IT-Sicherheit –
Zeit für einen Paradigmenwechsel?

Ergebnisse einer Umfrage vom August/September 2013

LANCOM
Systems

LANCOM Systems

Inhaltsverzeichnis

Zusammenfassung

Die Umfrage „IT-Sicherheit – Zeit für einen Paradigmenwechsel?“, durchgeführt von LANCOM Systems im August/September 2013, belegt: Das Qualitätsversprechen **„Made in Germany“ wird nach den Datenskandalen der letzten Wochen und Monate – Stichwort NSA und PRISM – in vielen Unternehmen zu einem wichtigen Entscheidungskriterium bei Investitionen in die IT-Sicherheit. Deutschen Produkten wird eine höhere Sicherheit bescheinigt. Insbesondere auf der Infrastrukturebene wollen Unternehmen künftig sehr viel stärker als bisher auf die Herkunft der eingesetzten Router achten.**

Generell haben derzeit etwa 76 Prozent der befragten Unternehmen überhaupt eine IT-Sicherheitsarchitektur. Weit über die Hälfte geht davon aus, dass diese sehr gut oder gut ist, etwa ein Viertel geht davon aus, dass sie befriedigend ist. Vor allem die Administration, der Schutz vor Hacker-Angriffen und Schad-Software werden etwas problematischer beurteilt, wohingegen Qualität und Zuverlässigkeit der Sicherheitsarchitektur von den Befragten besonders gut bewertet werden. Ein Viertel der teilnehmenden Unternehmen verfügt über keine Sicherheitsarchitektur.

17 Prozent der Befragten planen, die Investitionen in die IT-Sicherheit generell zu erhöhen. Unmittelbare Konsequenzen für die IT-Sicherheitsarchitektur zog nur jedes fünfte Unternehmen.

Die allgemeine Einstellung gegenüber der Herkunft von IT-Produkten hat sich stark verändert: Ein Großteil der Teilnehmer sieht einen gesteigerten Bedarf an IT-Sicherheitsprodukten „Made in Germany“ (71 Prozent) und wird in Zukunft mehr auf die Herkunft der eingesetzten IT-Produkte und insbesondere der Router (83 Prozent) achten.

73 Prozent der Befragten gehen nach PRISM davon aus, dass in ihren Produkten möglicherweise Hintertürchen, sogenannte Backdoors, vorhanden sind. Backdoors sind ein mehr oder weniger bekannter und oft leicht zu öffnender Zugang zu Unternehmensnetzen und dem darin verborgenen Wissen. Ihnen ist bewusst, dass Außenstehende Zugriff auf ihre Daten haben könnten. 67 Prozent der Befragten sind allerdings auch der Meinung, dass die Instanzen, die Zugriff auf die Backdoors haben – hier wurden vor allem Hardware- und Software-Hersteller und internationale Regierungs- und Sicherheitsstellen angeführt – dazu “befugt“ seien.

1. Methode

LANCOM System hat die Online-Umfrage „IT-Sicherheit – Zeit für einen Paradigmenwechsel?“ vom 06.08.2013 bis 19.09.2013 durchgeführt. **Ziel der Befragung war es, den derzeitigen Stellenwert von IT-Sicherheit in Unternehmen herauszufinden. Das Sicherheitsbewusstsein stand außerdem im Mittelpunkt der Umfrage. So wurde ergründet, ob sich durch PRISM und die Folgeskandale das Sicherheitsverständnis verändert hat: Wurden bereits Konsequenzen gezogen, oder sind zukünftig weitere Sicherheitsmaßnahmen geplant?. Ein weiterer Schwerpunkt der Umfrage lag auf der Beleuchtung der Infrastrukturebene.**

Die 242 Teilnehmer der nicht-repräsentativen Befragung wurden über Direktmailings an Kunden und Interessenten von LANCOM Systems, einen Newsletter von SecuMedia sowie über Social-Media-Kanäle und die unternehmenseigene Website gewonnen.

Der Fragebogen bestand aus zwei Fragen zur Bekanntheit von IT-Unternehmen im Bereich Netzwerksicherheit, 25 inhaltlichen Fragen rund um das Thema IT-Sicherheit und drei Fragen zum Unternehmen, in denen die Teilnehmer beschäftigt sind.

2. Ergebnisse

2.1. Demographie

98 Prozent der Teilnehmer sind männlich. 37 Prozent arbeiten in Unternehmen mit weniger als zehn Mitarbeitern. 13 Prozent sind in Firmen mit mehr als 1.000 Mitarbeitern beschäftigt. Die Teilnehmer arbeiten in Unternehmen unterschiedlicher Branchen. 57 Prozent gehören Unternehmen aus dem Bereich „IT/Telekommunikation“ an.

2.2. Ausgangslage

76 Prozent der befragten Unternehmen verfügen über eine IT-Sicherheitsarchitektur. Weit über die Hälfte geht davon aus, dass diese sehr gut oder gut ist, etwa ein Viertel geht davon aus, dass sie befriedigend ist. Vor allem Qualität und Zuverlässigkeit der Sicherheitsstruktur werden von den Befragten besonders gut bewertet. Administration, der Schutz vor Schad-Software und Hacker-Angriffen werden etwas schlechter eingestuft. In einem Viertel der befragten Unternehmen ist aktuell keine IT-Sicherheitsarchitektur vorhanden.

Die vorhandenen Sicherheitsarchitekturen der befragten Unternehmen decken sowohl den Bereich Software (Firewall, Spamfilter (E-Mail), Web-/Content-Filter), als auch Hardware (Router, Server, Clients) gut ab. Knapp 30 Prozent der Unternehmen setzen noch keinen Web-/Content-Filter ein. Als ein kritischer Punkt können die Prozesse für die IT-Sicherheitsarchitektur ausgemacht werden. Zwar sind Passwort-Regeln gängige Praxis – etwa 88 Prozent der Unternehmen bauen darauf – dagegen

sind in 44 Prozent der Unternehmen keine Security-Leitlinien vorhanden. Häufig wird auch auf die Zutritts-Kontrolle (44 Prozent) und auf ein Single-Sign-On-System (62 Prozent) verzichtet.

