21.07.2017

Spionage, Sabotage, Datendiebstahl: Deutscher Wirtschaft entsteht jährlich ein Schaden von 55 Milliarden Euro

- Jedes zweite Unternehmen wurde in den vergangenen beiden Jahren angegriffen
- Nur jedes dritte Unternehmen meldet Attacken – Sorge vor Imageschäden schreckt ab
- Bitkom und Bundesverfassungsschutz stellen Studie zu Wirtschaftsschutz vor

Berlin, 21. Juli 2017 – Mehr als die Hälfte der Unternehmen in Deutschland (53 Prozent) sind in den vergangenen beiden Jahren Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden. Dadurch ist ein Schaden von rund 55 Milliarden Euro pro Jahr entstanden. Das ist das Ergebnis einer Studie des Digitalverbands Bitkom, für die 1.069 Geschäftsführer und Sicherheitsverantwortliche quer durch alle Branchen repräsentativ befragt wurden. Verglichen mit der ersten Studie vor zwei Jahren ist der Anteil der Betroffenen nur leicht von 51 auf 53 Prozent gestiegen, der Schaden ist zugleich um rund 8 Prozent von 51 auf 55 Milliarden Euro gewachsen. „Unternehmen müssen viel mehr für ihre digitale Sicherheit tun. Die Studie zeigt, dass die Gefahr für Unternehmen aller Branchen und jeder Größe real ist. Jeder kann Opfer von Spionage, Sabotage oder Datendiebstahl werden“, sagte Bitkom-Präsident Achim Berg bei der Vorstellung der Studie heute in Berlin. „Die Studie unterstreicht, dass wir in Zeiten von Digitalisierung und Industrie 4.0 unser besonderes Augenmerk auf die Abwehr von Spionageangriffen auf die deutsche Wirtschaft richten müssen. Im Sinne eines ganzheitlichen und nachhaltigen Wirtschaftsschutzes gehören dazu nicht allein IT-bezogene Maßnahmen, sondern risikominimierende Pläne in den Bereichen Organisation, Personal und Sensibilisierung. Wichtig ist aber auch die intensive Zusammenarbeit zwischen Wirtschaft und Behörden sowie den Behörden untereinander - wie in der „Initiative Wirtschaftsschutz“, betonte Dr. Hans-Georg Maaßen, Präsident des Bundesamtes für Verfassungsschutz (BfV).

In jedem sechsten Unternehmen (17 Prozent) wurden in den vergangenen zwei Jahren demnach sensible digitale Daten gestohlen. Vor allem Kommunikationsdaten wie E-Mails (41 Prozent) oder Finanzdaten (36 Prozent) fielen dabei häufig in die Hände der Angreifer. In 17 Prozent der Fälle von Datendiebstahl wurden Kundendaten entwendet, in 11 Prozent Patente oder Informationen aus Forschung und Entwicklung, in 10 Prozent Mitarbeiterdaten.

Die Angreifer haben es aber nicht immer ausschließlich oder direkt auf digitale Daten abgesehen. Häufigstes Delikt ist der Diebstahl von IT- oder Telekommunikationsgeräten wie Notebooks oder Smartphones. Davon waren 30 Prozent der Unternehmen in den vergangenen zwei Jahren betroffen, wobei in der Regel unklar ist, ob die Täter es auf die Geräte an sich oder auf die darauf gespeicherten Daten abgesehen haben. Rund jedes fünfte Unternehmen berichtet von Social Engineering (Analoges Social Engineering 20 Prozent, Digitales Social Engineering 18 Prozent). Dabei werden Mitarbeiter manipuliert, um an sensible Informationen zu kommen, mit denen dann in einem weiteren Schritt zum Beispiel Schadsoftware auf die Firmenrechner gebracht werden kann. Jedes achte Unternehmen (12 Prozent) ist Opfer von digitaler Sabotage geworden, durch die zum Beispiel die Produktion gestört wurde. 8 Prozent berichten vom Ausspähen der digitalen Kommunikation wie E-Mails, 7 Prozent vom Abhören von

Telefonaten oder Besprechungen. Klassische analoge Angriffe kommen demgegenüber eher selten vor. So wurden 17 Prozent der Unternehmen Opfer eines klassischen Diebstahls von Dokumenten wie Papieren, Mustern oder Bauteilen, in lediglich 4 Prozent der Unternehmen wurden Produktionssysteme oder Betriebsabläufe auf analogem Weg sabotiert und lahmgelegt.

