Presseinformation

Digitale Angriffe auf jedes zweite Unternehmen

- **Vorfälle verursachen Schäden von rund 51 Milliarden Euro pro Jahr**
- **Automobilbau, Chemieindustrie und Finanzwesen am häufigsten betroffen**
- **Kempf: „Besonders der Mittelstand muss sich besser schützen."**

Berlin, 16. April 2015

Gut die Hälfte (51 Prozent) aller Unternehmen in Deutschland ist in den vergangenen zwei Jahren Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden. Das hat eine Studie des Digitalverbands BITKOM ergeben. Für die Studie wurden Geschäftsführer und Sicherheitsverantwortliche von 1.074 Unternehmen repräsentativ befragt. Es handelt sich um die bislang umfassendste empirische Untersuchung dieses Themas. Der am stärksten gefährdete Wirtschaftszweig ist die Automobilindustrie mit 68 Prozent betroffenen Unternehmen. Es folgen die Chemie- und Pharma-Branche mit 66 Prozent sowie Banken und Versicherungen mit 60 Prozent. Nach konservativen Berechnungen des BITKOM beläuft sich der entstandene Schaden für die gesamte deutsche Wirtschaft auf rund 51 Milliarden Euro pro Jahr. „Digitale Angriffe sind eine reale Gefahr für Unternehmen", sagte BITKOM-Präsident Prof. Dieter Kempf bei Vorstellung der Studie in Berlin. „Viele Unternehmen schützen ihre materiellen und immateriellen Werte nicht ausreichend. Gerade der Mittelstand muss beim Thema Sicherheit nachlegen." Laut Umfrage sind mittelständische Unternehmen mit 61 Prozent am stärksten von Spionage- oder Sabotageakten betroffen.

Das am häufigsten auftretende Delikt ist der Diebstahl von IT- und Kommunikationsgeräten: In 28 Prozent der befragten Unternehmen sind in den letzten zwei Jahren zum Beispiel Computer, Smartphones oder Tablets gestohlen worden. Fast ein Fünftel (19 Prozent) registrierten Fälle von Social Engineering. Bei dieser Methode geht es darum, Mitarbeiter zu manipulieren, um an bestimmte Informationen zu gelangen. 17 Prozent der befragten Unternehmen berichten vom Diebstahl sensibler elektronischer Dokumente bzw. Daten und 16 Prozent von Sabotage ihrer IT-Systeme oder Betriebsabläufe. Bei 8 Prozent der Unternehmen ist die elektronische Kommunikation ausgespäht worden. Unter den großen Unternehmen ab 500 Mitarbeitern beträgt dieser Anteil sogar 15 Prozent. In 8 Prozent aller Unternehmen sind Besprechungen oder Telefonate abgehört worden.

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
Tel.: +49.30.27576-114
m.shahd@bitkom.org

Marc Bachmann
Bereichsleiter öffentliche Sicherheit
Tel.: +49.30.27576-102
m.bachmann@bitkom.org

Marc Fliehe
Bereichsleiter IT-Sicherheit
Tel.: +49.30.27576-242
m.fliehe@bitkom.org

Präsident
Prof. Dieter Kempf

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Häufigstes Angriffsziel sind die IT-Systeme und die Kommunikationsinfrastruktur der Unternehmen. Ein Drittel (34 Prozent) der attackierten Unternehmen nennen diesen Bereich. „IT-Systeme und Datennetze sind das Einfallstor für digitale Spionage- und Sabotageakte“, sagte Kempf. In 20 Prozent der betroffenen Unternehmen hatten es die Angreifer auf die Bereiche Lager und Logistik abgesehen. Es folgen der Einkauf (18 Prozent), die Produktion (15 Prozent) sowie die Geschäftsleitung (14 Prozent). In 9 Prozent der Unternehmen sind die Forschungs- und Entwicklungsabteilungen gehackt oder ausspioniert worden. Bei den großen Unternehmen ab 500 Mitarbeitern sind die F&E-Bereiche mit 30 Prozent bei fast jedem dritten Unternehmen betroffen.

Den Schaden als Folge digitaler Wirtschaftsspionage, Sabotage und Datendiebstahl berechnet der BITKOM mit rund 51 Milliarden Euro pro Jahr. Fast ein Viertel dieser Summe machen Umsatzeinbußen durch Plagiate aus. Es folgen Patentrechtsverletzungen, die ähnliche Folgen wie Plagiate haben. An dritter Stelle liegen Umsatzverluste durch den Verlust von Wettbewerbsvorteilen. Ein weiterer großer Posten sind Kosten infolge des Diebstahls von ITK-Geräten sowie Ausgaben, die durch den Ausfall von IT-Systemen oder die Störung von Betriebsabläufen entstehen. „Ein weicher Faktor mit großem Gewicht sind Imageschäden, die nach Sicherheitsvorfällen eintreten“, sagte Kempf. „Gelten ein Unternehmen oder seine Produkte bei Kunden und Geschäftspartnern erst einmal als unsicher, ist das nur schwer aus der Welt zu schaffen. Ein solcher Reputationsverlust kann ein Unternehmen in seiner Existenz gefährden.“

