

Zumindest unabsichtliche Datenweitergabe kann verhindert werden



Spezialwerkzeuge stopfen Informationslecks in Firmen

19. Juni 2007

Wirtschaftsspionage ist real, mahnen Experten. Oft wird dabei die Schwachstelle Mensch attackiert. Beispielsweise nutzen gezielten Trojaner-Attacken verstärkt die Tricks des Social Engineering. Aber Firmen sollten auch die absichtliche oder unabsichtliche Weitergabe sensibler Informationen unterbinden.

„Innovatives Know-how weckt Begehrlichkeiten, das ist ganz normal.“ Für Wilfried Karden vom nordrhein-westfälischen Verfassungsschutz ist die Gefahr der Wirtschaftsspionage Alltag. Dabei gehe die Gefahr auch von ausländische Regierungen aus, die stets das Wohl der eigenen Wirtschaft im Auge haben.

„Der CIA-Chef hat zugegeben: Wir spionieren euch aus“, so Karden. Und in Russland gebe es sogar ein Gesetz, das Wirtschaftsspionage erlaubt, um die eigene Industrie voranzubringen. Jeder Provider müsse daher Schnittstellen für den Nachrichtendienst einrichten. Karden: „Das muss man wissen, wenn man mit russischen Partnern Geschäfte macht oder dort Filialen hat.“

Denn ein Know-how-Abfluss kommt teuer. Zwar steht laut Karden Industriespionage nur für ein Prozent aller Wirtschaftsdelikte, Sorge aber für 30 Prozent der Kosten. „Wirtschaftsspionage ist zwar selten, aber wenn sie stattfindet, verursacht sie immense Kosten“.

Auch in der Wirtschaft wächst daher die Sorge, wie eine Umfrage unter 208 Experten durch die Arbeitsgemeinschaft für Sicherheit der Wirtschaft (ASW) zeigt. Allerdings findet sich nur bei 37 Prozent der befragten Firmen ein Konzept zum Schutz des eigenen Know-hows. Und dies obwohl zwei Drittel der Sicherheitsprofis sagen, in ihren Betrieb falle schützenswertes Know-how an und ein Viertel schon von Spionagefällen in der eigenen Branche gehört hat.

Für Karden geht die größte Gefahr gar nicht unbedingt von Hightech-Attacken via Richtmikrofonen aus, sondern sie liegt schlicht in der Schwachstelle Mensch. Auch die staatliche Schweizer Melde- und Analysestelle Informationssicherung warnt: „Social-Engineering-Angriffe stellen die am weitesten verbreitete Angriffsart gegen Unternehmen und Privatanwender dar.“

Im Firmenbereich wird Social Engineering vor allem zur Wirtschaftsspionage eingesetzt, etwa um gezielt Malware auf Firmenrechner zu schleusen (Spear-Phishing). Im Visier der Angreifer stehen dabei meistens potenzielle Wissensträger. Laut Security-Dienstleister Verisign mehren sich zudem gezielte Trojaner-Mails gegen die Chefs großer global operierender Unternehmen.

Doch Manager und Mitarbeiter stellen nicht nur ein Einfallstor für Spionage-Trojaner dar. Sie können auch selbst – absichtlich oder unabsichtlich – Informationen in die falschen Hände spielen. So räumen bei einer McAfee-Umfrage unter 1400 IT-Experten immerhin 60 Prozent ein, dass es 2006 im eigenen Haus mindestens einen Verstoß gegen Datenschutzrichtlinien gegeben habe. Etwa zwei Drittel der Befragten halten eigene Mitarbeiter für diese Informationslecks verantwortlich. Etwa

cirosec GmbH
Edisonstraße 21
74076 Heilbronn
Tel: 07131 / 59455-0
Fax: 07131 / 59455-99
info@cirosec.de
www.cirosec.de

ein Viertel führt die Informationsverluste sogar auf vorsätzliche Taten zurück.

Oft werden Schäden aber eben auch bloß aus Unaufmerksamkeit verursacht. „Viele deutsche Firmen arbeiten eng mit Partnerunternehmen aus dem nahen und fernen Osten zusammen und tauschen ganz offiziell vertrauliche und wertvolle Informationen wie Konstruktionsdaten und Produktspezifikationen aus“, sagt Frank Böning, Sales Director beim Informationsschützer Workshare. „Besonders in der E-Mail-Kommunikation kann es schnell passieren, dass ein vertrauliches Dokument beim falschen Empfänger landet.“

Doch die Sensibilität für die Problematik nimmt zu. So zeigt eine Forrester-Umfrage unter 30 europäischen Security-Verantwortlichen, dass die Abdichtung von Informationslecks derzeit weit oben auf der Prioritätenliste steht – noch vor Viren- oder Spamschutz (siehe obere Grafik).

Auch bei einer Umfrage von Infowatch gilt der Datendiebstahl inzwischen als größere IT-Bedrohung (78 Prozent) als Viren (49 Prozent) oder Hacker-Attacken (41). Als gefährlichste Kanäle für den Datenverlust sehen die 410 von Infowatch-befragten europäischen IT-Profis vor allem E-Mail und tragbare Speichermedien.

Trotzdem setzen erst 16 Prozent spezielle Anti-Datenleck-Produkte ein. Als Haupthindernisse nennen die Firmen neben zu wenig Fachleuten und engen Budgets vor allem fehlende Industriestandards. Denn der Markt des Datenleck-Stopfens ist noch jung und recht heterogen – und sperrig bezeichnet. IDC nennt ihn Information Leakage Detection and Prevention (ILD&P), Forrester spricht von Information Leak Prevention (ILP), während Gartner das Segment unter Content Monitoring and Filtering and Data Loss Prevention (CMF/DLP) führt.

Websense sowie Vontu und Vericept stuft Gartner dabei als marktführend ein, Reconnex, Tablus und Code Green Networks gelten als Visionäre. Und am Markt tummeln sich noch weitere Anbieter. Neben Infowatch (eine Tochter der russischen Kaspersky-Virenjäger) und Workshare sind dies etwa Oakley Networks, Orchestria, Provilla, Verdasys und nicht zuletzt Security-Riese McAfee, der sich durch die Übernahme des Spezialisten Onigma in die Data Loss Prevention eingekauft hat. Auch Verschlüsselungshersteller wie RSA oder Utimaco bezeichnen die Abdichtung von Informationslecks als „interessanten Markt“.

Generell arbeiten solche Produkte so, dass sie auf PCs und/oder Mail- und Internet-Gateways sitzen und dort darauf achten, dass als vertraulich angesehene Daten nicht den Betrieb verlassen. Cirosec-Geschäftsführer Stefan Strobel hält diese Tools für eine „gute Geschichte“ – allein schon, um eine unabsichtliche Datenweitergabe zu unterbinden.

Professor Stefan Wolf von der Fachhochschule Lippe und Höxter dagegen kann die Tools trotzdem nicht empfehlen: „Sie nutzen vielleicht gegen unabsichtliche Datenweitergabe. Aber die User lernen schnell, wie sie – vielleicht zunächst im Sinne der Firma – umgangen werden können.“

Computerzeitung.de 19.06.2007