rainer Brüderle die Gewinnerurkunde für das Projekt, dessen Ergebnis das Produkt »Sealed Cloud« sein wird. Ziel des Vorhabens ist die Realisierung einer Cloud-Infrastruktur, in denen der Betreiber nicht auf die Daten seiner Kunden zugreifen kann. Einsatzgebiet für die »Sealed Cloud« ist die öffentliche Verwaltung und mittelständische Unternehmen, die so von den Vorteilen des Cloud Computings profitieren sollen.

Viele Unternehmen fordern berechtigterweise, dass ihre kritischen Daten in der Cloud sicher aufgehoben sein sollten. Der Schutz vor Angriffen von außen reicht jedoch nicht, denn auch interne Angreifer, etwa Mitarbeiter des Cloud-Anbieters, könnten Daten einsehen, kopieren, löschen. Das Risiko des Datenmissbrauchs liegt vor allem in den internen Prozessen begründet. Die meisten Cloud Computing Anbieter veröffentlichen so gut wie keine Informationen über ihre internen Sicherheitsprozesse und eingesetzten Technologien zum Schutz der Daten. Obwohl gerade mittelständische Unternehmen von den ökonomischen Vorteilen des Cloud Computings profitieren könnten, verzichten viele auf die Nutzung, da ihr Vertrauen in die Anbieter nicht ausreicht.

Wer hat Zugriff auf den Server? Gibt es nur eigene Administratoren oder auch externe Dienstleister? Wie sind die internen Prozesse gestaltet und wie abgesichert? Sind die Daten verschlüsselt? Wer hatte oder hat Zugang zu den Dekodierungsschlüsseln? Dass diese Fragen bis heute unbeantwortet sind, hält die Unternehmen bis heute davon ab, Clouds zu nutzen. Die Sealed Cloud kombiniert die ökonomischen Vorteile einer über das Internet nutzbaren Public Cloud mit der Sicherheit einer abgeschotteten Private Cloud.. Diese verhindert mittels technischer Verfahren und Vorrichtungen, dass der Betreiber der Cloud, sein Personal oder externe Dritte auf Daten seiner Kunden zugreifen können. Dieser Schutz wirkt in allen Phasen der Verarbeitung.

Rezensionen

Veranstaltungen

Helmut Reimer

22. RSA Conference, 25.02. – 01.03.2013 in San Francisco, USA

Die weltgrößte IT-Sicherheitskonferenz fand auch diesmal wieder im Moscone Center in San Francisco statt. Die RSA Konferenz ist nach wie vor die Welt-Leit-Messe für IT-Security mit starker internationaler Beteiligung und ist weiter gewachsen: mit etwa 24.000 Besuchern und 371 Ausstellern ist diese Veranstaltung an den Grenzen der Kapazitäten des Moscone Centers North und South angekommen. Bereits in diesem Jahr wurde eine zweite Ausstellungshalle operativ genutzt. Sie wird ab 2014 professionell für die Messestände der Sponsoren zur Verfügung stehen. Der bereits im Vorjahr erkennbare Trend zum prägenden Einfluss der Messe gegenüber der Konferenz hat sich fortgesetzt.

In diesem Jahr war Ausstellungsfläche ein knappes Gut. Für die Präsentation von ‚IT Security Made in Germany' – zum 13. Mal in ununterbrochener Folge – standen für die vom Bundesministerium für Wirtschaft und Technologie (BMWi) und vom Ausstellungs- und Messe-Ausschuss der deutschen Wirtschaft e.V. (AUMA) geförderten und von TeleTrusT, Bundesverband IT-Sicherheit, organisierten Gemeinschaftsausstellung lediglich 108 m^2 zur Verfügung. Erfreulicherweise wurde aus der Not eine Tugend. Der deutsche Pavillon beeindruckte mit einem hervorragenden Design und der qualitativ hochwertigen Ausführung im Gesamterscheinungsbild der Messe und bot den 15 ausstellenden Unternehmen beste Präsentations- und Verhandlungsbedingungen. Die Anziehungskraft für Fachbesucher hat sich gegenüber den Vorjahren deutlich erhöht.