Security Insider

Sicherheitsrisiko Industriespionage

Wirtschaftsspione nehmen den Mittelstand ins Visier

04.03.14 | Autor / Redakteur: Jürgen Schreier / Peter Schmitz

Mitarbeiter, die vertrauliche Unternehmens-Informationen aus Versehen, manchmal vielleicht wissentlich oder gar gegen Geld weitergeben, sind die Achillesferse jeder Sicherheitsstrategie. (Bild: Amir Kaljikovic - Fotolia.com)

Auch kleine und mittelständische deutsche Unternehmen werden immer häufiger Opfer von Industriespionage und Datenklau. Doch nicht immer ist es allein die IT und das Computernetzwerk, die große Angriffsflächen bieten. Der Faktor Mensch wird von den meisten Unternehmen gern übersehen oder unterschätzt.

Die Zahl der Fälle von Internetkriminalität und Wirtschaftsspionage ist in den vergangenen Jahren sprunghaft angestiegen. Nach Angaben des Bundeskriminalamtes in Wiesbaden wurden allein 2013 rund 60.000 Fälle registriert.

Seit 2007 attestiert die Wiesbadener Behörde sogar einen Anstieg der Fallzahlen von über 50 % mit einem geschätzten Schaden von 4,3 Mrd. Euro im Jahr. Folgeschäden und Verlust an Technologievorsprung nicht mitgerechnet.

Unternehmen haben Angst um das eigene Renommee

Gleichzeitig gäbe es ein riesiges Dunkelfeld, weil die meisten Unternehmen aus Angst um ihr Renommee den Gang zu den Behörden scheuen oder sogar Aufsehen

erregende Ermittlungen in der eigenen Belegschaft fürchten. Der Schaden für die Gesamtwirtschaft habe in der EU nach den konservativen Schätzungen von Europol im Jahr 2012 über 750 Mrd. Euro betragen. Damit steigt Wirtschaftsspionage neben Umweltrisiken und Finanzrisiken zu den größten Gefährdungen für Unternehmen auf.

„Die meisten Firmen tun auch heute noch zu wenig zum Schutz der eigenen Systeme“, sagt ein Pressesprecher des Bundesamtes für die Sicherheit in der Informationstechnologie, kurz BSI. Die Behörde ist in Deutschland für die Computersicherheit zuständig und warnt beispielsweise in ihren Veröffentlichungen vor akuten Gefahren aus dem Netz. Viel mehr kann die öffentliche Einrichtung für Firmen allerdings nicht leisten.

„Gerade im internationalen Geschäft sehen viele Unternehmen nur das, was man ihnen zeigt, oder nur das, was sie sehen wollen. Aber oft trügt der Schein“, sagt Frank Schurgers. Er ist Geschäftsführer von Integris International, einer Beratungsfirma, die sich auf das Erkennen und Minimieren von Sicherheitsrisiken im internationalen Geschäft spezialisiert hat.

Nicht nur Global Player haben Betriebsgeheimnisse

Schurgers bietet seinen Kunden daher umfassende Analysen und Lösungen, die Sicherheitslücken auch jenseits der IT diskret und kompetent ausfindig machen. Die erschreckende Zahl von 800.000 Netzangriffen, die laut Telekom jeden Tag auf deutsche Firmen und Privatanwender einprasseln, vermittelt einen Eindruck der schwierigen Lage.

Außerhalb des Stammhauses ist die Gefahr besonders groß

Besonders betroffen sind kleine und mittelständische Unternehmen. Sie verwenden oft Computerlösungen und Betriebsabläufe, die eher für Privatanwender zugeschnitten sind und lassen es überdurchschnittlich oft an einer geeigneten Abwehr oder Sicherheitsstrategie fehlen.

Doch die Daten über Transaktionen, Produktionsprozesse oder Fachpersonal sind als unternehmerisches Kapital bares Geld wert. Die meisten Chefs unterschätzen, dass viel Entwicklungszeit und Erfahrung allein in der Prozesskultur ihrer Firma stecken und was sie damit Konkurrenten voraushaben.

