

NIFIS: Ende-zu-Ende-Verschlüsselung verkommt zum Marketing-Buzzword

- NIFIS stellt drei Kriterien für sichere Ende-zu-Ende-Verschlüsselung auf
- Anwender sollten „Ende-zu-Ende“ bei der Anbieterswahl hinterfragen
- E-Mail-, Messaging- und Cloud-Dienste besonders betroffen
- Umfrage fördert geringes Vertrauen in US-Anbieter zutage

Frankfurt am Main, 22. November 2016 – Eine Ende-zu-Ende-Verschlüsselung, die von einer deutschen Firma mit einem Rechenzentrum, das in Deutschland steht, angeboten wird, stellt einen wesentlichen Faktor für die Sicherheit bei E-Mails, Messaging und Cloud-Diensten dar. Dies ist eine Kernaussage im aktuellen Report „IT-Sicherheit und Datenschutz 2017“, den die [Nationale Initiative für Informations- und Internet-Sicherheit e.V.](#) (NIFIS) herausgebracht hat. Der Bericht fußt auf einer Expertenbefragung unter 100 mit dem Thema befassten Fach- und Führungskräften aus der mittelständischen Wirtschaft in Deutschland.

Drei Kriterien für wirkliche Ende-zu-Ende-Sicherheit

Über drei Viertel der Befragten (76 Prozent) halten eine Ende-zu-Ende-Verschlüsselung für den entscheidenden Sicherheitsfaktor. Sie stellen dafür allerdings drei Bedingungen. Erstens dürfen die Daten bei der Übertragung „unterwegs“ nicht entschlüsselt werden (79 Prozent). Zweitens muss die Speicherung ebenfalls verschlüsselt erfolgen (72 Prozent). Und drittens muss gewährleistet sein, dass der Anbieter selbst keinen Schlüssel zu den Daten im Besitz hält (83 Prozent).

Ende-zu-Ende-Sicherheit verkommt zum Marketing-Buzzword

„Leider lassen viele Anbieter den Begriff Ende-zu-Ende-Verschlüsselung zu einem Marketing-Buzzword verkommen, weil sie die drei sicherheitskritischen Zusatzbedingungen nicht erfüllen“, hat RA Dr. Thomas Lapp, Vorstandsvorsitzender der Nationalen Initiative für Informations- und Internet-Sicherheit, beobachtet. Er erklärt: „Eine vermeintliche Ende-zu-Ende-Verschlüsselung, bei der die Speicherung unverschlüsselt erfolgt oder bei der der Anbieter selbst die Daten jederzeit entschlüsseln kann, stellt keine wirkliche Sicherheit dar. Es ist daher jedem Unternehmen und jedem IT-Verantwortlichen dringend zu raten, bei der Anbieterswahl für E-Mail-, Messaging- oder Cloud-Dienste die Aussagen der Firmen unter diesen Aspekten kritisch zu hinterfragen und sich schriftlich bestätigen zu lassen.“

Deutscher Standort ist gefragt

Laut Umfrage stufen 91 Prozent der Experten eine Ende-zu-Ende-Verschlüsselung als besonders sicher ein, wenn sie von einer deutschen Firma (91 Prozent) oder zumindest von einer Firma mit Sitz in der EU (78 Prozent) angeboten wird (Mehrfachnennungen waren erwünscht). Zum Vergleich: Bei einem US-amerikanischen Anbieter haben lediglich 17 Prozent der Befragten dieses Vertrauen. Rund zwei Drittel (68 Prozent) lehnen US-Firmen aus Sicherheitsbedenken ab. Anbieter, die außerhalb des EU-Raumes und außerhalb der USA angesiedelt sind, wecken bei einem Drittel (33 Prozent: britischer Anbieter, durch Brexit bald außerhalb der EU) bzw. gut einem Viertel (28 Prozent, Schweiz) mehr Vertrauen.

Neben dem Sitz des Unternehmens spielt laut NIFIS-Report der Standort des Rechenzentrums eine Schlüsselrolle bei der Einschätzung der Sicherheit. So vertreten 91 Prozent der befragten Fachleute die Auffassung, dass die Nutzung eines Rechenzentrums am sichersten ist, wenn dieses in Deutschland steht. 81 Prozent (Mehrfachnennungen waren erwünscht) genügt die Ansiedlung innerhalb der EU. Für gut die Hälfte (51 Prozent) stellt die neutrale Schweiz einen idealen Standort dar, für 39 Prozent Großbritannien. Rechenzentren in den USA lehnen hingegen 85 Prozent der Befragten ab.

Geringes Ansehen für die USA

„Es ist festzustellen, dass die USA kein hohes Ansehen in der deutschen Wirtschaft genießen, wenn es um IT-Sicherheit geht“, sagt der NIFIS-Vorsitzende RA Dr. Thomas Lapp. Er führt dies unter anderem darauf zurück, dass 65 Prozent den neuen EU-US Privacy Shield, der den Datenschutz zwischen der EU und den USA regelt, genauso kritisch einstufen wie das vorherige Safe-Harbor-Abkommen, das der Europäische Gerichtshof im Oktober 2015 für ungültig erklärt hatte.

[NIFIS Nationale Initiative für Informations- und Internet-Sicherheit e.V.](#) ist eine neutrale Selbsthilfeorganisation, die die deutsche Wirtschaft im Kampf gegen die täglich wachsenden Bedrohungen aus dem Netz technisch, organisatorisch und rechtlich unterstützen möchte. Vornehmliches Ziel der Arbeit der unter dem Dach der NIFIS organisierten Gremien ist es, Vertraulichkeit, Verfügbarkeit und Integrität sowie den sicheren Transport von Daten in digitalen Netzwerken sicherzustellen. Dazu entwickelt die NIFIS seit ihrer Gründung im Jahr 2005 unterschiedliche Konzepte und setzt diese in pragmatische Lösungen um. Zu den Schwerpunkten der Tätigkeit zählen die aktive Kommunikation und die Bereitstellung von Handlungsempfehlungen und Dienstleistungen.

Weitere Informationen: NIFIS Nationale Initiative für Informations- und Internet-Sicherheit e.V., Berkersheimer Bahnstraße 5, 60435 Frankfurt, Tel.: 069 2444 4757, Fax: 069 2444 4746, E-Mail: nifis@nifis.de, Web: www.nifis.de

PR-Agentur: euromarcom public relations GmbH, Tel. +49 (0) 611 97315-0, E-Mail: team@euromarcom.de, Web: www.euromarcom.de

