IT-Sicherheit, die von innen kommt

Unternehmen sind nur wenig sensibilisiert, was die Gefahren durch Innentäter betrifft. Doch die Bedrohung ist real, und Sicherheitsmaßnahmen sind keine Zauberei.

Angesichts zunehmender Hacker-Angriffe auf Online-Plattformen und Datenschutz-Probleme bei sozialen Netzen ist ein sogenannter Angriffsvektor aus dem Blick der Öffentlichkeit geraten: der Innentäter. Dabei ist die Gefahr weiter virulent: So berichtete das Computer Emergency Response Team (CERT), dass im Jahr 2010 über 40 % der überwachten Organisationen Vorfälle mit Innentätern verzeichneten. Und in der „e-Crime-Studie 2010“ des Beratungshauses KPMG heißt es: „Insbesondere bei Datendiebstahl oder der Verletzung von Geschäfts- und Betriebsgeheimnissen kommen die Täter aus dem eigenen Haus.“

Der zurzeit bekannteste Innentäter ist Bradley Manning, dem vorgeworfen wird, die Enthüllungsplattform Wikileaks mit brisanten Informationen versorgt zu haben. In der Regel schlagen interne Angriffe aber keine derart hohen Wellen – das Thema wird nicht öffentlich diskutiert. Häufig gehen die Attacken von frustrierten, genervten oder böswilligen Mitarbeitern aus, die es dem Unternehmen auf ihre Weise heimzahlen wollen.

Innentäter sind überwiegend männlich – und unachtsam

Zudem finden sich Innentäter, die zum eigenen wirtschaftlichen Nutzen Informationen ausspionieren oder die schlicht unvorsichtig handeln. Allerdings: „Statistiken können auch beim Thema Innentäter nur das Hellfeld erfassen und daher beim Aufbau effektiver Schutzmechanismen kaum eine große Hilfe bieten“, sagt Wilfried Karden, Projektverantwortlicher für Spionageabwehr im Innenministerium von Nordrhein-Westfalen. Immerhin verraten die Zahlen, dass der Innentäter in der Regel zwischen 30 und 50 Jahre alt, zumeist männlich und mehr als fünf Jahre im Unternehmen tätig ist. Dies erfasst jedoch gleichzeitig auch die wertvollsten Mitarbeiter und nicht nur die Innentäter – „bei der Verbesserung einer Sicherheitskonzeption hilft dieses Wissen also nicht weiter“, sagt Karden. Überhaupt liege die größere Bedrohung nach seiner

Wahrnehmung nicht im böswilligen, sondern im unachtsamen Täter, der Informationen leichtfertig nach außen gelangen lässt: „Täter im strafrechtlichen Sinne sind sehr selten."

Ob böse oder unvorsichtig – traditionelle Sicherungsmaßnahmen wie Firewalls und Antivirenprogramme büßen angesichts der Bedrohung durch Innentäter nicht ihre Berechtigung ein. Jedoch sind sie als isolierte Systeme kaum in der Lage, die Datensicherheit zu gewährleisten. Hierzu ist eine Mischung von Technologien, Prozessen und Verhaltensregeln nötig. Zwar legten Unternehmen den Fokus zunehmend auf das Thema IT-Sicherheit, berichtet Michael Seele aus der Praxis: „Allerdings verstehen viele Unternehmen IT-Security noch nicht als Prozess", sagt der Geschäftsführer der IT-Sicherheitsfirma Protea Networks aus Unterhaching. Nur wer sich stetig informiere und die ergriffenen Maßnahmen regelmäßig überprüfe und anpasse, sei dem dynamischen Bedrohungswandel gewachsen.

Auch für den Verfassungsschützer Karden müssen es nicht ausnahmslos ausgefeilte technische Lösungen sein, um Daten wirksam zu schützen. Der Experte verweist zum Einstieg auf die Fünfprozentregel: „Unternehmen haben 5 % werthaltiges Know-how für künftige Projekte, das kein anderer bekommen sollte." Diese Informationen müssen bestimmt, ein Sicherheitskonzept entwickelt und die Mitarbeiter sensibilisiert werden – „damit sie nicht im Sportverein darüber reden". Alle Rechner, auf denen diese Informationen verarbeitet würden, müssten verschlüsselt sein – auch heute noch werde dies zu wenig genutzt. Kardens Devise für den Umgang mit den geschäftskritischen Daten ist simpel und effektiv: „Gesichert aufbewahren, gesichert kommunizieren."

Alle unternehmenskritischen Informationen auf Rechnern verschlüsseln

Grundsätzlich sei die Verschlüsselung der schnellste Weg, um ein deutlich höheres Sicherheitsniveau zu erreichen, pflichtet Protea-Networks-Geschäftsführer Seele bei. Ob die Sensibilisierung der Mitarbeiter gelungen ist, zeigt ein einfaches und effektives Angriffsszenario, das insbesondere im Rahmen von Audits verwendet wird: „Wir verteilen an verschiedenen stark frequentierten Orten eines Unternehmens präparierte USB-Sticks, die sich mit den Daten des Systems an einem zentralen Steuerrechner zurückmelden, sobald sie an einem Rechner angeschlossen werden.“ Dieser Sicherheitstest verlaufe in der Regel „immer sehr erfolgreich“. Aus Sicht eines Angreifers, versteht sich.