Pressekonferenz

Prof. Dieter Kempf, BITKOM-Präsident
Vortrag bei der Pressekonferenz zu digitaler Wirtschaftsspionage, Sabotage und Datendiebstahl in Unternehmen

Berlin, 16. April 2015

Guten Tag, meine Damen und Herren!

Wer die Berichterstattung zum Thema Sicherheit verfolgt, kennt die spektakulären Fälle des vergangenen Jahres: den Millionenfachen Identitätsdiebstahl in Deutschland gleich zu Jahresanfang, den groß angelegten Sony-Hack oder den Diebstahl von Prominenten-Fotos aus Apples iCloud. In der vergangenen Woche ist der französischsprachige Fernsehsender „TV5 Monde“ attackiert worden. Die Angreifer haben nicht nur Webseiten und Social-Media-Profile gehackt, sondern sind tief in die Sendetechnik eingedrungen. Das hat eine besondere Qualität. Bereits im vergangen Jahr hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) von gezielten Angriffen auf Industrieanlagen und Produktionsnetze berichtet. All diese Fälle sind nur die Spitze des Eisbergs. Die Gefahr für Unternehmen, Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl zu werden, ist real. Mit der vorliegenden Studie wollen wir für mehr Aufklärung sorgen und die Unternehmen sensibilisieren.

Mit 51 Prozent ist mehr als die Hälfte der 1.000 befragten Unternehmen in den vergangen zwei Jahren Opfer von Datendiebstahl, digitaler Wirtschaftsspionage oder Sabotage geworden. Weitere 28 Prozent sagen, dass ihr Unternehmen vermutlich betroffen ist. Am stärksten trifft es den Mittelstand mit 61 Prozent. Etwas über dem Durchschnitt (54 Prozent) liegen die großen Unternehmen ab 500 Mitarbeitern und etwas darunter die kleineren Betriebe mit 10 bis 99 Beschäftigten (47 Prozent). Der Mittelstand ist aus mehreren Gründen ein besonders lukratives Angriffsziel. Viele Unternehmen bieten sehr innovative Produkte an und haben in ihrem Marktsegment international eine starke Stellung. Häufig sind sie als Zulieferer fest in den Lieferketten von Großkonzerne verankert. Sie verfügen aber nicht über die gleichen Mittel zur Abwehr entsprechender Angriffe und können somit als Einfallstor dienen, um an die Geschäftsgeheimnisse der Großkonzerne zu gelangen.

Einen Schwerpunkt haben wir bei der Befragung auf die Betreiber kritischer Infrastrukturen gelegt, weil sie besonders wichtig für das Funktionieren unseres Gemeinwesens sind. Der Begriff ist relativ weit gefasst. Neben Energie- und Wasserversorgern, den Betreibern von Kommunikationsnetzen oder staatlichen Einrichtungen

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

gehören dazu auch die Ernährungswirtschaft oder die Medien. Die Befragung zeigt allerdings, dass die KRITIS-Branchen nicht stärker von den untersuchten Delikten betroffen sind als andere Wirtschaftszweige. Allerdings interessieren sich zum Teil andere Täterkreise für die Betreiber Kritischer Infrastrukturen. Dazu später mehr.

Der am stärksten gefährdete Wirtschaftszweig ist die starke deutsche Automobilindustrie mit 68 Prozent betroffener Unternehmen. Das überrascht nicht, denn die deutschen Fahrzeugbauer und ihre Zulieferer gehören zu den innovativsten Unternehmen weltweit. Es folgen die Chemie- und Pharma-Branche mit 66 Prozent sowie das Finanz- und Versicherungswesen mit 60 Prozent. Das Gesundheitswesen und die Medien kommen auf jeweils 58 Prozent. Die besonders kritischen Energie- und Wasserversorger liegen mit 45 Prozent unter dem Schnitt. Genauso wie der Maschinen- und Anlagenbau sowie die Ernährungsindustrie (44 Prozent).

