Entdeckt bei
http://www.maschinenmarkt.vogel.de/themenkanaele/managementundit/recht/articles/431983/?cmp=nl-97 von Jürgen Schreier 30. Januar 2014

Deutsche Industrie wird großflächig ausspioniert

Die Wirtschaftsspionage hat in Deutschland offenbar beträchtliche Ausmaße angenommen. Über die Täter weiß man wenig. (Bild: commons.wikimedia.org)

Fatal ist, dass sich in den Unternehmen ein Klima des *Misstrauens* entwickelt.

Deutsche Unternehmen sind nach Kenntnissen der Telekom-Sicherheitsabteilung auf breiter Front von Wirtschaftsspionage betroffen. Das hat der Leiter der Telekom-IT Sicherheit, Thomas Tschersich, gegenüber dem NDR bestätigt.

„Wir kennen durchaus Fälle, in denen erfolgreich mit Cyberwaffen angegriffen worden ist, um gezielt Informationen abzugreifen. Das Spektrum reicht vom Mittelstand bis zu Industrieunternehmen. Letzten Endes ist jeder betroffen“, so Tschersich im Gespräch mit NDR-Autor Klaus Scherer bei Recherchen für einen Film über Risiken neuer Technologien.

Herkunft der Täter unklar

„Wir wissen das, weil wir selbst Kundenunternehmen dabei unterstützen, ihre Systeme wieder zu sichern“, so Tschersich. Über mögliche Angreifer äußerte er sich zurückhaltend. „Es ist unheimlich schwer zu sagen, wer das ist, ob mutmaßlich nachrichtendienstliche Täter dahinter waren oder ein Onlinekrimineller, der sich nur eine verfügbare Angriffssoftware kopiert hat. Anhand der Waffen ist die Motivation gar nicht mehr zu unterscheiden.“

Die Diskussion über die Aktivitäten des US-Geheimdienstes NSA begrüßt Tschersich. „Der Vorteil der Debatte ist, dass der Stein ins Rollen gekommen ist. Wir haben Rechtsräume, die sich an nationalen Grenzen orientieren, und wir haben das Internet, das genau diese Grenzen überspannt. Das müssen wir irgendwie zusammenbekommen.“

Der Wirtschaft empfehle er eine digitale Nachbarschaftshilfe: „Wenn Sie wissen, wie bei Ihrem Nachbarn eingebrochen worden ist, dann sind Sie in der Lage, Ihre Fenster und Türen besser zu sichern.“

Sowohl in inhabergeführten Unternehmen mit wenigen *bestens bekannten* Angestellten als auch in Klein- und Großunternehmen keimt heutzutage ein *Generalverdacht* schnell auf.

30.000 Attacken im Monat auf Smartphone-Attrappen

Allein auf speziell eingerichteten Smartphone-Attrappen (Honeypots) registriert die Telekom 30.000 Attacken im Monat, die sie analysiert. Auch die Sorge vor eingeschleusten Spionen

wächst im Konzern. Dr. Bernd Eßer, Chef des konzerneigenen Cyber Emergency Response Teams (CERT), gegenüber dem NDR: „Hier im CERT würde ich nur sehr zögernd jemanden einstellen, der keinen deutschen Pass hat."

Dank Edward Joseph Snowden (und ich meine tatsächlich, dass wir ihm gar nicht genug danken könnten) sind wir alle im Privaten wie im Geschäftlichen für das Thema Ausspähen und Wirtschaftsspionage sensibilisiert worden.

Gegen derlei Spionage helfe keine äußere Firewall. „Da bekomme ich irgendwann eine Bewerbung von jemandem, der perfekt qualifiziert ist und genau auf die Stelle passt, der wahrscheinlich auch gar keine hohen Lohnforderungen hat, aber vielleicht sein Gehalt auch noch von anderen bezieht."