In allen befragten Unternehmen wird ein Schwerpunkt auf die Aktualität der IT-Sicherheitssoftware gelegt. Bei drei Viertel der Befragten ist das jüngste Element der IT-Sicherheitssoftware vor weniger als einem Jahr gekauft worden. Über 50 Prozent haben ihre Software sogar erst vor einem halben Jahr erworben. Auf der Hardwareseite sind die Router, die als Schnittstelle zwischen öffentlicher Infrastruktur und internen Netzen eine wichtige Schutzfunktion einnehmen, in über der Hälfte der Fälle älter als zwei Jahre.

Dagegen divergiert das Aktualisierungsverhalten kaum. 62 Prozent der Befragten gaben an, ihre Software im letzten Monat zuletzt aktualisiert zu haben, den Router hatten im Vergleich dazu 48 Prozent in diesem Zeitraum aktualisiert. Die Aktualisierungsfrequenz steht dabei in keinem Zusammenhang mit dem Alter des Routers oder der Software.

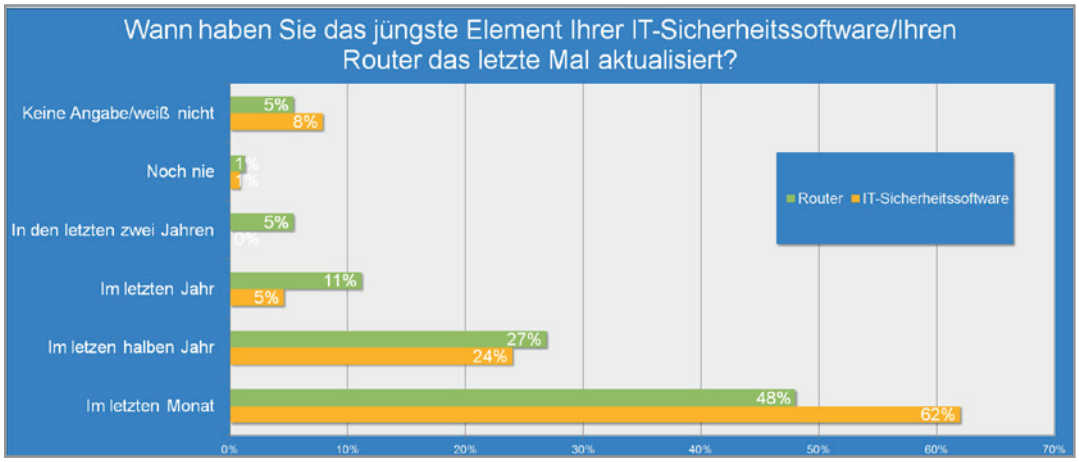

Abbildung 1: Wann haben Sie das jüngste Element Ihrer IT-Software/Ihren Router das letzte Mal aktualisiert?

96 Prozent der Befragten kennen die Bedeutung des Begriffs Backdoor. Gerade durch die Berichterstattung über den NSA-Datenskandal ist dieser Begriff sehr präsent. 32 Prozent der Befragten gehen davon aus, dass Backdoors in ihren IT-Komponenten vorhanden sind, 42 Prozent schließen es nicht aus und 20 Prozent glauben nicht, dass ihre IT-Komponenten diese Schwachstelle aufweisen.

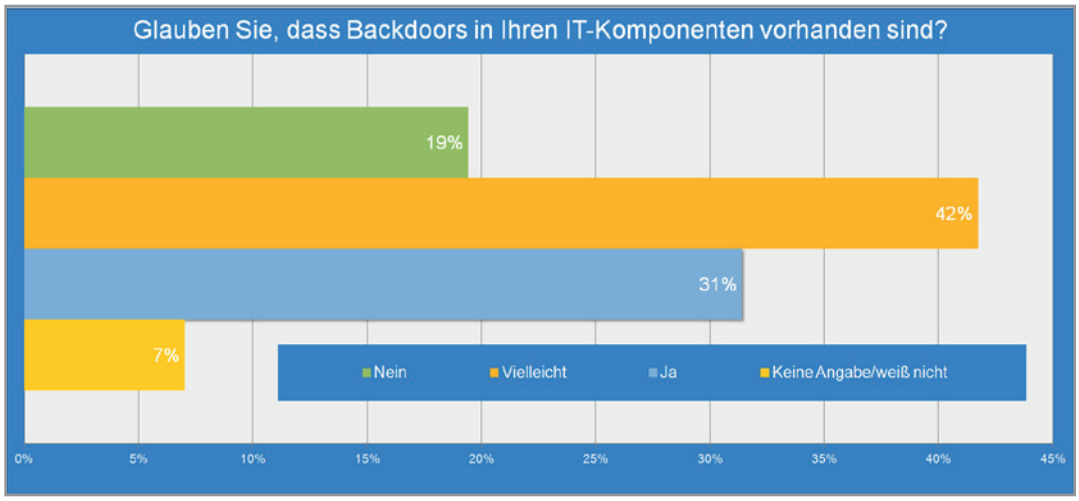

Abbildung 2: Glauben Sie, dass Backdoors in Ihren IT-Komponenten vorhanden sind?

Diejenigen Befragten, die glauben, dass ihre IT-Komponenten Backdoors enthalten, gehen davon aus, dass primär Hardware-Hersteller (65 Prozent), internationale Regierungs- und Sicherheitsstellen (60 Prozent) sowie Software-Hersteller (50 Prozent) auf diese zugreifen können. Jeweils rund 30 Prozent gehen auch davon aus, dass EU-Regierungs- und Sicherheitsstellen und sogar deutsche Behörden diese Backdoors nutzen könnten.