Täter sind besonders häufig aktuelle oder ehemalige Mitarbeiter des Unternehmens. 62 Prozent der Unternehmen, die in den vergangenen zwei Jahren Opfer von Spionage, Sabotage oder Datendiebstahl wurden, haben die Täter in diesem Personenkreis identifiziert. 41 Prozent der betroffenen Unternehmen machen Wettbewerber, Kunden, Lieferanten oder Dienstleister für die Angriffe verantwortlich, 21 Prozent Hobby-Hacker und 7 Prozent Personen aus der organisierten Kriminalität. Ausländische Nachrichtendienste wurden in 3 Prozent der Unternehmen als Täter identifiziert. 7 Prozent der Unternehmen geben an, dass die Täter unbekannt waren. Jedes dritte von Angriffen betroffene Unternehmen (37 Prozent) berichtet, dass die Täter aus Deutschland kamen. Der Großteil der Angriffe aber kommt aus dem Ausland: 23 Prozent der Unternehmen berichten von Tätern aus Osteuropa, 20 Prozent aus China und 18 Prozent aus Russland. Erst danach folgen die USA (15 Prozent), die Summe aller westeuropäischen Länder (12 Prozent) und Japan (7 Prozent).

Nicht einmal jedes dritte betroffene Unternehmen (31 Prozent) schaltet staatliche Stellen ein. Dr. Maaßen: „Es gilt der Grundsatz „Need to share“, wenn wir gemeinsam die deutsche Volkswirtschaft widerstandsfähiger gegen Wirtschaftsspionage machen wollen. Nur wenn Unternehmen Angriffe melden, können die Sicherheitsbehörden ein realitätsnahes Lagebild erstellen und Abwehrstrategien entwickeln.“ Eine interne Untersuchung haben 46 Prozent der Unternehmen eingeleitet, externe Spezialisten wurden von 34 Prozent hinzugezogen. Überhaupt keine Untersuchung wurde nur von 3 Prozent der Betroffenen veranlasst, vor zwei Jahren waren es noch 10 Prozent. Erster Ansprechpartner bei den Behörden für die Unternehmen ist die Polizei, an die sich 84 Prozent jener Unternehmen wenden, die überhaupt staatliche Stellen einschalten. Die Staatsanwaltschaft informieren 57 Prozent. An die Datenschutz-Aufsicht oder an das Bundesamt für Sicherheit in der Informationstechnik wenden sich jeweils 15 Prozent, an den Verfassungsschutz 3 Prozent.

Hauptgrund dafür, sich nicht an die Behörden zu wenden, ist die Angst vor Imageschäden. Das geben 41 Prozent der Unternehmen an, die auf das Einschalten staatlicher Stellen verzichtet haben. Jeweils gut jedes dritte Unternehmen gibt an, man habe auf eine entsprechende Information verzichtet, weil man Angst vor negativen Konsequenzen habe (35 Prozent), weil die Täter ohnehin nicht gefasst würden (34 Prozent) oder weil der Aufwand zu hoch sei (29 Prozent).