Nach den Ergebnissen der Umfrage treten vor allem aktuelle oder ehemalige Mitarbeiter als Täter in Erscheinung. Gut die Hälfte (52 Prozent) der betroffenen Unternehmen gibt diesen Personenkreis an. „Die eigenen Mitarbeiter sind für Unternehmen die wichtigste Ressource, aber auch das größte Risiko“, sagte Kempf. „Unternehmen sollten ihren Mitarbeitern nicht misstrauen, aber eine Sicherheitskultur etablieren.“ Die zweite große Tätergruppe mit 39 Prozent umfasst das unternehmerische Umfeld, bestehend aus Wettbewerbern, Lieferanten, Dienstleistern und Kunden. „Diese Gruppe ist häufig eng mit den Unternehmen verbunden und verfügt über Insiderkenntnisse, die kriminelle Handlungen erleichtern“, sagte Kempf. 17 Prozent nennen Hobby-Hacker als Täter. 11 Prozent sind Opfer organisierter Bandenkriminalität geworden und 3 Prozent standen im Visier ausländischer Geheimdienste. Bei 18 Prozent ist der Täterkreis unbekannt.

Als Reaktion auf die Vorfälle haben 53 Prozent der Betroffenen eine interne Untersuchung durchgeführt. Fast ein Drittel (30 Prozent) hat externe Spezialisten hinzugezogen. Dagegen hat nur jedes fünfte betroffene Unternehmen staatliche Stellen eingeschaltet. Gut ein Drittel (35 Prozent) derjenigen, die keine staatlichen Stellen informiert haben, nennt als Grund „Angst vor negativen Konsequenzen". Das kann zum Beispiel die Sicherung von Beweismitteln wie Computern sein. „Im Extremfall ist das Unternehmen während der Ermittlungen nicht mehr arbeitsfähig", sagte Kempf. 31 Prozent nennen den hohen Aufwand als Ursache. Fast ein Viertel (23 Prozent) hat Sorge vor einem Imageschaden, wenn die Vorfälle öffentlich werden. Ebenso viele sind der Meinung, die Täter würden ohnehin nicht gefasst. „Die Betroffenen sollten sich an die Behörden wenden. Diese müssen aber mehr tun, um das Vertrauen der Unternehmen zu gewinnen und ein kompetenter Ansprechpartner zu sein", betonte Kempf. Die geringe Meldequote spreche eine deutliche Sprache.

Aus Sicht des BITKOM müssen die Unternehmen mehr für den Schutz ihrer materiellen und immateriellen Werte tun und an folgenden Punkten ansetzen:

- IT-Sicherheit: Der Grundschutz, über den alle befragten Unternehmen verfügen, besteht aus Virenscannern, Firewalls und regelmäßigen Updates sämtlicher Programme. Dieser sollte durch spezielle Angriffserkennungssysteme ergänzt werden. Zusätzlichen Schutz bietet die Verschlüsselung sensibler Daten.
- Organisatorische Sicherheit: Dazu gehören unter anderem Regelungen, wer im internen Netzwerk auf welche Daten zugreifen darf und wer Zutritt zu sensiblen Bereichen eines Unternehmens bekommt. Ein Notfallmanagement gewährleistet eine schnelle Reaktion im Krisenfall. Darüber verfügt bisher nur knapp die Hälfte (49 Prozent) der Unternehmen in Deutschland.
- Personelle Sicherheit: Nur 52 Prozent der Befragten führt Schulungen der Mitarbeiter oder Sicherheitsüberprüfungen von Bewerbern durch. Eine angemessene Sicherheitskultur umfasst darüber hinaus die richtige Verwendung von Zugangsdaten, den korrekten Umgang mit externen Datenträgern oder Verhaltensregeln auf Reisen.
- Sicherheitszertifizierungen: Sie zwingen das Unternehmen, sich mit dem Thema intensiv auseinanderzusetzen. In der Praxis sind sie ein geeignetes Mittel, um höhere Sicherheitsstandards im gesamten Unternehmen zu etablieren.

Schärfere gesetzliche Regelungen über das geplante IT-Sicherheitsgesetz hinaus sind nach Ansicht der BITKOM-Branche nicht notwendig. „Das IT-Sicherheitsgesetz nimmt die Betreiber Kritischer Infrastrukturen in die Pflicht und wird perspektivisch zu mehr Sicherheit in der gesamten Wirtschaft führen“, sagte Kempf. Im laufenden Gesetzgebungsverfahren komme es darauf an, wie das Gesetz konkret ausgestaltet und wie es dann in der Praxis gelebt wird.

Hinweis zur Methodik: Grundlage der Angaben ist eine Umfrage, die Bitkom Research in Zusammenarbeit mit Aris Umfrageforschung im Auftrag des BITKOM durchgeführt hat. Dabei wurden im Januar und Februar 1.074 Unternehmen ab 10 Mitarbeitern befragt. Die Interviews wurden mit Führungskräften durchgeführt, die in ihrem Unternehmen für das Thema Wirtschaftsschutz verantwortlich sind. Dazu zählen Geschäftsführer sowie Führungskräfte aus den Bereichen Unternehmenssicherheit, IT-Sicherheit, Risikomanagement oder Finanzen. Die Umfrage ist repräsentativ für die Gesamtwirtschaft.