Spionageangriffe im Mittelstand

10.10.2012, 08:22 | Handel, Wirtschaft, Finanzen, Banken & Versicherungen

Pressemitteilung von: *SIUS Consulting*

Die zunehmende Globalisierung mit ihren ökonomisch wertvollen Verbindungen zu anderen Unternehmen wirkt sich aus wirtschaftlicher Sicht positiv für die deutsche Industrie aus. Gleichzeitig gehen hiervon aber auch eine Reihe massiv unterschätzter Gefahren aus. Ein Risiko ist nicht nur die Zunahme von staatlich gelenkter Wirtschaftsspionage, sondern auch die rasant ansteigenden Fälle der Konkurrenz- und Industriespionage.

Spionageaktivitäten in Deutschland
Nach der Definition geht die Wirtschaftsspionage von den Nachrichtendiensten der Staaten aus. Während es sich bei der Industrie- und Konkurrenzspionage um die illegale Beschaffung von Know-how und Waren durch konkurrierende Unternehmen handelt. Letztendlich kann es dem betroffenen Unternehmen jedoch egal sein, wer die Spionageangriffe veranlasst hat.

Experteneinschätzungen zufolge beträgt das jährliche Schadenspotential 4,5 Milliarden Euro. Reale Angaben zu den geschädigten Unternehmen können jedoch kaum abgegeben werden. Denn viele Geschädigte zeigen die Spionageangriffe wegen der Gefahr eines Imageschadens nicht an oder sind sich gar nicht bewusst, dass sie Opfer eines solchen Angriffs geworden sind. Letzteres gilt insbesondere für Spionageangriffe auf dem elektronischen Sektor.

Unternehmen in Deutschland kommen nicht über den Rohstoffmarkt zum Erfolg, sondern durch Know-how, Innovation und der Kunstfertigkeit von Ingenieuren, die zielorientiert und wirtschaftlich am Markt etabliert wird. Natürlich würden auch andere Staaten und Unternehmen gerne auf dieses Wissen zurückgreifen können, um Entwicklungsschritte zu optimieren, Kosten zu senken und ihre eigenen Erfolge langfristig zu steigern.

Die Folge sind daher oftmals Spionageangriffe, um an das Vorsprungwissen aus innovativen Technologien und strategisch wertvollen Informationen zu gelangen. Vorrangig begehrt sind Unternehmensinformationen aus den Branchen Maschinenbau, Motoren- und Fahrzeugbau sowie Elektro-, Mess- und Steuerungstechnik. Wobei auch Marktstrategien in den aktuell krisengeschüttelten Zeiten sehr gefragt sind.

Methoden der Spionageangriffe
In vergangenen Zeiten mussten Spione durch Befragungen und Beobachtungen aufwendige Recherchearbeiten leisten. Das Internetzeitalter und die modernen Techniken erleichtern den Zugriff auf Informationen und Daten jedoch ungemein. Websites und soziale Netzwerke können kinderleicht durchleuchtet werden. Digitale Abhörtechniken im Kleinstformat sind auch für den Laien unkompliziert und kostengünstig im Internet erhältlich.

Nach wie vor zählt jedoch der Mensch als wichtigste Informationsquelle und ist damit für Unternehmen der größte Risikofaktor. So sind es Menschen, die sich in Foren und Blogs austauschen oder auf sozialen Netzwerken Kontakte pflegen und dabei meist unabsichtlich mehr Informationen preisgeben, als prinzipiell sinnvoll. Auch an Bahnhöfen, Flugsteigen und im Zug werden sensible Informationen am Mobiltelefon mitgeteilt oder in zufällig einsehbarer Weise per Nachrichtenfunktion übermittelt, was den Tätern immens zugutekommt.

Schutz vor Spionage
Zunächst sollten Unternehmen ihre Sicherheitsstandards überarbeiten, was Besucherregelungen, Eingangskontrollen, Zutrittsprofile, Sicherheitsrichtlinien und IT-Sicherheit anbelangt. Unternehmensinterne Sicherheitsstandards müssen den Mitarbeitern in Schulungen nachhaltig vermittelt werden. Immer größeren Anklang finden dabei auch Security Awareness Kampagnen.

Bei Geschäftsreisen von Mitarbeitern kann ebenfalls aktiv Prävention betrieben werden. Eine klare Definition der wichtigsten Unternehmensdaten hilft dem Mitarbeiter, das Risiko von Spionageangriffen vorab selbst einzuschätzen und entsprechende Vorsicht walten zu lassen. Es gilt die Kerninhalte zu schützen, die oft nur 5% der gesamten Unternehmensdaten ausmachen. Der Zugriff auf diese besonders sensiblen Informationen sollte zudem nur einem auserwählten Personenkreis vorbehalten bleiben. Bereits im Vorhinein kann festgelegt werden, welche Informationen der Mitarbeiter auf Reisen mitführen darf. Der Dateninhalt auf mobilen Geräten sollte entsprechend begrenzt und verschlüsselt werden. Im Anschluss an Geschäftsreisen empfehlen sich Gespräche mit den Mitarbeitern, ob ihnen während der Reise besondere Vorkommnisse aufgefallen sind. Nur so können etwaige sicherheitsrelevante Vorfälle als solche auch identifiziert und ausgewertet werden. Eine abschließende Überprüfung von Datenträgern klärt auf, ob Unbefugte unbemerkt Spionageangriffe unternommen haben.

Für die Zukunft gilt, interne Sicherheitskonzepte ganzheitlich zu überdenken, Schwachstellen nachhaltig zu schließen, Mitarbeiter ausreichend auf potentielle Gefahren zu sensibilisieren und praktikable Abwehrmaßnahmen umzusetzen.

Heute zählt ein integriertes Security Management zu den Grundvoraussetzungen, um mit innovativen Produkten zukunftsfähig am Markt Bestand zu haben. Hierbei bieten spezialisierte Sicherheitsunternehmen bereits seit einigen Jahren die passenden Leistungspakete für den Mittelstand an.

Fazit
Die Spionage in Deutschland nimmt fortlaufend zu. Beim Kampf gegen das Ausspähen von Wirtschaftsdaten wird immer eine Dysbalance herrschen. Die Täter machen sich die kleinste Lücke im Sicherheitssystem zunutze, während die Unternehmen immer höheren Aufwand betreiben, um möglichst alle Schwachstellen zu schließen. Nur unter der ganzheitlichen Betrachtung einzelner sicherheitsrelevanter Faktoren ist es möglich, ein nachhaltiges Sicherheitsniveau im Unternehmen zu etablieren.
Wer als Unternehmen die heutige Vielfalt der Risiken erkennt und das Thema Sicherheit ernst nimmt, kommt nicht umhin einen kompetenten Partner für das Security Management zu verpflichten.

Portrait

SIUS Consulting bietet europaweit professionelle Sicherheitsberatungen und weitere Dienstleistungen rund um das Thema Unternehmenssicherheit - mit uns gehen Sie auf Nummer sicher!

News-ID: 669638 • Views: 137 (Stand: 05.06.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/669638/Spionageangriffe-im-Mittelstand.html