Pressestatement

Prof. Dieter Kempf, Präsident des BITKOM
Vortrag im Rahmen der Pressekonferenz „IT-Sicherheit in Unternehmen“

Hannover, 11. März 2014

Guten Morgen, meine sehr geehrten Damen und Herren!

Acht Monate nach den ersten Enthüllungen können wir sagen: Die NSA-Affäre hat sowohl die Einstellungen als auch das Verhalten der Anwender von Informations- und Kommunikationstechnologien verändert. Das betrifft Privatnutzer genauso wie die IT-Verantwortlichen in Unternehmen und anderen Organisationen. Es hat sich ein diffuses Gefühl der Unsicherheit breit gemacht. Konkret zeigen unsere Umfragen, dass es einen massiven Vertrauensverlust gibt, wenn es zum Beispiel um die Sicherheit von Daten im Internet geht. Unser aktueller Cloud Monitor hat ergeben, dass sich das Wachstum beim Einsatz von Cloud-Lösungen in Unternehmen infolge der Enthüllungen verlangsamt hat. Heute werfen wir einen genaueren Blick auf das Thema IT-Sicherheit in Unternehmen. Eine gut ausgestatte und organisierte IT-Sicherheit ist der Schlüssel zu einem besseren Schutz sowohl vor schnüffelnden Geheimdiensten als auch vor Cyber-Kriminellen.

Chart: Studiendesign: Umfrage zu IT-Sicherheit

Dazu haben wir eine Umfrage unter 403 Unternehmen in Deutschland durchgeführt. Befragt wurden IT-Verantwortliche und Geschäftsführer von Unternehmen ab 20 Mitarbeitern. Die Umfrage ist repräsentativ für die Gesamtwirtschaft. Eine ähnliche Umfrage haben wir im Jahr 2012 durchgeführt, so dass wir bei einigen Fragen einen Vergleich zur Vor-Snowden-Ära ziehen können.

Chart: Drei Viertel befürchten Cybercrime-Attacken

Fast drei Viertel (74 Prozent) der befragten Unternehmen sehen Angriffe auf ihre IT-Systeme als reale Gefahr. Dabei spielt es keine Rolle, ob diese von kriminellen Hackern, Wettbewerbern oder ausländischen Geheimdiensten ausgehen. Zum Vergleich: Im Jahr 2012 waren es 63 Prozent, also gut zehn Prozentpunkte weniger. Ein solcher Anstieg auf einem bereits sehr hohen Niveau ist ungewöhnlich. Das Positive: Mit dem Bewusstsein für Gefahren steigt auch die Bereitschaft,

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10
10117 Berlin
Tel. +49.30.27576-0
Fax +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Maurice Shahd
Pressesprecher
+49. 30. 27576-114
m.shahd@bitkom.org

Präsident
Prof. Dieter Kempf

Hauptgeschäftsführer
Dr. Bernhard Rohleder

mehr für die eigene IT-Sicherheit zu tun. Darauf werde ich gleich noch im Detail eingehen.

Chart: Reale Gefahr für die IT-Sicherheit

Die gefühlte Bedrohung ist stärker ausgeprägt als die tatsächliche Gefahr. Aber immerhin 30 Prozent der befragten Unternehmen stellten in den vergangenen zwei Jahren mindestens einen IT-Sicherheitsvorfall fest. Die Umfrage zeigt, dass die kleineren und mittleren Unternehmen mit 20 bis 499 Mitarbeitern mit einem Anteil von 31 Prozent deutlich stärker betroffen sind. Bei den großen Unternehmen ab 500 Mitarbeitern verzeichneten dagegen laut eigenen Angaben nur 11 Prozent IT-Sicherheitsvorfälle in den letzten zwei Jahren. Darüber hinaus müssen wir von einer hohen Dunkelziffer ausgehen, da viele Angriffe unentdeckt bleiben.