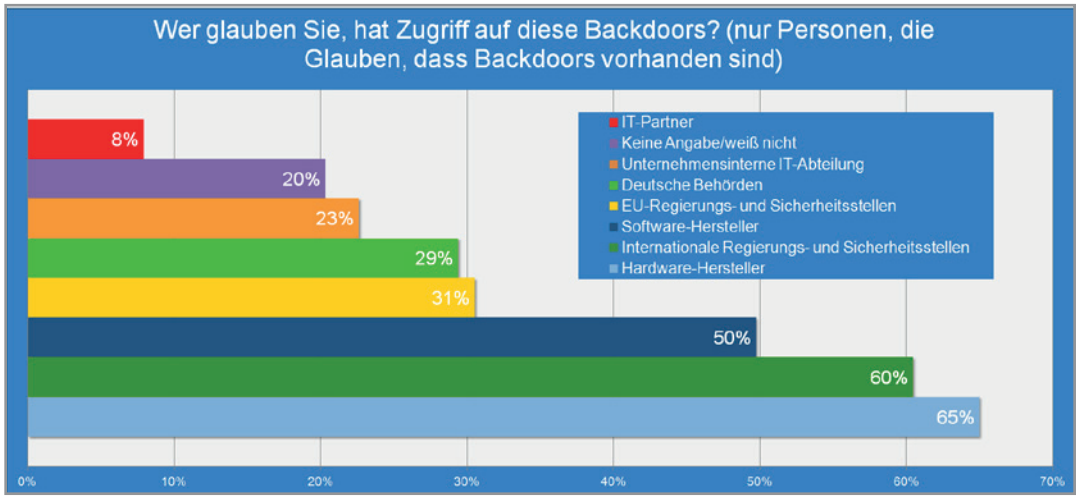

Abbildung 3: Wer glauben Sie, hat Zugriff auf diese Backdoors? (nur Personen, die glauben, dass Backdoors vorhanden sind)

3. Auswirkungen des NSA Datenskandals auf die IT-Sicherheit

3.1. Unsicherheit nach PRISM

Betrachtet man die Zustimmung zu der Aussage „Unberechtigte können nicht auf unsere Daten zugreifen“, die immerhin 65 Prozent der Befragten bejahen, scheinen die Befragten der Meinung zu sein, dass die Instanzen, die auf die Backdoors zugreifen können, auch dazu befugt sind.

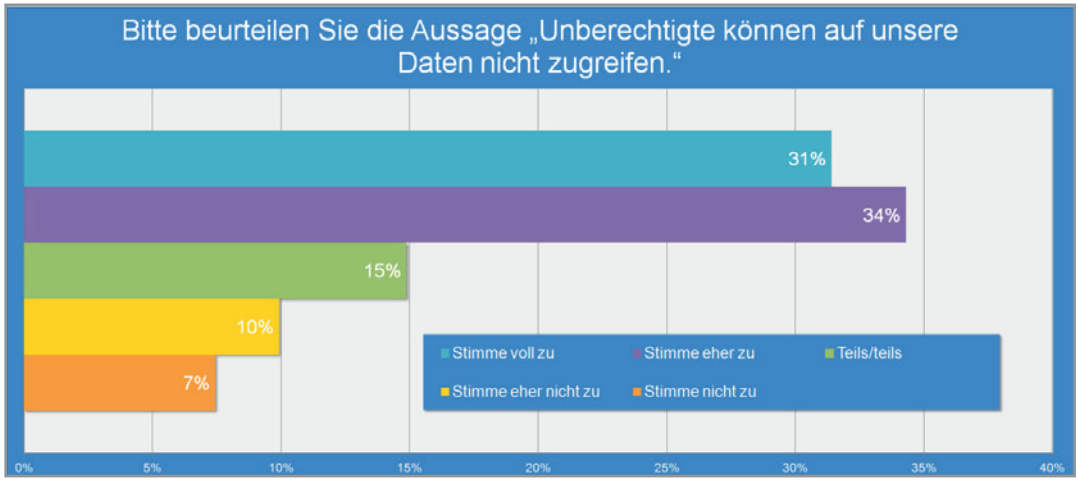

Abbildung 4: Bitte beurteilen Sie die Aussage „Unberechtigte können auf unsere Daten nicht zugreifen.“

3.1.1 Investitionsbereitschaft in die IT-Sicherheit

Um dieser Unsicherheit zu begegnen, ließe sich die IT-Sicherheit durch neue, sichere IT-Komponenten ausbauen.

Häufig priorisieren Unternehmen bei Entscheidungen den Kostenfaktor anstelle des Sicherheitsaspekts, sprich die Lösung mit der geringsten finanziellen Belastung wird favorisiert.

Zwar planen Unternehmen künftig nicht weniger in die IT-Sicherheit zu investieren – eine Erhöhung des Etats zu Gunsten der IT-Sicherheit ist jedoch nur in jedem sechsten Unternehmen (17 Prozent) geplant: Bei 65 Prozent der Unternehmen wird die Investition in die IT-Sicherheit gleich bleiben. In 17 Prozent der Unternehmen sollen sie steigen, und nur in 2 Prozent sinken.

