

## Studie von forsa und Hiscox zeigt: Digital Economy in Cyber-Gefahr

**Deutsche Digitalwirtschaft fürchtet Folgen von Cyberschäden / Durchwachsenes Zeugnis für Politik / Mitarbeiter rangieren auf Rang zwei und drei der Top-Risiken / Hauptbevollmächtigter von Hiscox Deutschland fordert: „Wir alle müssen gemeinsam für mehr IT-Sicherheit eintreten“. Die Digital Economy ist für die Sicherung des Standorts Deutschland im globalen Wettbewerb ein entscheidender Faktor. Als Innovationsindustrie ist sie in stärkerem Ausmaß als andere Branchen neuen Trends, Herausforderungen und Bedrohungen unterworfen. Vor diesem Hintergrund befragte forsa im Auftrag des Spezialversicherers Hiscox kleine und mittelständische Unternehmen der deutschen Digitalwirtschaft zu ihrem Umgang mit digitalen Cyber-Risiken. Die Studie zeigt: Trotz Wissens um die Bedrohung ist das Gefährdungspotential für die deutsche Digitalwirtschaft und damit den Wirtschaftsstandort Deutschland erheblich. Cyber-Risiken stellen eine handfeste Gefahr für die Unternehmensbilanzen und die künftige wirtschaftliche Entwicklung des digitalen Mittelstands in Deutschland dar: Zwei Drittel (66%) der Digitalunternehmen geben an, im Falle eines Cybervorfalls den laufenden Betrieb unterbrechen zu müssen.**

Deutsche Digitalwirtschaft fürchtet Folgen von Cyberschäden / Durchwachsenes Zeugnis für Politik / Mitarbeiter rangieren auf Rang zwei und drei der Top-Risiken / Hauptbevollmächtigter von Hiscox Deutschland fordert: „Wir alle müssen gemeinsam für mehr IT-Sicherheit eintreten“

Die Digital Economy ist für die Sicherung des Standorts Deutschland im globalen Wettbewerb ein entscheidender Faktor. Als Innovationsindustrie ist sie in stärkerem Ausmaß als andere Branchen neuen Trends, Herausforderungen und Bedrohungen unterworfen. Vor diesem Hintergrund befragte forsa im Auftrag des Spezialversicherers Hiscox kleine und mittelständische Unternehmen der deutschen Digitalwirtschaft zu ihrem Umgang mit digitalen Cyber-Risiken. Die Studie zeigt: Trotz Wissens um die Bedrohung ist das Gefährdungspotential für die deutsche Digitalwirtschaft und damit den Wirtschaftsstandort Deutschland erheblich.

Cyber-Risiken stellen eine handfeste Gefahr für die Unternehmensbilanzen und die künftige wirtschaftliche Entwicklung des digitalen Mittelstands in Deutschland dar: Zwei Drittel (66%) der Digitalunternehmen geben an, im Falle eines Cybervorfalls den laufenden Betrieb unterbrechen zu müssen. Eine Betriebsunterbrechung würde wiederum für 66% der Unternehmen spürbare Umsatzeinbußen bedeuten. Beinahe drei Viertel (73%) der befragten Digitalunternehmen würden im Falle eines Hackerangriffs oder von Datenverlust unter Reputationsverlust leiden und mehr als die Hälfte (55%) rechnet für diesen Fall damit, Kunden zu verlieren. Und die Gefahr ist real: Jedes vierte deutsche Digitalunternehmen (25%) hatte in der Vergangenheit bereits mindestens einen Cyberschaden zu verkraften. 72% dieser Schäden wurden verursacht durch Hackerangriffe, 36% waren Folge technischen Versagens und 14% bedingt durch den Verlust mobiler Devices oder den Diebstahl von Hardware.

Robert Dietrich, Hauptbevollmächtigter von Hiscox Deutschland, sagt dazu: „Die Digital Economy entwickelt sich in atemberaubendem Tempo und legt dabei die Grundlagen für die Zukunftsfähigkeit der deutschen Wirtschaft. Das Problem einer existenziellen Bedrohung der deutschen Digitalindustrie durch Cyber-Gefahren verlangt dringend nach einer Lösung: Wer kann der deutschen Digitalwirtschaft wie helfen? Um diese Frage zu beantworten, haben wir gemeinsam mit forsa untersucht, wie digitale Marktteilnehmer sich bereits schützen, wo ihre IT-Sicherheit Lücken aufweist und von wem sich die Wirtschaft Hilfe erhofft.“