Chart: „Innentäter“ sind das größte Problem

Die Umfrage bestätigt die Erfahrung, dass die meisten IT-Sicherheitsvorfälle „vor Ort“ verursacht werden. 58 Prozent der Unternehmen mit Sicherheitsvorfällen berichten, dass die Störungen von eigenen oder externen Mitarbeitern ausgelöst wurden. Dabei handelt es sich oft um Attacken von so genannten Innentätern, die gezielt bestimmte Datensätze stehlen oder Viren einschleusen. Die Ursache ist aber nicht selten Unachtsamkeit oder Unwissenheit, wenn Mitarbeiter zum Beispiel mit Schadprogrammen verseuchte USB-Sticks verwenden oder von Kriminellen dazu verleitet werden, Informationen preiszugeben. Im Fachjargon wird hier von Social Engineering gesprochen. Darüber hinaus berichtet fast ein Drittel (30 Prozent) der Unternehmen, dass Angriffe über das Internet erfolgt sind. Hierzu zählen zum Beispiel Denial-of-Service-Attacken oder gezielte Einbrüche in IT-Systeme über das Internet.

Chart: Deutlich mehr Unternehmen haben Notfallpläne

Eine positive Entwicklung zeigt sich bei der Verbreitung von Notfallplänen für den Fall eines Datenverlustes. Zeit ist bei Angriffen auf IT-Systeme immer ein kritischer Faktor. Ein Notfallplan listet die wichtigsten Geschäftsprozesse des Unternehmens auf und beschreibt, was im Schadensfall zu tun und wer zu informieren ist. Wer hier ein klares Vorgehen und die richtigen Ansprechpartner dokumentiert hat, kann den Schaden eines IT-Sicherheitsvorfalls begrenzen. Umso wichtiger ist es, dass die Unternehmen vorbereitet sind. Neun von zehn Unternehmen (88 Prozent) haben inzwischen einen Notfallplan für Datenverluste. Vor zwei Jahren waren es

bei Unternehmen ab 20 Mitarbeitern erst 63 Prozent. Bezieht man kleinere Unternehmen ab 3 Mitarbeitern ein, war es damals sogar nur die Hälfte.

Chart: Bewusstsein für IT-Sicherheit steigt

Interessant ist die Frage, wie die Unternehmen auf die Enthüllungen über die nachrichtendienstlichen Spähaktionen reagiert haben. 36 Prozent geben an, dass sie ihre Maßnahmen im Bereich der IT-Sicherheit verstärkt haben. Übrigens gibt es kaum Unterschiede zwischen den mittelständischen und den großen Unternehmen ab 500 Mitarbeitern. Die Bewertung, ob 36 Prozent viel oder wenig sind, überlasse ich Ihnen. Wir wollen keine Panik machen, empfehlen aber, die NSA-Affäre zum Anlass zu nehmen, die eigene IT-Sicherheitsarchitektur kritisch zu überprüfen.

Chart: Unternehmen erhöhen technische und organisatorische Sicherheit

Mehr IT-Sicherheit lässt sich, vereinfacht gesagt, durch technische und organisatorische Maßnahmen erreichen. Zwei Drittel der Unternehmen, die aktiv geworden sind, haben organisatorische Verbesserungen eingeführt. Dazu gehören zum Beispiel ein Zugriffsmanagement für bestimmte Daten oder auch physische Zugangskontrollen für sicherheitskritische Bereiche. 43 Prozent haben Firewalls und 35 Prozent Virenschutzprogramme eingeführt oder erneuert. Ein Drittel der Unternehmen hat die Schulungen für die Mitarbeiter verstärkt – aus unserer Sicht ein ganz wichtiger Schritt zu mehr Sicherheit. Weitergehende Schritte wie Zertifizierungen oder die Einführung spezieller Angriffserkennungssysteme haben nur sehr wenige Unternehmen unternommen. Zur Einstellung zusätzlicher IT-Sicherheitsexperten hat die NSA-Affäre übrigens nicht geführt.

Chart: Fast ein Viertel investiert mehr in IT-Sicherheit

Fast ein Viertel (23 Prozent) der befragten Unternehmen hat seine Investitionen in IT-Sicherheit als Folge der NSA-Affäre verstärkt. Auch hier gibt es, was uns überrascht hat, kaum Unterschiede zwischen kleineren und größeren Unternehmen. Ganz offenkundig holt der Mittelstand in puncto Sicherheit auf.

Chart: Kaum Auswirkungen auf die IT-Investitionen

Abschließend haben wir die Frage gestellt, ob die Unternehmen infolge des Geheimdienstskandals generell Investitionen in neue IT-Lösungen verschieben oder sogar ganz auf diese verzichten. Das sind nur sehr wenige: 6 Prozent sagen, dass sie IT-Investitionen verschieben und 2 Prozent, dass sie auf Investitionen

verzichten. Was wir aber durchaus feststellen, ist dass sich Investitionen verlagern. So stehen eine Reihe von Unternehmen Cloud-Lösungen wieder distanzierter gegenüber und favorisieren traditionelle Inhouse-Ansätze.