Das am häufigsten auftretende Delikt ist mit 28 Prozent der Diebstahl von IT- und Kommunikationsgeräten. Allerdings geht daraus nicht hervor, ob es die Täter auf das Gerät oder die darauf befindlichen Informationen abgesehen haben. Fast ein Fünftel (19 Prozent) der Unternehmen registrierte in den vergangenen zwei Jahren Fälle von Social Engineering. Bei dieser Methode geht es darum, Mitarbeiter zu manipulieren, um an bestimmte Informationen zu gelangen. Häufig geht Social Engineering gezielten Hacking- oder Phishing-Angriffen voraus. Ein Beispiel: Die Täter geben sich am Telefon als Dienstleister aus und fragen nach Namen und Funktionen bestimmter Mitarbeiter. Auf dieser Grundlage entwerfen sie täuschend echte E-Mails, die die Adressaten veranlasst, eine mit einem Trojaner infizierte Datei zu öffnen, fingierte Rechnungen zu bezahlen oder persönliche Informationen preiszugeben.

17 Prozent der befragten Unternehmen berichten vom Diebstahl sensibler elektronischer Dokumente und 16 Prozent von Sabotage der IT-Systeme oder der Betriebsabläufe. Der Angriff auf den französischsprachigen TV-Sender war ein typischer Fall von erfolgreicher Sabotage. Das BSI hat einen Fall dokumentiert, bei dem in Deutschland ein Hochofen nach einem IT-Angriff schwer beschädigt wurde. Solche Vorfälle werden mit der immer stärkeren Vernetzung zunehmen. Bei 8 Prozent der Unternehmen ist elektronische Kommunikation ausgespäht worden. Bei großen Unternehmen ab 500 Mitarbeitern sind es sogar 15 Prozent. Ebenfalls 8 Prozent berichteten davon, dass Besprechungen und Telefonate abgehört wurden.

Bei den verschiedenen Delikten ist der Anteil der vermutlich Betroffenen unterschiedlich hoch. Beim Diebstahl von elektronischen Dokumenten und dem Ausspähen elektronischer Kommunikation ist er mit 19 bzw. 20 Prozent besonders hoch. Hier kommt vermutlich der NSA-Effekt zum Tragen. Die Frage ist, ob es echte Verdachtsfälle gab oder ob die Aussage „vermutlich betroffen" der allgemeinen Stimmungslage entspricht. Klar ist, dass es bei diesen Formen der digitalen Wirtschaftsspionage und -kriminalität eine sehr hohe Dunkelziffer gibt.

Drei Viertel der Unternehmen sind IT-Angriffen ausgesetzt. Sie sind in der Regel die Grundlage für Datendiebstahl oder Sabotageakte. Nahezu die Hälfte (45 Prozent) wird regelmäßig angegriffen, also mindestens einmal pro Monat, 30 Prozent seltener. Bei einem IT-Angriff handelt es sich meist um den Versuch, über das Internet in die IT-Systeme einer Organisation einzudringen. Der Angriff kann aber auch über einen infizierten USB-Stick oder andere Datenträger ausgelöst werden. Der Großteil wird von Firewall oder Virenscanner abgewehrt. Auf der anderen Seite bleiben viele Angriffe unentdeckt. Manche Schadsoftware ist so raffiniert programmiert, dass sie von normalen Virenscannern nicht mehr erkannt wird.

Häufigstes Angriffsziel sind die IT-Systeme und die Kommunikationsinfrastruktur der Unternehmen. Sie sind das Einfallstor für digitale Spionage- und Sabotageakte. Es folgen die Bereiche Lager und Logistik, der Einkauf, die Produktion sowie die Geschäftsleitung. Dass der Bereich Forschung und Entwicklung mit 9 Prozent am Ende dieses Rankings liegt, überrascht nur auf den ersten Blick. Die meisten kleinen Unternehmen, die den Großteil der Befragten ausmachen, haben gar keine eigenen Forschungs- und Entwicklungsabteilungen. Dagegen geben fast ein Drittel (30 Prozent) der großen Unternehmen ab 500 Mitarbeitern an, dass ihre F&E-Bereiche gehackt oder ausspioniert worden sind.

