News

Sicherheitstipp: Wirtschaftspionage per USB-Stick (www.it-sicherheit.de):

... manchmal gefährlicher als man denkt

Unternehmen und Akteure aus der Wissenschaft sind zunehmend Opfer von Wirtschafts- und Konkurrenzspionage. Dabei versuchen Kriminelle auf vielfältige und kreative Art, Know-how, Innovationen und sensible Daten abzugreifen. Um sich wirksam gegen solche Versuche zu schützen, ist ein sorgsamer Umgang mit Firmendaten und IT-Systemen zwingend erforderlich.

Wirtschaftsspionage vs. Industriespionage

Experten unterscheiden zwischen staatlich gelenkter Wirtschaftsspionage und Industriespionage durch konkurrierende Unternehmen. Staatliche Geheimdienste sind zunehmend aktiv, wenn es darum geht neue Entwicklungen aller Art aus dem Ausland auszuspähen. Ein besonderes Interesse fällt dabei den Querschnitttechnologien zu, sie sind demnach besonders betroffen. Allein in Deutschland liegt der jährliche Schaden von Wirtschaftsspionage zwischen 20 und 40 Milliarden Euro.

Branchenführende Unternehmen sind ebenfalls besonders gefährdet, da gerade sie sich durch herausragende Neuentwicklungen, Technologien und Know-how ausweisen. Eine Neuentwicklung ist nicht nur zeit- sondern auch kostenintensiv und wird durch eine Ausspionierung schnell zum unternehmerischen Ärgernis. Beliebte Ziele von Wirtschaftsspionen sind Unternehmens- oder Institutseigene Websites, Informationen die Marketingzwecken dienen, wissenschaftliche Arbeiten (z.B. Examensarbeiten), Produktbeschreibungen und Inhalte von Öffentlichkeitsarbeit. Besonders beliebt sind auch Messen, wie beispielsweise die CeBIT in Hannover. Hier sind Spione gezielt am Werk und greifen offen Informationen ab, die nicht selten in Joint Ventures münden.

Vom einfachen USB-Stick zum Spionageinstrument

Wer kennt es nicht? Sie besuchen eine Messe und bekommen auf den Unternehmensständen nach Abschluss eines Gesprächs kleine Werbe-geschenke angeboten. Darunter ist auch ein USB-Speicherstick mit einer Kapazität von einigen Gigabytes. Natürlich ist gerade ein USB-Speicherstick ein hochwertiges „Give-away", trotzdem ist bei solchen Geschenken Vorsicht geboten! USB-Speichermedien dieser Art sind nur sekundär Werbegeschenke, primär verfolgen die Absender das Ausspionieren der Adressaten. In einigen Fällen ist ein solches Speichermedium mit einem Trojaner infiziert, der den Datenverkehr ausspioniert und diesen kontinuierlich an den Verursacher leitet.

Materialen dieser Art gehen gezielt an Firmen bzw. deren Vertreter, die für die Spione interessant sind. Die Beschenkten nutzen den Stick nach Erhalt oft bedenkenlos in Verbindung mit ihren Firmen-PCs zum Speichern und Übertragen von Dateien.

Was können Firmen dagegen tun?

Mitarbeiter sollten neue USB-Sticks generell vor der ersten Datenspeicherung mit einem aktuellen Virenprogramm prüfen oder formatieren. Ein entdeckter Trojaner wird so entfernt und stellt keine Gefahr mehr dar.

Generell sollten Unternehmen dazu Folgendes beachten:

1. Informationsschutz als Bestandteil der Firmenstrategie festschreiben.
2. Sicherheitskonzept ganzheitlich anlegen, regelmäßig analysieren und gegebenenfalls aktualisieren.
3. Einhaltung der Sicherheitsvorkehrungen kontrollieren, Sicherheitsverstöße sanktionieren.
4. Schutzmaßnahmen auf den Kernbestand zukunftssichernder Informationen konzentrieren.
5. Frühwarnsystem zur Erkennung von Know-how-Verlust installieren. Auffälligkeiten und konkrete Hinweise konsequent verfolgen.

Ob ein Unternehmen leicht ins Visier von Wirtschaftsspionen gerät, können Firmen in nur wenigen Minuten mit einem vom NRW-Innenministerium entwickelten Internet-Tool selber schnell teste: "Wirtschaftsspionage - Ist mein Unternehmen gefährdet?"

Der Draht zum richtigen Lösungsanbieter in Sachen IT-Sicherheit
Nutzen Sie die umfangreichen Suchmöglichkeiten vom *Branchenbuch IT-Sicherheit*, um in Ihrer Nähe geeignete Lösungsanbieter der IT-Sicherheit zu finden.

Autor: Kathrin Beckert

Institut für Internet-Sicherheit - if(is)
Fachhochschule Gelsenkirchen
Neidenburger Straße 43
D-45877 Gelsenkirchen