

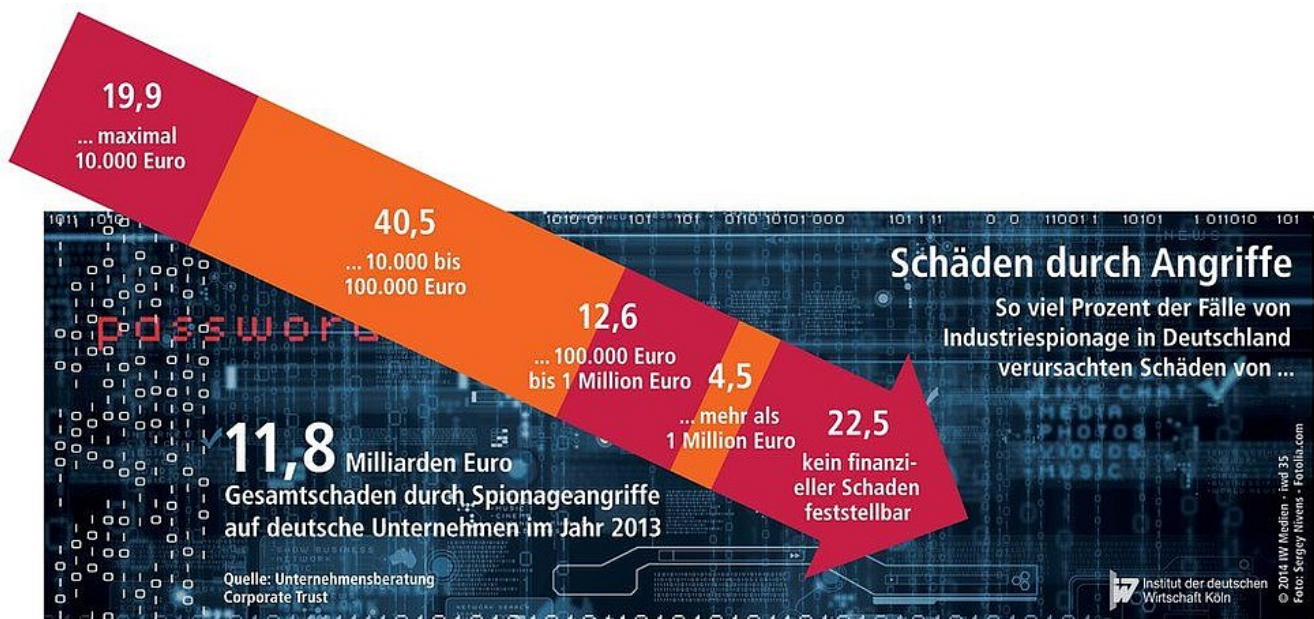
Industriespionage | 28.08.2014 | Lesezeit 3 Min.

Jedes zweite Unternehmen wird angezapft

Durch Datenklau und allzu plauderfreudige Mitarbeiter entstehen den deutschen Unternehmen jedes Jahr Schäden von mindestens 12 Milliarden Euro. Um sie vor Cyberattacken besser zu schützen, will das Bundesinnenministerium nun ein IT-Sicherheitsgesetz verabschieden.

Wenn E-Mails den klassischen Geschäftsbrief ersetzen, Firmendaten nur noch elektronisch gespeichert werden und sogar Maschinen über das Internet gewartet werden können, dann nennt man das die Digitalisierung der Wirtschaft. Diese an sich modernen Methoden machen die Firmen allerdings auch angreifbar: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) geht davon aus, dass 95 Prozent der E-Mails und ein Großteil der mobilen Kommunikation nicht verschlüsselt sind – also vergleichsweise leicht mitgelesen oder abgehört werden können. Kein Wunder also, dass angesichts dieser „elementaren Lücke“, wie BSI-Präsident Michael Hange die digitale Datensorglosigkeit betitelt, kräftig spioniert wird:

Mehr als jedes zweite Unternehmen in Deutschland wurde in den vergangenen beiden Jahren angezapft: Knapp 27 Prozent der Betriebe beklagten einen konkreten Spionagefall, rund 27 Prozent registrierten einen Verdachtsfall.



Rund drei Viertel der attackierten Unternehmen erlitten aufgrund des Informationslecks finanzielle Einbußen – im Jahr 2013 summierten sich die Schäden durch Spionagefälle laut Corporate Trust auf fast 12 Milliarden Euro (Grafik). Das Bundesinnenministerium geht sogar von einem noch weit höheren Finanz-Fiasko aus: Demnach beträgt der jährliche Schaden, den Unternehmen in Deutschland durch Industriespionage und Hackerattacken erleiden, 50 Milliarden Euro.

Besonders betroffen ist der Mittelstand. Schätzungsweise jeder zweite Betrieb wurde in den vergangenen Jahren ein Opfer von Wirtschaftskriminellen. Die verursachten Schäden werden auf jährlich mehr als 20 Milliarden Euro geschätzt. Oft kommt es bei Industriespionage nicht nur zu einem Datenklau, der das laufende Geschäft oder die Entwicklung eines neuen Produkts beeinträchtigt, sondern auch zu materiellen Schäden, weil zum Beispiel IT- und Kommunikationsgeräte in Mitleidenschaft gezogen werden.