Den Schaden als Folge digitaler Wirtschaftsspionage, Sabotage und Datendiebstahl in Unternehmen beziffern wir auf rund 51 Milliarden Euro pro Jahr. Fast ein Viertel dieser Summe machen Umsatzeinbußen durch Plagiate aus. Es folgen Patentrechtsverletzungen. Diese haben ähnliche Folgen wie Plagiate, sind aber schwieriger zu bewerten. Gelangen zum Beispiel Wettbewerber an Patente für geplante Produkte, können sie diese vor oder zeitgleich mit dem Besitzer der Schutzrechte auf den Markt bringen. Das kann auch einzelne Features oder das Design eines Produkts betreffen. An dritter Stelle liegen Umsatzverluste durch Verlust von Wettbewerbsvorteilen. Ein weiterer großer Posten sind Kosten infolge des Diebstahls von ITK-Geräten und

Ausgaben, die bei Störungen von IT-Systemen oder der Betriebsabläufe entstehen. Ein weicher Faktor sind Imageschäden für die Unternehmen, die nach Sicherheitsvorfällen eintreten. Das darf man nicht unterschätzen. Gelten ein Unternehmen bzw. seine Produkte oder Dienste erst einmal mal als unsicher, ist das nur noch schwer aus der Welt zu schaffen. Und das wirkt sich auch finanziell negativ aus.

Wie sind unsere Statistiker bei der Berechnung der Schäden vorgegangen? Zunächst wurden die Schadenssummen für die einzelnen Delikte abgefragt und diese dann für jedes Unternehmen addiert. Diesen Gesamtschaden pro Unternehmen haben wir uns von den Befragten noch einmal verifizieren lassen. Dann wurden die Schadenssummen der einzelnen Delikte für die Gesamtwirtschaft hochgerechnet. Dabei wurden die Mittelwerte um Ausreißer nach oben und unten bereinigt. Natürlich können wir uns der Wirklichkeit nur annähern, haben aber eine solide statistische Grundlage. Damit vermittelt die Zahl eine realistische Größenordnung der verursachten Schäden.

Der mit Abstand wichtigste Täterkreis sind aktuelle oder ehemalige Mitarbeiter. Gut die Hälfte (52 Prozent) der betroffenen Unternehmen gibt diesen Personenkreis als Täter an. Die zweite Gruppe mit 39 Prozent umfasst das unternehmerische Umfeld, das aus Wettbewerbern, Lieferanten, Dienstleistern und sogar Kunden besteht. 17 Prozent nennen Hobby-Hacker als Täter. 11 Prozent sind Opfer Organisierter Bandenkriminalität geworden und nur 3 Prozent standen im Visier ausländische Geheimdienste. Bei 18 Prozent ist der Täterkreis unbekannt.

Bei dieser Frage lohnt ein Blick auf die Betreiber Kritischer Infrastrukturen. Von den betroffenen KRITIS-Unternehmen nennen 22 Prozent organisierte Banden als Täter im Vergleich zu 9 Prozent der Nicht-KRITIS-Unternehmen. Und 9 Prozent der Betreiber Kritischer Infrastrukturen identifizieren ausländische Geheimdienste als Täter, bei den sonstigen Branchen nur 2 Prozent. Wie stark die Nachrichtendienste tatsächlich aktiv sind, ist schwer einzuschätzen. Sie operieren ihrer Aufgabe entsprechend im Geheimen. Dagegen zeigen sich andere Hacker irgendwann, beispielsweise wenn sie ein Unternehmen erpressen oder einen Propagandaerfolg landen wollen.

Auffällige Unterschiede sind auch beim regionalen Ursprung der Taten erkennbar. Handlungen aus Deutschland und aus dem Ausland sind etwa gleich verteilt. Allerdings stammen bei den Betreibern Kritischer Infrastrukturen die Täter deutlich häufiger aus Russland, den USA, Westeuropa und China. Dagegen liegen bei den anderen Branchen Japan und Osteuropa – hinter Deutschland – ganz vorne.

Mit 53 Prozent der Betroffenen hat die Mehrheit der Unternehmen eine interne Untersuchung der Vorfälle durchgeführt. Fast ein Drittel (30 Prozent) hat externe Spezialisten hinzugezogen. Dagegen hat nur jedes fünfte betroffene Unternehmen staatliche Stellen eingeschaltet. Jedes zehnte Unternehmen gibt an, gar nichts unternommen zu haben. Ein Grund dafür kann sein, dass der Vorfall als zu unwichtig eingestuft wurde.

Was sind die Gründe, dass weder die Polizei noch anderen staatliche Stellen eingeschaltet wurden? Zuständig für diese in den Bereich Wirtschaftsschutz fallenden Delikte ist eigentlich der Verfassungsschutz. Gut ein Drittel 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 dann nicht mehr arbeitsfähig. 31 Prozent nennen den hohen Aufwand als Grund. Die Ereignisse müssen sauber dokumentiert und die Ermittler bei ihrer Arbeit unterstützt werden. 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.