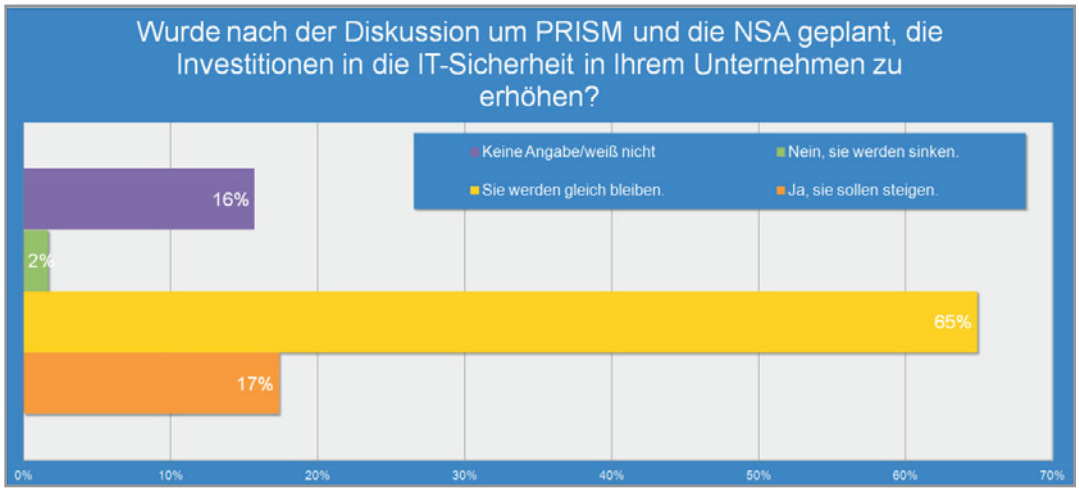

Abbildung 5: Wurde nach der Diskussion um PRISM und die NSA geplant, die Investitionen in die IT-Sicherheit in Ihrem Unternehmen zu erhöhen?

67 Prozent der befragten Unternehmen haben aufgrund des NSA-Datenskandals keine unmittelbaren Änderungen in der IT-Sicherheitsarchitektur vorgenommen und planen dies auch nicht. Immerhin jedes fünfte Unternehmen (19 Prozent) hat bereits Änderungen in seiner IT-Sicherheitsarchitektur vorgenommen oder plant dies.

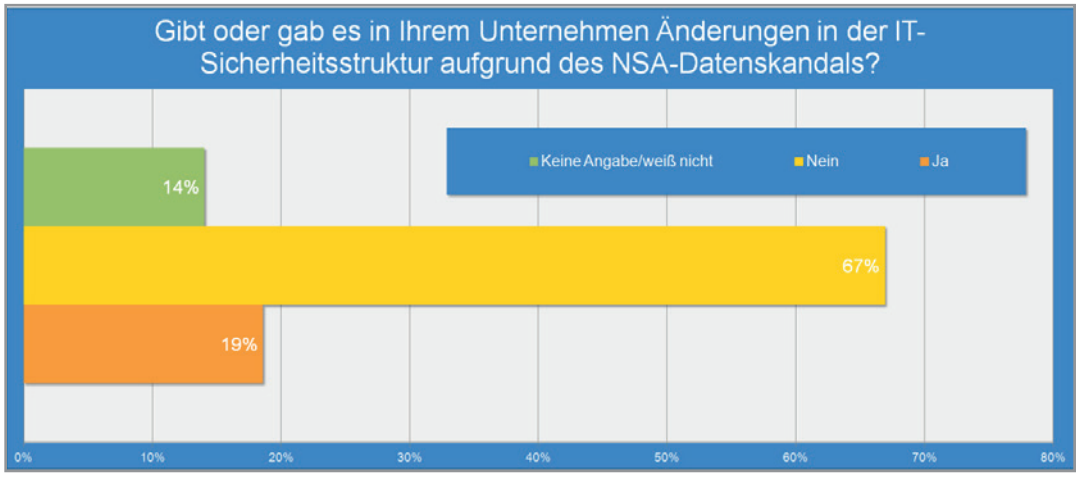

Abbildung 6: Gibt oder gab es in Ihrem Unternehmen Änderungen in der IT-Sicherheitsstruktur aufgrund des NSA-Datenskandals?

3.2 „Made in Germany" – der Ausweg aus der Unsicherheit?

Vor allem die Einstellung gegenüber deutschen Produkten und dem Qualitätssiegel „Made in Germany" hat sich gewandelt. Es überrascht nicht, dass nach den NSA-Datenskandalen deutsche Produkte höher im Kurs stehen. Den Bedarf an deutschen IT-Sicherheitsprodukten im Allgemeinen beurteilen die Befragten mit über 71 Prozent als gestiegen und stark gestiegen (14 Prozent). Nur ein Viertel (27 Prozent) der Befragten ist der Meinung, dass hier kein höherer Bedarf entsteht.

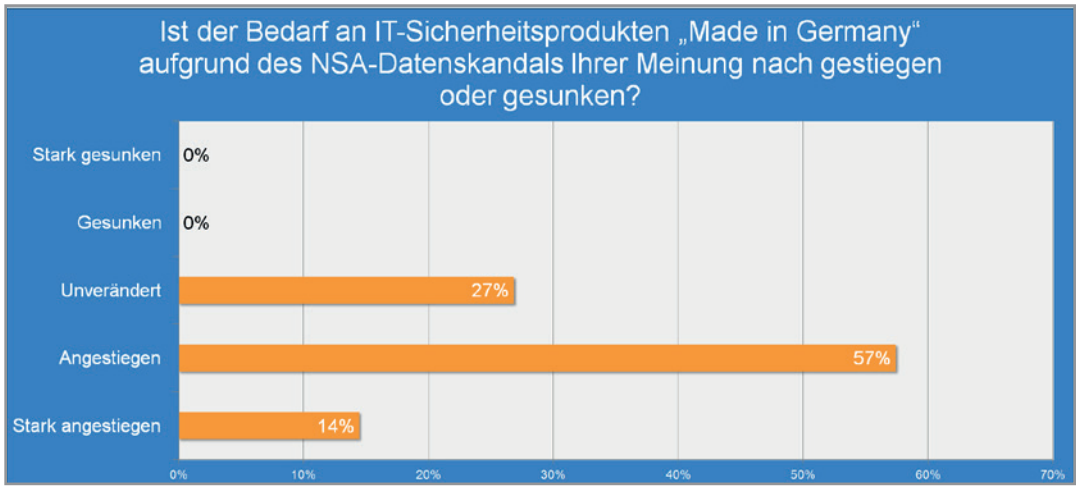

Abbildung 7: Ist der Bedarf an IT-Sicherheitsprodukten „Made in Germany“ aufgrund des NSA-Datenskandals Ihrer Meinung nach gestiegen oder gesunken?

