# NIFIS erwartet massiven Anstieg der Ausgaben für IT-Sicherheit

**RA Dr. Thomas Lapp, Vorsitzender der Nationalen Initiative für Informations- und Internet-sicherheit: „Datenschutz, Hackerabwehr und der Kampf gegen Industriespionage sind die Kosten-treiber für die IT-Sicherheit“**

Frankfurt am Main, 7. März 2017 – Die deutsche Wirtschaft wird 2017 massiv in ihre IT-Sicherheit investieren. Dies legt der aktuelle Report „IT-Sicherheit und Datenschutz 2017“ nahe, den die Nationale Initiative für Informations- und Internet-Sicherheit e.V. (NIFIS) vorgelegt hat. Der Bericht basiert auf einer Umfrage unter 100 Fach- und Führungskräften überwiegend aus mittelständischen Unternehmen in Deutschland.

Demnach schätzt beinahe die Hälfte (48 Prozent), dass die deutschen Unternehmen 2017 rund ein Drittel mehr für die IT- und Informationssicherheit ausgeben werden als noch im Jahr zuvor. 14 Prozent erwarten sogar einen Anstieg um 50 Prozent, 8 Prozent eine Verdoppelung. 28 Prozent gehen davon aus, dass die Ausgaben 2017 auf Vorjahresniveau bleiben werden. Lediglich 2 Prozent rechnen mit einem sinkenden Aufwand für die IT-Sicherheit.

**50 Prozent Ausgabenzuwachs bis 2025**

Langfristig – bis zum Jahr 2025 – gehen 58 Prozent der von NIFIS befragten Fach- und Führungskräfte von einem Ausgabenanstieg um 50 Prozent aus. 14 Prozent prognostizieren eine Verdoppelung, 16 Prozent eine Ausweitung um 30 Prozent. 12 Prozent erwarten ein Verharren des Ausgabevolumens auf dem heutigen Stand.  Kein einziger der Befragten geht davon aus, dass 2025 weniger für IT-Sicherheit ausgegeben wird als heutzutage.

„Datenschutz, die Abwehr von Hackerangriffen und der Schutz vor Industriespionage werden zu den wesentlichen Kostentreibern für die IT-Sicherheit in den nächsten Jahren gehören“, wagt RA Dr. Thomas Lapp, Vorsitzender der Nationalen Initiative für Informations- und Internet-Sicherheit e.V. (NIFIS) eine Vorhersage. Seit den Vorgängen um NSA und andere Geheimdienste ist die deutsche Wirtschaft bezüglich Datenschutz sensibilisiert, stimmen 87 Prozent der befragten Fach- und Führungskräfte zu. 71 Prozent gehen schon für 2017 von einer Verstärkung der Bemühungen in der deutschen Wirtschaft aus, um Spähangriffen entgegenzuwirken. Bemerkenswert: 83 Prozent stufen den Datendiebstahl durch die eigenen Mitarbeiter als sehr ernst zu nehmende Gefahr ein. Für 78 Prozent gehört der Schutz vor externen Hackerangriffen zu de Topthemen des Jahres 2017.

Nach möglichen Abwehrmaßnahmen befragt, räumen 93 Prozent ein, dass es keinen sicheren Schutz vor Spähattacken gibt. Dennoch halten es 95 Prozent für geraten, bei Cloud-Services auf europäische oder noch besser auf deutsche Anbieter zurückzugreifen. Für 91 Prozent ist es dabei von Bedeutung, dass nicht nur die Daten nicht in die USA gelangen, sondern darüber hinaus auch der Anbieter keinen Sitz in den USA hat. Zudem verlangen 92 Prozent der Befragten nach einer wirksamen Verschlüsselung der Daten. 88 Prozent vertreten die Auffassung, dass die Unternehmen in Deutschland ihre Beschäftigten noch besser in Bezug auf den vertraulichen Umgang mit Daten schulen sollten. Für die Abwicklung geschäftskritischer Transaktionen ist den Unternehmen auf jeden Fall zur Nutzung sicherer virtueller Datenräume zu raten, meinen 87 Prozent.

**Viele Firmen haben keinen Überblick über ihre Sicherheit**

RA Dr. Thomas Lapp erklärt: „Viele Unternehmen übrigens unterschiedlicher Firmengröße haben keinen wirklichen Überblick darüber, welche möglicherweise sensiblen Daten inhouse oder bei externen Cloud-Diensten gespeichert werden. Wenn ein Mitarbeiter vertrauliche Kundendaten auf seinem Smartphone hält und dieses mit einem US-amerikanischen Cloud-Service synchronisiert, liegt bereits eine Verletzung des Datenschutzes vor, weil die Kunden dieser Auslagerung in die USA in der Regel zuvor nicht wirksam zugestimmt haben“, gibt RA Dr. Thomas Lapp ein prägnantes Beispiel. 79 Prozent der Fach- und Führungskräfte stimmen ihm zu und fordern, dass die deutschen Firmen stärker kontrolliert werden sollten dahingehend, ob sie ihre sensiblen und vertraulichen Daten ausreichend gut schützen und bei Verstößen mit Sanktionen rechnen müssen.“ Der deutsche Gesetzgeber sieht beim Datenschutz für fahrlässige Verstöße bis zu 50.000 Euro Bußgeld vor, in schweren Fällen bis zu 300.000 Euro. Bei Vorsatz droht eine Freiheitsstrafe von bis zu zwei Jahren. Lapp macht deutlich „Schon jetzt gilt, dass das Bußgeld den wirtschaftlichen Vorteil, der aus dem Verstoß erzielt wurde, überschreiten muss und die genannten Beträge gegebenenfalls auch überschritten werden können. Ab Mai 2018 wird durch die Datenschutzgrundverordnung der EU (EU DSGVO) der Rahmen für das Bußgeld je nach Verstoß auf 2% bzw. 4 % des weltweiten Vorjahresumsatzes erhöht, so dass mit wirklich empfindlichen Geldbußen gerechnet werden muss.“

**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