In der Regel sind es Computerspezialisten, die den Betrieben zusetzen (Grafik):

Industriespionage in Deutschland

Angaben in Prozent für den Zeitraum April 2012 bis April 2014

Wer ist betroffen?



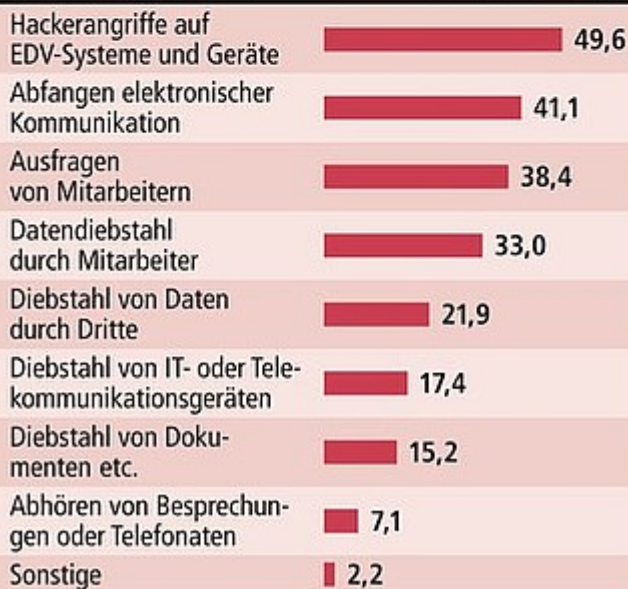
Wo sitzen die Angreifer?

Mehrfachnennungen



Wie wird spioniert?

Mehrfachnennungen



Befragung von 6.767 Unternehmen in Deutschland aus allen Wirtschaftsbereichen im April 2014
Quelle: Unternehmensberatung Corporate Trust

 Institut der deutschen
Wirtschaft Köln

© 2014 IW Medien - iwd 35

Etwa die Hälfte der Firmen machte Erfahrungen mit Hackern, die in EDV-Systeme, Server, Laptops, Smartphones und Tablets der Unternehmen eindringen.

Jenseits des Abfischens von Daten gibt es allerdings auch noch ganz klassische Methoden, um an Firmeninformationen zu kommen. Schon auf Platz drei der häufigsten Spionagemethoden steht das Ausfragen von Mitarbeitern, denen beispielsweise auf einer Messe oder gar im privaten Umfeld so manche Betriebsinterna entlockt werden. Stattdliche 38 Prozent der befragten Unternehmen in Deutschland mussten feststellen, dass diese Form der Industriespionage in den vergangenen beiden Jahren bei ihnen vorgekommen ist.

Insbesondere bei Cyberattacken ist es nicht leicht, den Angriff zurückzuverfolgen – zumal weltweit spioniert wird. Fest steht jedoch, dass ein Großteil der Spähversuche auf deutsche Unternehmen in Asien (knapp 39 Prozent) oder Nordamerika (knapp 22 Prozent) ihren Ursprung haben. Bekannt ist beispielsweise der Fall der Bonner Solarworld AG, deren amerikanische Tochterfirma von mutmaßlichen Hackern im Dienst der chinesischen Volksbefreiungsarmee ausspioniert worden sein soll. Deshalb und wegen ähnlicher Fälle haben die Vereinigten Staaten nun – erstmals in der Geschichte – eine Klage eingereicht, in der sie strafrechtlich gegen eine Cyberattacke durch einen anderen Staat vorgehen.

Tatsächlich ist Wirtschaftsspionage im Dienst der nationalen Sache gar nicht so selten:

Die Unternehmensberatung Corporate Trust geht davon aus, dass etwa 6 Prozent der Angriffe auf deutsche Unternehmen von staatlichen Geheimdiensten durchgeführt werden.

Um den Schutz der Unternehmen zu verbessern, hat das Bundesinnenministerium vergangene Woche einen Gesetzentwurf vorgelegt, der den Betrieben Mindeststandards für ihre IT-Sicherheit vorschreiben will. Zusätzlich sollen große Unternehmen, Versorgungsbetriebe und Banken künftig dazu verpflichtet werden, Angriffe und Spionageversuche dem Bundesamt für Sicherheit in der Informationstechnik zu melden. Bislang schlagen nämlich nur sehr wenige betroffene Unternehmen Alarm: Das Bundesamt für Verfassungsschutz geht davon aus, dass sich derzeit nur jeder vierte ausspionierte Betrieb in Deutschland an die Behörden wendet.

Kernaussagen in Kürze:

- Durch Datenklau und allzu plauderfreudige Mitarbeiter entstehen den deutschen Unternehmen jedes Jahr Schäden von mindestens 12 Milliarden Euro.
- Mehr als jedes zweite Unternehmen in Deutschland wurde in den vergangenen beiden Jahren angezapft: Knapp 27 Prozent der Betriebe beklagten einen

konkreten Spionagefall, rund 27 Prozent registrierten einen Verdachtsfall.

- Die Unternehmensberatung Corporate Trust geht davon aus, dass etwa 6 Prozent der Angriffe auf deutsche Unternehmen von staatlichen Geheimdiensten durchgeführt werden.