Wir plädieren dafür, dass sich die Unternehmen an die Behörden wenden. Es gibt spezielle Dezernate, die sich um solche Fälle kümmern. Zudem ist es wichtig, dass die Behörden von möglichst vielen Fällen erfahren, um sich ein Bild über die jeweilige Bedrohungslage machen zu können. Diese Erkenntnisse fließen dann in die Ermittlungs- und Präventionsarbeit ein. Die Behörden müssen aber selbst mehr tun, um das Vertrauen der Unternehmen zu gewinnen und als kompetenter Ansprechpartner zu gelten. Die geringe Meldequote spricht hier eine deutliche Sprache.

Die Antworten auf die Frage nach den Sicherheitsmaßnahmen sehen auf den ersten Blick positiv aus, sind es aber nur bedingt. Alle Unternehmen geben an, dass sie über bestimmte technische Sicherheitsmaßnahmen verfügen. Dazu zählen zum Beispiel Virenscanner und Firewalls. Allerdings reichen diese in vielen Fällen nicht mehr aus. Neun von zehn Unternehmen (87 Prozent) ergreifen organisatorische Sicherheitsmaßnahmen in der einen oder anderen Form. Allerdings verfügt nur die Hälfte (51 Prozent) über ein Notfallmanagement, das im Ernstfall Schlimmeres verhindern kann. Maßnahmen der so genannten personellen Sicherheit ergreift nur die Hälfte (52 Prozent) der Unternehmen. Und das, obwohl die meisten Täter aktuelle oder ehemalige Mitarbeiter sind. In der Praxis zählen dazu zum Beispiel Schulungen, aber auch Sicherheitsüberprüfungen von Mitarbeitern oder Bewerbern.

Aus unserer Sicht müssen die Unternehmen mehr in den Schutz ihrer materiellen und immateriellen Werte investieren.

- An erster Stelle steht die Verbesserung der IT-Sicherheit: Der Grundschutz besteht aus Virencannern, Firewalls und regelmäßigen Updates aller eingesetzten Programme. Dieser sollte durch spezielle Angriffserkennungssysteme ergänzt werden. Zusätzlichen Schutz bietet die Verschlüsselung sensibler Daten.
- Ein weiterer wichtiger Bereich ist die organisatorische Sicherheit. Dazu gehören unter anderem die Regelung von Zugriffsrechten der Mitarbeiter auf Daten sowie der physischen Zugangsrechte für sensible Bereiche eines Unternehmens.
- Ein Notfallmanagement gewährleistet eine schnelle Reaktion im Krisenfall. Die Maßnahmen reichen vom Erstellen einer Kontaktliste mit den wichtigsten Ansprechpartnern bis zu mehrtägigen Übungen, bei denen verschiedene Szenarien durchgespielt werden.
- Deutlich unterschätzt wird der Faktor Mensch. Es geht nicht darum, seinen eigenen Mitarbeitern zu misstrauen. Es geht um die Entwicklung einer Sicherheitskultur, in der gewisse Standards selbstverständlich sind. Von dem gehackten TV-Sender sind Videos aufgetaucht, bei denen im Hintergrund Passwörter – sehr simple Passwörter – aufgetaucht sind. Das erscheint haarsträubend, dürfte von der Realität in vielen Unternehmen aber nicht weit entfernt sein.
- Letzter Punkt sind Sicherheitszertifizierungen. Sie zwingen das Unternehmen, sich mit dem Thema auseinanderzusetzen. In der Praxis sind sie ein geeignetes Mittel, um höhere Sicherheitsstandards im gesamten Unternehmen zu etablieren.

Bleibt die Frage nach schärferen Gesetzen. Aus unserer Sicht reicht das geplante IT-Sicherheitsgesetz aus. Es nimmt in erster Linie die Betreiber Kritischer Infrastrukturen in die Pflicht und wird perspektivisch zu mehr Sicherheit in der gesamten Wirtschaft führen. Im laufenden Gesetzgebungsverfahren kommt es darauf an, wie das Gesetz konkret ausgestaltet wird und wie es dann in der Praxis gelebt wird.

Vielen Dank!