Chart: Schutzniveau erhöhen – Aufgabe von Politik und Wirtschaft

Meine Damen und Herren, die Folgen der NSA-Affäre werden Politik und Wirtschaft noch länger beschäftigen. Vor allem die politische Aufarbeitung steht erst ganz am Anfang. Notwendig sind unter anderem Verhandlungen über internationale No-Spy-Abkommen, auch wenn deren Umsetzung schwierig ist. Zumindest innerhalb der EU sollte man sich auf entsprechende Vereinbarungen einigen, um die Grundrechte der Bürger zu schützen und Wirtschaftsspionage durch Geheimdienste zu verhindern. Weitere wichtige Themen sind die Regelungen für internationale Datentransfers und die rechtlichen Voraussetzungen, unter denen Anbieter von Online-Diensten Kundendaten an staatliche Stellen herausgeben müssen.

Die Bedeutung der IT-Sicherheit reicht über die Abhöraffäre hinaus. Mit der zunehmenden Digitalisierung steigen die Gefahren durch professionell organisierte Cyber-Kriminelle. Sowohl auf nationaler als auch auf EU-Ebene sind deshalb gesetzliche Vorgaben in Arbeit. Ziel ist es, das Schutzniveau zu erhöhen. Diese Absicht unterstützen wir. Dabei müssen Nutzen, Wirtschaftlichkeit und technische Umsetzbarkeit berücksichtigt werden. Das gilt ganz besonders für die geplanten Meldepflichten für IT-Sicherheitsvorfälle. Es besteht Einigkeit darüber, dass mehr Informationen über die aktuelle Gefährdungslage notwendig sind. Es sollte aber klar definiert werden, welche Unternehmen meldepflichtig sind und welche Vorfälle gemeldet werden müssen. Andernfalls schaffen wir teure, bürokratische Strukturen, die nicht den gewünschten Zweck erzielen. Zudem müssen die Meldungen anonym erfolgen können. Es handelt sich bei Sicherheitsvorfällen häufig um sehr kritische Informationen, die Rückschlüsse auf die Sicherheitssysteme der Unternehmen und Betriebsgeheimnisse zulassen.

Der BITKOM fordert schon jetzt alle Unternehmen auf, Informationen zu IT-Sicherheitsvorfällen freiwillig zu teilen. Unter dem Dach der „Allianz für Cybersicherheit“ haben wir zusammen mit dem Bundesamt für Sicherheit in der Informationstechnik ein entsprechendes Meldesystem aufgebaut. Unser Ziel ist es, damit auch einen Beitrag zu einer neuen Sicherheitskultur zu leisten. Aktuell wagt es kaum ein Unternehmen öffentlich über Sicherheitsprobleme zu sprechen, weil die Angst groß ist, zusätzlich durch einen Reputationsverlust geschädigt zu

werden. Ein verlässlicher Schutz ist aber nur möglich, wenn IT-Anwender von den Erfahrungen anderer lernen. Eine Institution wie die Allianz für Cybersicherheit ist dafür eine geeignete Plattform, über die sich IT-Sicherheitsexperten austauschen können. Die Allianz hat aktuell rund 700 Mitglieder.

Die Unternehmen müssen sich so aufstellen, dass sie in der Lage sind, ihre Organisation bestmöglich zu schützen. Das fängt mit der Identifizierung sicherheitskritischer Daten an, reicht über Schulungen der Mitarbeiter bis zur regelmäßigen Überprüfung aller technischen Maßnahmen.

Die neue Bundesregierung hat dem Thema digitale Sicherheit, auch vor dem Hintergrund der NSA-Affäre, eine hohe Bedeutung gegeben. Die IT-Branche wird sich hier aktiv einbringen. Erster Schritt ist die Verabschiedung der IT-Strategie durch das BITKOM-Präsidium am Donnerstag. Damit wollen wir einen Beitrag zur geplanten „Digitalen Agenda“ der Bundesregierung leisten. IT-Sicherheit ist darin ein Kernthema.

Vielen Dank!