Viele Unternehmen haben bereits Maßnahmen ergriffen, um sich besser gegen Angreifer zu schützen. So setzen alle Unternehmen einen technischen Basisschutz wie etwa Passwörter auf allen Geräten, Firewalls und Virenscanner ein und fertigen regelmäßig Backups ihrer Daten an. Anspruchsvollere Maßnahmen sind dagegen selten, etwa Intrusion Detection Systeme (20 Prozent) oder Penetrationstests (17 Prozent). Auch im Bereich der organisatorischen Sicherheit sind Standardmaßnahmen weit verbreitet, etwa die Festlegung von Zugriffsrechten für bestimmte Informationen (99 Prozent), die eindeutige Kennzeichnung von Betriebsgeheimnissen (85 Prozent) oder die Festlegung von Zutrittsrechten in bestimmte Unternehmensbereichen (81 Prozent). Dagegen setzt nur eine Minderheit auf Sicherheits-Zertifizierungen (43 Prozent) oder regelmäßige Sicherheits-Audits durch externe Spezialisten (24 Prozent). Großen Nachholbedarf gibt es im Bereich der personellen Sicherheit. Nur 6 von 10 Unternehmen (58 Prozent) führen Background-Checks bei Bewerbern für sensible Positionen durch, nur jedes zweite hat einen Sicherheitsverantwortlichen benannt (54 Prozent) oder schult Mitarbeiter zu Sicherheitsthemen (53 Prozent). „Wenn man bedenkt, dass Angriffe sehr oft durch aktuelle oder frühere Mitarbeiter erfolgen, so verwundert die Nachlässigkeit bei der Mitarbeiterschulung. Hier ließe sich die Sicherheit in den Unternehmen mit vergleichsweise geringem Aufwand und in kurzer Zeit deutlich verbessern“, so Berg.

Bitkom und Bundesverfassungsschutz geben Unternehmen, die Ihre Sicherheit verbessern wollen, folgende Tipps:

1. Sicherheit zur Chefsache machen

- Sensibilisierung der Geschäftsführung
- Initiieren firmenspezifischer Schutzüberlegungen auf Leitungsebene
- Einrichtung eines Wirtschaftsschutz-Beauftragten oder eines Informations-Sicherheitsbeauftragten

2. Technische IT-Sicherheit steigern

- Basisschutz ergänzt um Verschlüsselung und spezielle Angriffserkennung
- Security Information Event Management: Überwachung vernetzter Geräte und Erkennung von Anomalien
- Security by Design bei allen Schnittstellen und vernetzten Geräten
- Regelungen zum Umgang mit privaten und geschäftlichen mobilen Endgeräten

3. Organisatorische Sicherheit erhöhen

- Präventives und permanentes Risikomanagement etablieren: Externe Gefahren identifizieren, interne Schwachstellen aufdecken und rechtzeitig beheben
- Praxisorientierung aller Sicherheitsregularien
- Zugriffsrechte auf Daten sowie physische Zugangsrechte für sensible Bereiche
- Besuchermanagement: Umgang mit Gästen und Delegationen
- Notfallmanagement: Schnelle Reaktion im Krisenfall mit Notfallplan und Zuständigkeitsregelungen
- Etablierung einer „clean-desk-policy“: Welche Daten sind am Arbeitsplatz wirklich nötig?

4. Personelle Sicherheit verbessern

- Etablierung einer Sicherheitskultur
- Arbeitsplatzspezifische Schulungen/Sensibilisierungen
- Informationssicherheit auf Geschäftsreisen im Ausland beachten
- IT-Experten mit Produktions-Know-how

5. Sicherheitszertifizierungen anstreben.

Hinweis zur Methodik: Grundlage der Angaben ist eine Umfrage, die Bitkom Research im Auftrag des Digitalverbands Bitkom durchgeführt hat. Dabei wurden 1.069 Unternehmen mit 10 oder mehr 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 und Finanzen. Die Umfrage ist repräsentativ für die Gesamtwirtschaft.

Hier finden Sie die Präsentation zum Download: Wirtschaftsschutz in der digitalen Welt .

Diesen Beitrag teilen

Andreas Streim

Media Relations Manager E-Mail: a.streim@bitkom.org Tel.: +49 30 27576-112 Bitkom e.V.

Marc Bachmann

Bereichsleiter Luftfahrt und Verteidigung Bitkom e.V.