Ein Bericht aus dem Jahre 2009 zeigt, wie man noch vor wenigen Jahren der Illusion technischer Sicherheit zugeneigt war.

http://www.maschinenmarkt.vogel.de/themenkanaele/managementundit/recht/articles/191693/

Wirtschaftskriminalität

Deutsche Unternehmen verlieren 50 Mrd. Euro pro Jahr durch Wirtschaftsspionage

Viele Unternehmen in Deutschland betreiben einen hohen Aufwand beim Schutz vor Angriffen auf ihre Computernetzwerke. Sie vernachlässigen aber häufig, sich gegen herkömmliche Spionagemaßnahmen wie Diebstahl von Unterlagen oder Einbruch zu rüsten. Davor warnte Reinhard Vesper aus der Abteilung Verfassungsschutz des Innenministeriums Nordrhein-Westfalen, wie der ZVEI berichtet.

Insgesamt wird laut Vesper der jährliche Schaden (Erhebung aus dem Jahre 2009) durch Wirtschaftskriminalität in Deutschland auf bis zu 50 Mrd. Euro geschätzt: „Dabei ist von einer beträchtlichen Dunkelziffer auszugehen." Belastbare Zahlen zum Thema Wirtschaftsspionage gebe es nicht.

Sicherheitstechnik hilft gegen Wirtschaftsspionage

Viele bemerkte Fälle in der Wirtschaftsspionage seien klassische Diebstähle von Informationen, zum Beispiel durch Fotografieren von nicht ausreichend verschlossenen Papieren, sagte Vesper bei der Jahres-Pressekonferenz des Fachverbandes Sicherheitssysteme im ZVEI. „Ähnliche Vorsicht wie bei der Computersicherheit ist auch dringend von Nöten, wenn sensible Firmenunterlagen unterzubringen sind", sagte Vesper. „Unternehmen tun gut daran, sie durch mechanische und elektronische Sicherheitstechnik zu schützen."

Der im Mai veröffentlichte Verfassungsschutzbericht mache deutlich, dass insbesondere Russland und China sich um Know-how aus Deutschland bemühen, so Vesper. „Rezession und wachsender Konkurrenzdruck verschärfen die Situation

Auch kleine und mittlere Unternehmen von Wirtschaftsspionage betroffen

Interessant für ausländische Dienste seien nicht nur große Unternehmen. „So genannte Opfer- und Dunkelfeld-Studien zeigen, dass mindestens jedes dritte Unternehmen bereits Ziel eines Angriffs war.“ Neben technischem Wissen hätten auch Vertriebsdaten, Marktstrategien, Kalkulationen oder Personalplanungen kleiner und mittlerer Firmen besondere Anziehungskraft.

„Spione verhalten sich oft wie normale Diebe: Je einfacher und risikoloser sich eine Tat begehen lässt, umso wahrscheinlicher wird sie ausgeführt“, sagte der Sicherheitsexperte. Häufig könnten schon einfache Maßnahmen mit mechanischer und elektronischer Sicherheitstechnik erfolgreich abschrecken.

Fazit:

Loyalität, Vertrauen, Anstand, Sitte und Moral müssen im Unternehmen gelebt werden.

Mal abgesehen vom vermutlichen Ausspionieren durch NSA und Konsorten, wem kann man im Unternehmen heute noch trauen?

Wo Leitende, Geschäftsführer, Vorstände und Eigentümer aufgrund von Fehlverhalten sowie Mangel an Sitte und Moral Zutrauen und Vertrauen verspielen, wird es schwer den Mitarbeitern Loyalität, Ehrlichkeit und Anstand abzuverlangen.

Das Bewusstsein darüber ist die nächste aufkeimende Diskrepanz, die uns beschäftigen wird.

Wenn Sie als Start-Up oder KMU auf loyale und zuverlässige MitarbeiterInnen aufbauen wollen, dann sollten Sie umgehend strategisches Business Development und Education als ein Ganzes umsetzen.

Ich sage Ihnen, wie das funktioniert.

Rufen Sie mich jetzt an 02853 844 9165 oder senden Sie einfach sofort eine eMail

Stichwort: Spionieren und Ausspähen.

Carpe Diem, Ihr

Heinz-Peter Hippler

www.marketing4hightech.eu