Die Befragten stimmen nicht nur zu, dass der Bedarf generell gestiegen ist. Auf die konkrete Frage, ob sie selbst nach PRISM mehr auf das Siegel „Made in Germany“ achten werden, antworteten 43 Prozent der befragten Teilnehmer mit „Stimme voll zu“ oder „Stimme eher zu“. Jeder Dritte (33 Prozent) kann dazu keine eindeutige Aussage treffen. Jeder Vierte (23 Prozent) gab an, dass „Made in Germany“ für ihn künftig keine oder kaum Bedeutung haben wird.

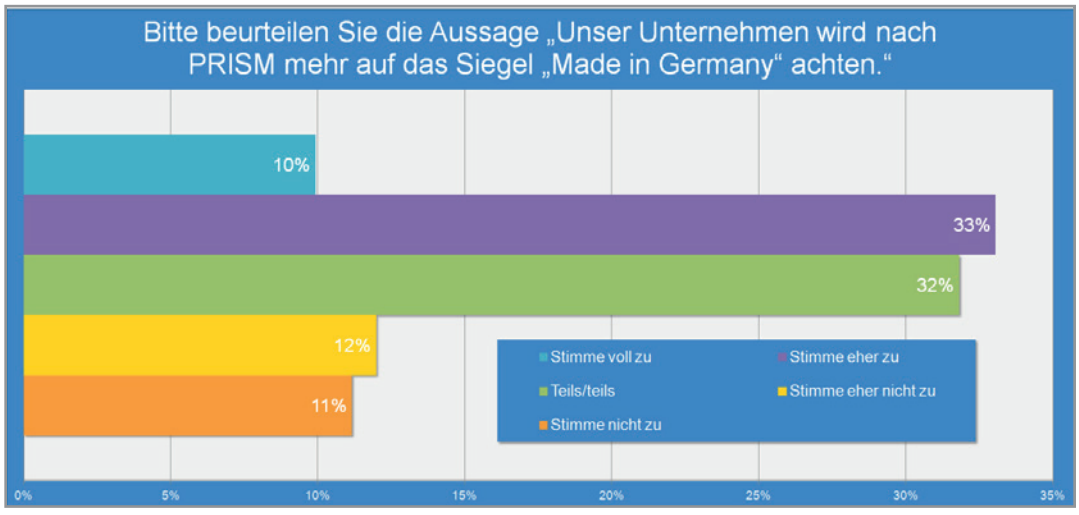

Abbildung 8: Bitte beurteilen Sie die Aussage „Unser Unternehmen wird nach PRISM mehr auf das Siegel „Made in Germany“ achten.“

Damit im Einklang steht die Beurteilung der Aussage „Deutsche Produkte sind grundsätzlich sicherer“. Diese beantworteten mehr als die Hälfte der Befragten (58 Prozent) entweder mit „Stimme voll zu“ oder „Stimme eher zu“

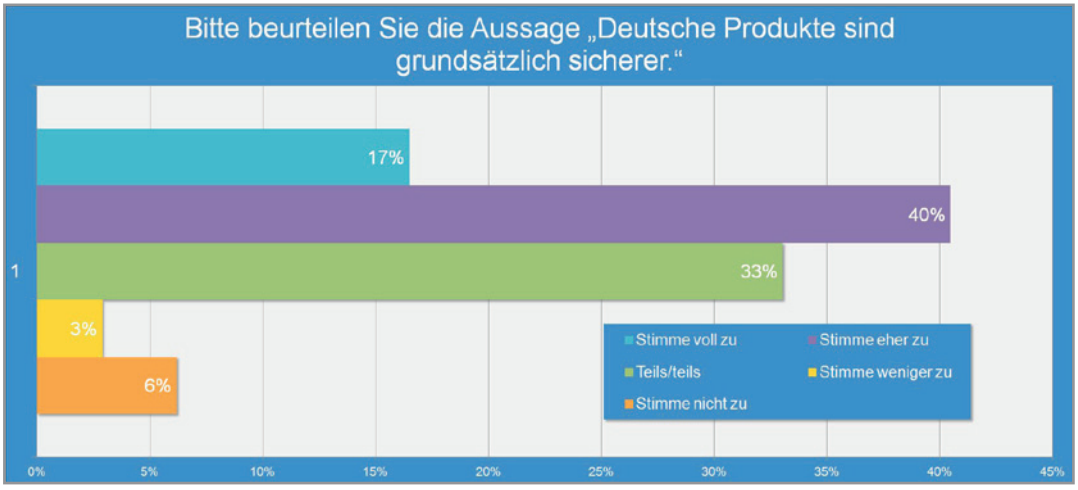

Abbildung 9: Bitte beurteilen Sie die Aussage „Deutsche Produkte sind grundsätzlich sicherer.“

3.2.1 Herkunft der Router

Betrachtet man insbesondere die Infrastrukturebene und die verwendeten Router, wird diese Entwicklung bzw. das Umdenken ebenfalls sichtbar. In der Vergangenheit achteten die Befragten nicht (39 Prozent) oder nur gelegentlich (27 Prozent) darauf, wo ihre Router produziert wurden. In der Zukunft wollen die Befragten der Herkunft dieser wichtigen Schnittstelle wesentlich mehr Beachtung zu schenken: 83 Prozent der Befragten gaben an, in Zukunft wahrscheinlich oder sicher auf die Herkunft ihres Routers zu achten – nur 7 Prozent werden dies nicht tun.