## **Digitalunternehmen setzen auf technische Absicherung – und vernachlässigen andere Schutzmechanismen**

Das Ergebnis: Einen klaren Fokus setzt die deutsche Digital Economy bei der IT-Sicherheit auf technische Schutzmaßnahmen. Weitergehende Sicherheitsmechanismen werden jedoch vernachlässigt. Judith Leicht, stellvertretende Leiterin der Politik- und Sozialforschung bei forsa, fasst die Ergebnisse zum bestehenden Schutz zusammen: „Die höchsten Werte ermittelten wir bei technischen Sicherheitsmaßnahmen: 99%, also beinahe alle Befragten, nutzen eine Firewall und einen Virenschanner, 96% ein systematisches Backup-System, 88% verschlüsseln Kundendaten. Wesentlich geringer fielen die Werte jedoch bei nicht-technischen Maßnahmen aus: Nur 43% der Befragten nehmen externe Beratungsunternehmen für IT-Sicherheit in Anspruch, 36% besitzen einen Versicherungsschutz gegen Cyberrisiken. 38% halten keinen konkreten Krisenplan für den Umgang mit Datenverlust oder Hackerattacken vor oder wissen nicht, ob es so einen Plan für das Unternehmen gibt.“

## **Die Belegschaft: Vertrauenspersonen oder Risikofaktor?**

Wie schneiden die Mitarbeiter in der Risikobewertung der digitalen Spieler ab? Ob ungewollt oder böswillig: Das Verhalten der eigenen Belegschaft steht an Platz zwei und drei der Top-Risiken für Unternehmen. Befragt, welche Datenschäden den Unternehmensfortbestand gefährden würden, nennen nach Hackerattacken (67%) die meisten Befragten den gezielte Geheimnisverrat und Datendiebstahl durch Angestellte sowie die unbeabsichtigte Weitergabe sensibler Daten an Dritte (jeweils 56%). Robert Dietrich sagt: „Trotz aller Risiken, die von Mitarbeitern ausgehen – Im Bereich der Cybersicherheit ist das Vertrauensverhältnis zur eigenen Belegschaft ungebrochen. Stolze 88% der digitalen Unternehmen bewerten den Beitrag ihrer eigenen Mitarbeiter zur IT-Sicherheit als gut oder sehr gut.“

## **Digital Economy: Politische Maßnahmen bei Cybersicherheit ungenügend**

Die Politik wird vom deutschen Digital-Mittelstand kritisch beäugt: Mangelnde politische Vorkehrungen bedrohen in den Augen von mehr als der Hälfte (58%) den digitalen Wirtschaftsstandort Deutschland. Mehr als drei Viertel (76%) aller Befragten bewerten den Beitrag der Politik zur Steigerung der Datensicherheit in Deutschland insgesamt als weniger gut oder schlecht. In den Augen der Digital Economy ist die digitale Welt für große Teile der Politik offensichtlich noch immer absolutes Neuland. So erklärt sich jedenfalls die Entfremdung von Digital Economy und Politik: 87% fordern von den Volksvertretern, sich mehr Knowhow und Verständnis im Bereich IT-Sicherheit anzueignen. Selbst sonst zumeist ungeliebte staatliche Regulierungen scheinen vielerorts zu fehlen: Fast jedes zweite Digitalunternehmen (48%) wünscht sich mehr gesetzliche Eingriffe auf dem Feld der Datensicherheit. Von der deutschen Regierung fordern 72% zudem, den Druck auf Länder zu erhöhen, von denen Hackerattacken ausgehen.

## **Wer kann helfen: Unternehmen, Branchenverbände, Medien, Politik, Versicherungen und IT-Dienstleister**

Auf der Suche nach effektiver Unterstützung im Kampf gegen Cyber-Risiken fragte die Studie die Bedeutung unterschiedlicher Akteure aus Unternehmensperspektive ab: 96% der digitalen Marktteilnehmer sehen die Unternehmen selbst eher stark oder sehr stark in der Pflicht, die IT-Sicherheit zu stärken. Die Wirtschaft nimmt aber auch Hardware- und Softwarehersteller (92%) sowie Dienstleister und Berater (85%) ins Gebet. 66% fordern von den Medien, über Cyber-Risiken aufzuklären und ebenfalls rund zwei Drittel der Befragten (68%) setzen auf Information und Aufklärung durch Branchenverbände. Die staatliche Infrastruktur (61%) und die

Gesetzgebung (57%) werden ebenfalls von der Mehrheit der Befragten in Verantwortung genommen. Ein gutes Viertel (27%) betont den Beitrag von Versicherungen.

