

Link: <https://www.computerwoche.de/a/china-in-der-leitung,1903766>

Wirtschaftsspionage gefährdet 70.000 Arbeitsplätze

China in der Leitung!

Datum: 25.08.2009

Autor(en):Thomas Pelkmann

Die Versuche aus China und Russland, Unternehmen gezielt nach verwertbaren Informationen auszuhorchen, nehmen zu. Rund 70.000 Arbeitsplätze sind dadurch allein in Deutschland pro Jahr gefährdet. Wie Sie sich gegen das Aushorchen schützen können, weiß das Bundesamt für Verfassungsschutz.



Der Verfassungsschutz rät: Schauen Sie potentiellen Datendieben genau auf die Finger!

Foto: CW/Fotolia.com

Ein "Hauch Kalter Krieg" verspürte das Handelsblatt jüngst mit schaurig-wohligen Gruseln. Der Grund: Ein chinesischer Staatsanwalt hat vor wenigen Tagen vier Mitarbeiter eines australisch-britischen Bergbaukonzerns mit dem eher an Rotwein erinnernden Namen Rio Tinto wegen Spionage angeklagt. Die vier waren im Juli noch unter dem Vorwurf des Diebstahls von Staatsgeheimnissen inhaftiert worden. Nun werden sie lediglich beschuldigt, Geschäftsgeheimnisse der Stahlindustrie gestohlen und Personen bestochen zu haben, die keine Staatsbeamten waren. Damit rückt China vom direkten Vorwurf der Spionage ab und tritt offiziell auch Vermutungen entgegen, dass eigene Staatsbeamte in den Fall verwickelt sind.

Ausgerechnet China, das neben den Staaten der russischen Föderation sowie Ländern aus dem nahen und mittleren Osten in jüngster Zeit laut Bundesamt für Verfassungsschutz "umfangreiche elektronische Angriffe" auf deutsche Unternehmen startet.

Die Attacken zielen, wie der Verfassungsschutz analysiert, auf die "Beschaffung von Daten, die der Förderung des eigenen Unternehmens dienen" - oft auch mit Unterstützung staatlicher Geheimdienste.

Eine zunehmende Rolle beim Ausspähen von Daten nehmen dabei elektronische Angriffe ein, Maßnahmen mit und gegen IT-Infrastrukturen. Neben der reinen Informationsbeschaffung fallen darunter auch Aktivitäten, die zur Schädigung und Sabotage solcher Systeme geeignet sind.

"Dazu gehören das Ausspähen, Kopieren oder Verändern von Daten, die Übernahme einer fremden elektronischen Identität, der Missbrauch fremder IT-Infrastrukturen oder die Übernahme von computergesteuerten, netzgebundenen Produktions- und Steuereinrichtungen", heißt es im aktuellen Bericht der Verfassungsschützer. "Die Angriffe können dabei sowohl von außen über Computernetzwerke wie das Internet, als auch durch einen direkten, nicht netzgebundenen Zugriff auf einen Rechner mittels manipulierter Hardwarekomponenten erfolgen."

Eine der gängigsten Angriffsmethoden ist das Versenden von E-Mails, die einen durch ein Schadprogramm verseuchten Anhang besitzen. Solchen Angriffen gegen "erkennbar gezielt ausgesuchte Empfänger" geht ein umfangreiches "Social Engineering" voraus. Das dient dazu, persönliche Daten und Interessen auszuspähen, um den Angriff danach möglichst punktgenau setzen zu können.

Ein besonderer Risikofaktor in einer auf Unternehmensebene nahezu vollständig digitalisierten Welt sind die modernen IuK-Systeme. Die wichtigsten Unternehmensdaten liegen in elektronischer Form vor und werden bei Bedarf über Datenleitungen in Sekundenschnelle in die Welt versandt. So wichtig das für das Funktionieren global aufgestellter Unternehmen ist; es ist zugleich eine Einladung an Datendiebe und Saboteure. "Spionage via Internet", heißt es in einer Präventionsbroschüre des Verfassungsschutzes, "kennt keine zeitlichen und sprachlichen Barrieren, sie ist effizient und kostengünstig zugleich. Zudem birgt sie für den Angreifer, aufgrund der geografischen Unabhängigkeit, auch nur ein geringes Entdeckungsrisiko". Der wirtschaftliche Erfolg eines Unternehmens, heißt es denn auch weiter, hänge auch davon ab, wie gut es den Unternehmen gelingt, "sensible Datenbestände und die elektronische Kommunikation vor Datenverlust und Datenmissbrauch zu schützen".

Wie hoch der Schaden ist, der durch Wirtschaftsspionage in Deutschland verursacht wird, ist nur schwer zu beziffern. Zu groß ist die Dunkelziffer der Angriffe auf deutsches Unternehmens-Know-how. Anita Brandt-Zimmermann, Ministerialrätin aus dem nordrhein-westfälischen Innenministerium, versucht dennoch eine Schätzung. Sie beziffert den Schaden im Bereich der Wirtschaftsspionage auf rund 30 Milliarden Euro pro Jahr und rechnet, dass bis zu 70.000 Arbeitsplätze durch Ideendiebstahl und Markenpiraterie gefährdet sind.

Die 10 goldenen Regeln zum Schutz vor Wirtschaftsspionage

Dabei ist es nach übereinstimmender Meinung verschiedener Experten gar nicht so schwierig, sich vor dem Ausspähen von Daten zu schützen. Das Bundesamt für Verfassungsschutz hat in einer **Broschüre (PDF)**¹ die wichtigsten Verhaltenshinweise in den "10 Goldenen Regeln" der Prävention zusammengefasst.

Regel 1: Nicht warten, bis der Spionagefall eingetreten ist.

Regel 2: Aktuelle Informationen bei kompetenten Partnern einholen.

Regel 3: Informationsschutz als wichtigen Bestandteil der Firmenphilosophie und Firmenstrategie verankern.

Regel 4: Sicherheitsstandards regelmäßig analysieren.

Regel 5: Ganzheitliches Sicherheitskonzept realisieren und permanent fortschreiben.

Regel 6: Schutzmaßnahmen auf den Kernbestand zukunftssichernder Informationen konzentrieren.

Regel 7: Einhaltung und Erfolg der Sicherheitsvorkehrungen kontrollieren, Sicherheitsverstöße sanktionieren.

Regel 8: "Frühwarnsystem" zur Erkennung von Know-how-Verlusten installieren.

Regel 9: Auffälligkeiten und konkrete Hinweise konsequent verfolgen, professionelle Hilfe in Anspruch nehmen.

Regel 10: Informationsschutz als strategischen Erfolgsfaktor nutzen.

Eine der wichtigsten Voraussetzungen für die erfolgreiche Abwehr von Angriffen, so das Amt weiter, sei eine "Sensibilität gegenüber den Angriffsverfahren, Kenntnisse über die Methoden und Ziele der Nachrichtendienste, der Einsatz geeigneter Schutzmaßnahmen und die Einsicht in deren Notwendigkeit". Darüber sowie über alle weiteren Sicherheitsfragen bietet der **Verfassungsschutz**² kostenlose Beratungen an. Zuständig für Spionageabwehr und -prävention ist auf Firmenebene aber auch das **Bundesamt für die Sicherheit in der Informationstechnik (BSI)**³.

Links im Artikel:

¹ http://www.verfassungsschutz.de/download/SHOW/broschuere_0608_wirtschaftsspionage.pdf

² http://www.verfassungsschutz.de/de/arbeitsfelder/af_spionageabwehr_und_geheimschutz/

³ https://www.bsi.bund.de/cIn_134/DE/Home/home_node.html