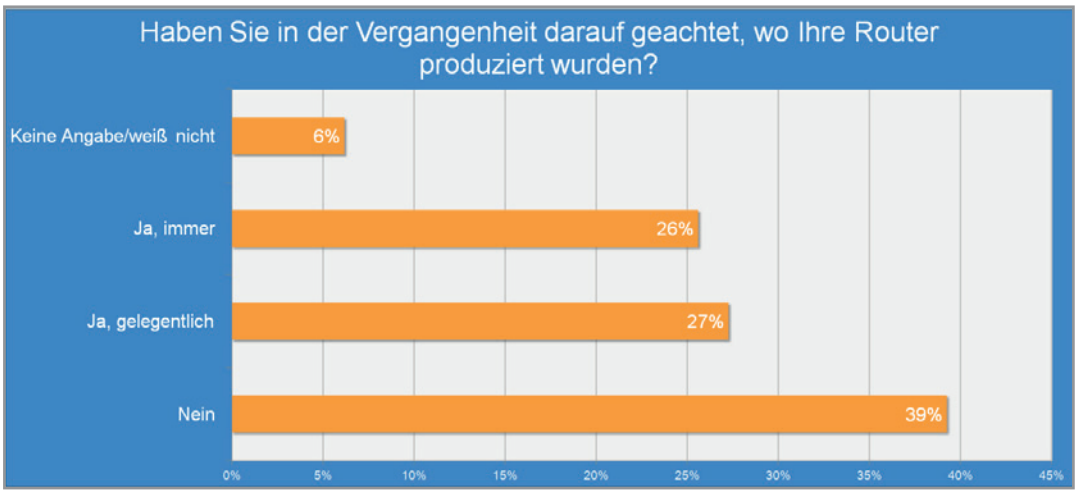

Abbildung 10: Haben Sie in der Vergangenheit darauf geachtet, wo Ihre Router produziert wurden?

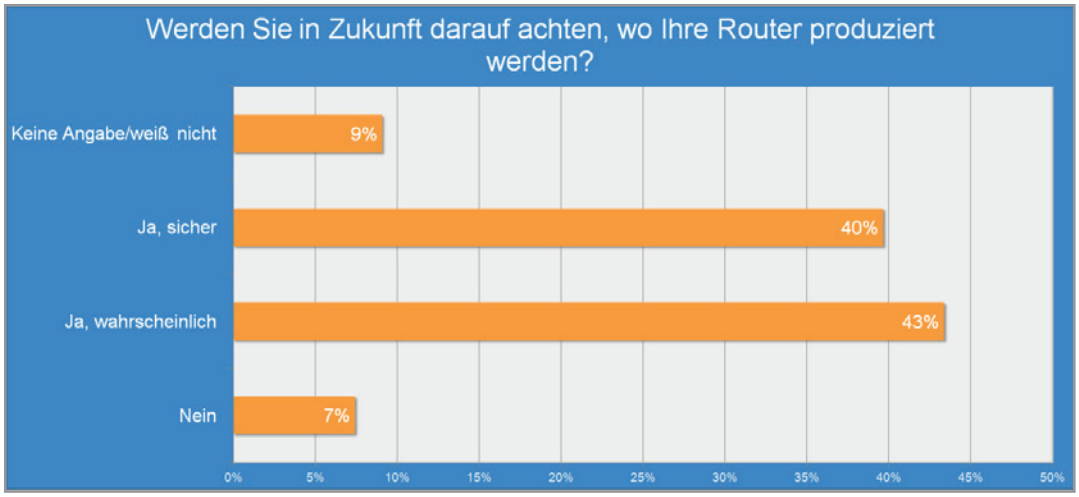

Abbildung 11: Werden Sie in Zukunft darauf achten, wo Ihre Router produziert werden?

3.2.2 Cloud und Server

Bisher halten etwa 36 Prozent der Befragten Teile ihrer Unternehmensdaten in der Cloud. Da die Datenschutzbestimmungen in Deutschland im Vergleich zu anderen Ländern strikter sind, sind Cloud-Dienste, die Server in Deutschland betreiben, potentiell sicherer. So wurde mit PRISM öffentlich, dass Daten, die auf US-amerikanischen Servern gespeichert sind, einfacher abgegriffen werden können – von Geheimdiensten, wie auch Unbefugten.

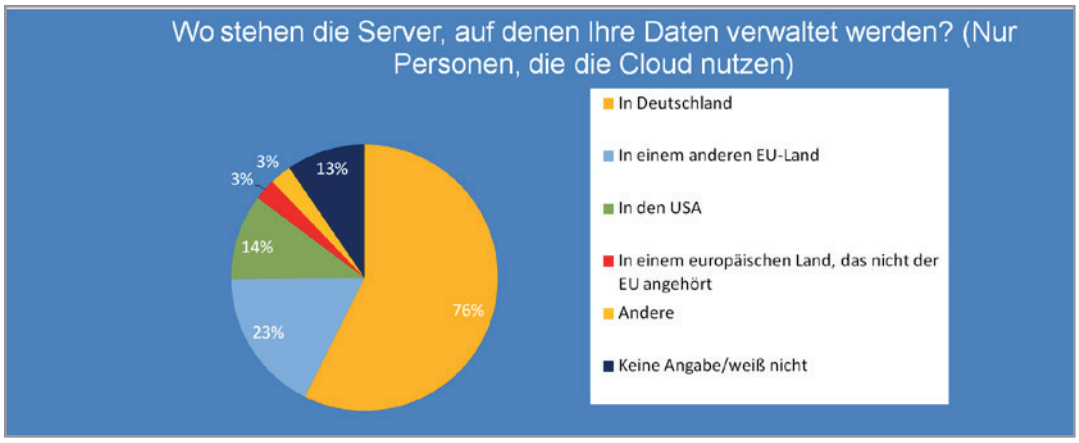

Abbildung 12: Wo stehen die Server, auf denen Ihre Daten verwaltet werden?