### **Gemeinsam für mehr IT-Sicherheit**

Zusammengefasst zeichnet die Studie ein deutliches Bild: Die Digital Economy fühlt sich durch Cyber-Gefahren bedroht. Die eigene IT-Sicherheit ist jedoch nicht immer imstande, den Gefahren effektiv zu begegnen. Robert Dietrich fasst zusammen: „Die digitale Wirtschaft sagt ganz klar: Nur im Zusammenspiel aller Akteure kann die IT-Sicherheit effektiv verbessert werden. Unternehmen, Branchenverbände, Politik, Versicherungen und IT-Dienstleister müssen an einen Tisch und gemeinsam für eine Verbesserung der IT-Sicherheit eintreten. Nur so kann die digitale Wettbewerbsfähigkeit Deutschlands erhalten und gestärkt werden.“

### **Einfache Versicherungslösungen gefragt**

Ein wichtiger Baustein im digitalen Risikomanagement ist eine Versicherung gegen digitale Risiken. Die Studie liefert Antworten auf die Frage, warum nur 36% der Digitalunternehmen sich mit einer digitale Risiken umfassenden Police absichern: 94% wünschen sich einfache Versicherungsbedingungen mit nur wenig Kleingedrucktem, 82% fordern passende und maßgeschneiderte Lösungen und mehr als die Hälfte (51%) will einen unkomplizierten Versicherungsabschluss im Internet. Hiscox brachte bereits im Februar 2011 als erster Anbieter eine Cyberversicherung auf den deutschen Markt: Cyber Risk Management by Hiscox. Egal ob online oder über Makler zeichnet sich die Cyber-Police durch vereinfachte Versicherungsbedingungen, weniger Ausschlüsse und ein für mittelständische Unternehmen nur sieben Fragen umfassendes Antragsmodell aus.

#### Über die Studie

Im Auftrag des Spezialversicherers Hiscox hat forsa Politik- und Sozialforschung GmbH eine Befragung von Unternehmen des Bereichs „digitale Dienstleistungen“ mit bis zu 200 Mitarbeitern und einem Jahresumsatz von mehr als Euro 17.500 durchgeführt. Zudem wurden ausschließlich Unternehmen befragt, die mindestens die Hälfte ihres Jahresumsatzes unter Einbezug digitaler Kanäle wie Webshops, Apps, E-Commerce, Hosting o.ä. erwirtschaften. Die Interviews wurden mit 204 Geschäftsführern bzw. Mitgliedern der oberen Führungsebene im Unternehmen durchgeführt.

Im Rahmen der Befragung wurde untersucht, wie die Unternehmen Daten-Risiken insgesamt wahrnehmen und sich über solche informieren, ob sie schon einmal Opfer von digitalen Schäden geworden sind und ob bzw. wie sie sich vor solchen digitalen Risiken schützen. Zudem wurde abgefragt, ob die Unternehmen sich auch gegen digitale Risiken versichern, welche Akteure ihrer Ansicht nach die Verantwortung für die Steigerung der IT-Sicherheit in Deutschland tragen und wie sie deren Beitrag bewerten.

Die Erhebung wurde vom 18. März bis 2. April 2015 mithilfe computergestützter Telefoninterviews (CATI) durchgeführt.

#### [Infografik](#)

#### **Pressekontakt:**

#### **HISCOX**

Thomas Heindl                    Indira Wulfange  
+49 (0)89 / 54 58 01 566 +49 (0) 89 54 58 01 567  
[thomas.heindl@hiscox.de](mailto:thomas.heindl@hiscox.de) [indira.wulfange@hiscox.de](mailto:indira.wulfange@hiscox.de)

**LoeschHundLiepold Kommunikation**

Jessica Vanscheidt  
Tegernseer Platz 7  
81541 München  
+49 (0) 89 72 01 87 271  
[j.vanscheidt@lhlk.de](mailto:j.vanscheidt@lhlk.de)

**Unternehmen:**

HISCOX  
Arnulfstraße 31  
80636 München  
Internet: [www.hiscox.de](http://www.hiscox.de)

**Über die HISCOX**

Hiscox ist ein internationaler Spezialversicherer mit einem auf die Absicherung beruflicher Risiken und privater Vermögenswerte fokussierten Versicherungsportfolio. Gegründet vor über 100 Jahren ist das Unternehmen an der London Stock Exchange notiert (LSE:HSX) und hat Büros in elf Ländern. Kunden mit hochwertigem Privatbesitz bietet Hiscox Versicherungen mit einer umfassenden Allgefahrendeckung, insbesondere für Kunst, wertvollen Hausrat, Ferienhäuser und Oldtimer sowie Lösegeldversicherungen. Für Kunstsammlungen und Kunstausstellungen bietet Hiscox spezielle Konzepte an. Für Geschäftskunden bietet Hiscox branchenspezifische Berufshaftpflicht- und D&O-Lösungen, die auf mittelständische Dienstleistungsunternehmen zugeschnitten sind. Hier konzentriert sich Hiscox auf die IT-, Medien-, Telekommunikations- sowie Unternehmensberatungsbranche.

hiscox