Auch der Leumund ist Gold wert. „Ein einziger Zwischenfall, kann den Ruf der ganzen Firma ruinieren“, weiß Marius M., der deshalb seinen vollen Namen nicht gedruckt sehen will. Der Geschäftsführer aus einem Zulieferbetrieb für die Flugzeugbranche aus Norddeutschland wunderte sich zusammen mit mehreren Mitarbeitern über Fehlfunktionen im Computersystem. Was er zu diesem Zeitpunkt noch nicht wusste -

Unbekannte hatten Zugriff auf etwa ein Dutzend Rechner in der Firma erlangt. Wie viele digitale Blaupausen dabei kopiert wurden, kann heute niemand mehr nachvollziehen.

In den Rechnern des produzierenden Betriebes war sprichwörtlich der Wurm drin. „Nach dem, was wir heute wissen, haben wir den Schädling auf einer Luftfahrmesse eingeschleppt. Er übertrug sich auf das System, als der Außenlaptop für einen Datentransfer an das Firmennetz angeschlossen wurde“, berichtet Marius M.

Der virtuelle Spion vom USB-Stick

Vielleicht kam der virtuelle Spion mit einer anderen Firmenpräsentation oder einer Bilderstrecke von einem USB-Stick auf den Computer. Dass einer seiner Mitarbeiter geschlampt hat oder die Sicherheit nicht so genau genommen hat, kann der Chef ebenfalls nicht ausschließen. Er war bei der Veranstaltung in Übersee nicht dabei und auch sonst kümmert sich niemand in der Firma hauptamtlich um Sicherheit und Abwehr. Wer genau wie lange in den Rechnern mitlas, weiß Marius M. auch deshalb bis heute nicht.

Das Szenario ist typisch und die große Angst vieler Betriebe. Bei Außenterminen, Zulieferern oder in Zweigniederlassungen, die weniger gut als das Stammhaus geschützt sind, haben Wirtschaftsspione oft leichtes Spiel. Vor allem kleine Unternehmen suchen daher oft händeringend nach einer Beratung, die sich in die eigene Betriebsführung einfügt und diskret, professionell und sicher ist. Statt reiner Sicherheitslösungen brauchen Firmen sinnvolle Geschäftslösungen. Daher ist es umso wichtiger das Sicherheitskonzept mit viel Erfahrung der Firma anzupassen.

„Als Private Intelligence Company stellen wir den Unternehmen Erkenntnisse und Kapazitäten zur Verfügung, die traditionell Regierungen und Geheimdiensten vorbehalten waren“, betont der Integris-Sicherheitsberater Schurgers.

Faktor Mensch wird unterschätzt

Doch der Schutz von Informationen ist auch mit IT-Sicherheit allein noch nicht geleistet. Ein viel größerer Unsicherheitsfaktor ist der Mensch. Mitarbeiter, die Informationen aus Versehen, manchmal vielleicht wissentlich oder gar gegen Geld weitergeben, sind die Achillesferse jeder Sicherheitsstrategie.

Daher hat sich die Entwicklung und Vermittlung von Sicherheitsbewusstsein in der Belegschaft zu einer wichtigen Säule in der Firmensicherheit entwickelt. Nur wenn auch die Mitarbeiter gegen Anfälligkeit, Erpressbarkeit oder Anwerbung abgeschirmt werden, kann eine Sicherheitsstrategie bestehen.

Wenn dann noch das Verhalten der Mitarbeiter und deren Schnittstellen zu

Betriebsgeheimnissen sinnvoll miteinander abgestimmt sind, lässt sich der Spionage vorbeugen. Dazu müssen alle Teile der Firma konkret wissen, was im täglichen Betrieb unbedenklich und was ein gefährliches Einfallstor für Kriminelle ist.