Die befragten Unternehmen, die Cloud-Services einsetzen, nutzen zu über 50 Prozent bewusst Cloud-Anbieter, die Server in Deutschland betreiben. In Deutschland stehen insgesamt 76 Prozent der Cloud-Service-Server, auf die die befragten Unternehmen zugreifen. 23 Prozent stehen in einem anderen EU-Land und nur 14 Prozent in den USA.

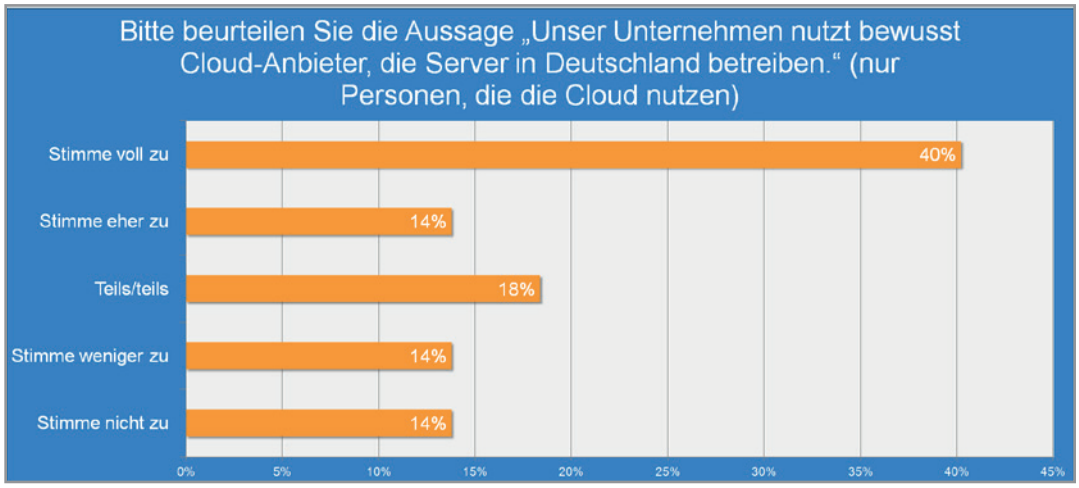

Abbildung 13: Bitte beurteilen Sie die Aussage „Unser Unternehmen nutzt bewusst Cloud-Anbieter, die Server in Deutschland betreiben.“ (nur Personen, die die Cloud nutzen)

58 Prozent der befragten Unternehmen, die Cloud-Services nutzen, verschlüsseln ihre Daten vor der Übertragung in die Cloud. 20 Prozent greifen zum Teil auf Verschlüsselung zurück und immer noch 22 Prozent verzichten auf die Verschlüsselung, bevor sie ihre Daten in die Cloud übertragen.

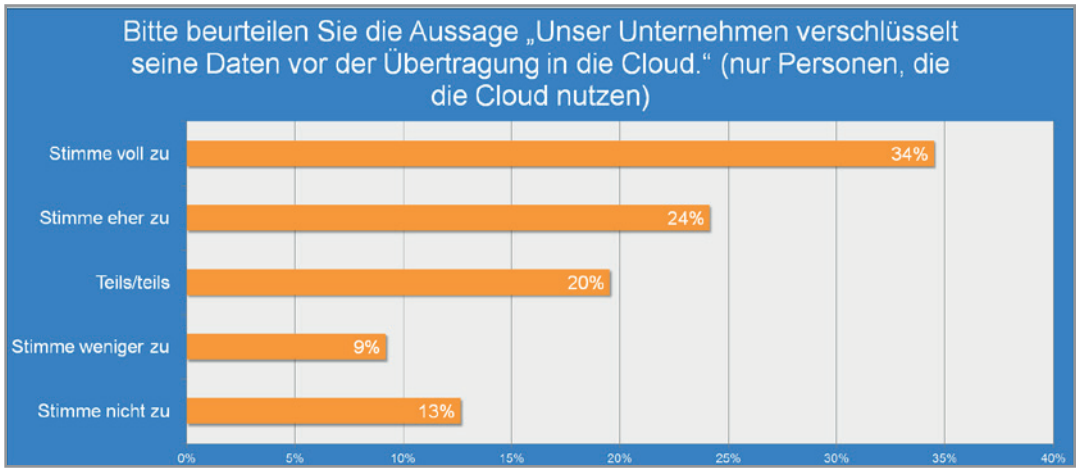

Abbildung 14: Bitte beurteilen Sie die Aussage „Unser Unternehmen verschlüsselt seine Daten vor der Übertragung in die Cloud.“ (nur Personen, die die Cloud nutzen)

3.3 Sicherheitszertifizierungen – ein sicherer Anker in unsicheren Zeiten

Über die Hälfte (57 Prozent) der Befragten kennt keine Zertifizierungen für IT-Sicherheitsprodukte. Zertifikate sind allerdings ein Anhaltspunkt dafür, wie sicher und vertrauenswürdig ein IT-Produkt ist. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) etwa erteilt Zertifizierungen, die Transparenz bei den Sicherheitseigenschaften und der Vertrauenswürdigkeit von IT-Produkten schaffen. Immerhin 60 Prozent der Befragten, die Zertifizierungen für IT-Sicherheitsprodukte kennen (43 Prozent), sind mit den vom BSI erteilten Zertifizierungen vertraut.

30 Prozent der Umfrageteilnehmer werden künftig mehr auf zertifizierte Produkte achten. 36 Prozent der Befragten geben an, dass sie seit PRISM keinen größeren Wert auf zertifizierte Produkte legen. Dabei macht es keinen Unterschied, ob die befragte Person Zertifizierungen für IT-Sicherheitsprodukte kennt oder nicht.

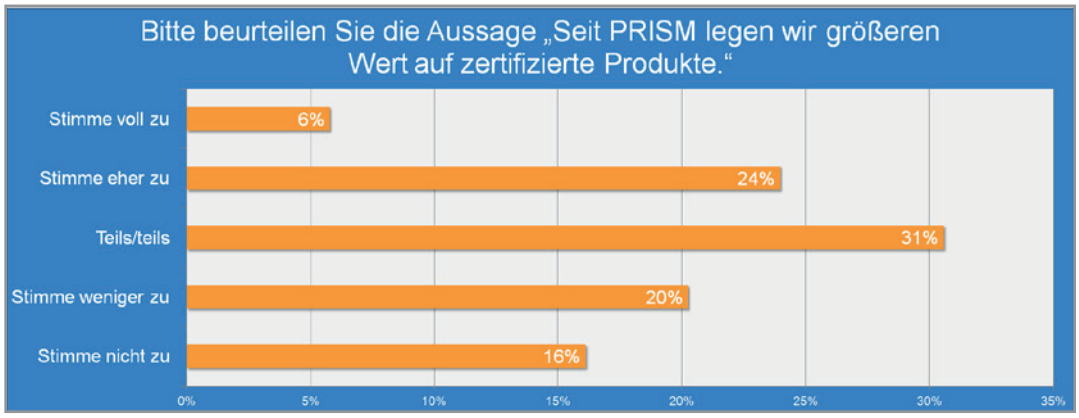

Abbildung 15: Bitte beurteilen Sie die Aussage „Seit PRISM legen wir größeren Wert auf zertifizierte Produkte.“

4. FAZIT

Die Mehrheit der befragten Unternehmen verfügt heute über eine umfassende IT-Sicherheitsarchitektur und stuft diese als gut bis sehr gut ein. Das ist ein erfreuliches Ergebnis der Umfrage IT-Sicherheit. Dies darf aber nicht darüber hinweg täuschen, dass es in jedem vierten Unternehmen keine IT-Sicherheitsarchitektur gibt.

Die Investitionsbereitschaft in die IT-Sicherheit ist nach PRISM bei den wenigsten Unternehmen gestiegen. Das mag einerseits überraschen, lässt andererseits aber vermuten, dass sie sich gut aufgestellt fühlen.

Unsicherheit – wem kann man vertrauen?

Es herrscht nach PRISM eine große Unsicherheit, die sich darin äußert, dass viele der befragten Unternehmen bei IT-Sicherheitsfragen keine eindeutige Meinung haben – so antwortete der größte Teil der Teilnehmer auf die Frage nach Backdoors, also bewusst eingebauten Hintertüren, in ihren IT-Komponenten mit "vielleicht". Auch bei der Frage, ob Unbefugte darauf zugreifen können, war das Meinungsbild recht unterschiedlich. Es ist naheliegend, dass die Schlagzeilen der letzten Wochen und Monate zu einer großen Verunsicherung geführt haben, Backdoors als potenzielles Risiko aber auch unterschätzt werden.

Anbieter, die sich offen verpflichten, ihre Geräte Backdoor-frei zu halten, können der steigenden Verunsicherung in der aktuellen Backdoor-Diskussion mit klaren Argumenten begegnen. Backdoor-Freiheit kann zu einem wichtigen Differenzierungsmerkmal gegenüber der Konkurrenz werden.

"Made in Germany" hoch im Kurs

Es zeichnet sich ein Trend hin zu heimischen Produkten ab. Deutschen IT-Produkten wird von den Umfrageteilnehmern eine höhere Sicherheit bescheinigt. Ein Großteil der Teilnehmer sieht nach PRISM einen gesteigerten Bedarf an IT-Sicherheitsprodukten „Made in Germany" und will in Zukunft mehr Wert auf die Herkunft der eingesetzten IT-Produkte. Auf der Infrastrukturebene wird der Herkunft der Router – der Schnittstelle zwischen öffentlicher Infrastruktur des Internets und internen Unternehmensnetzen und damit ein bevorzugtes Angriffsziel – künftig eine viel größere Bedeutung beigemessen als bisher. Hier spiegelt sich vermutlich die Vertrauenskrise gegenüber IT-Anbietern aus den USA und Asien wider.

Sicherheitszertifizierungen – noch nicht bekannt genug

Das Informationsniveau zu Sicherheitszertifizierungen erwies sich unter den Umfrageteilnehmern als recht unterschiedlich. Während die Mehrheit der Befragten keinerlei Sicherheitszertifizierungen kennt, sind die restlichen Befragten sehr gut über die einzelnen BSI-Zertifizierungen informiert.

Hier sind die Anbieter selbst, aber vor allem auch die Politik sowie andere öffentliche Instanzen gefordert, Aufklärungsarbeit zu leisten, um den Zertifizierungen zu einer stärkeren Bekanntheit zu verhelfen, damit diese in Zukunft als Kriterium für sichere und vertrauenswürdige IT-Komponenten stärker wahrgenommen werden.

Kurz: Es ist Zeit für einen Paradigmenwechsel! PRISM hat in deutschen Unternehmen zu einem Sicherheitsumdenken geführt. Die Verunsicherung und Vertrauenskrise kann für deutsche Hersteller zu einer echten Chance werden.