Weihnachtsgeschenk oder Spionageangriff?

Werbegeschenke als potenzielle Gefahrenquelle für sensible Unternehmensdaten / Wirtschaftsspionage bedroht nicht nur innovative Konzerne – längst ist sie auch bei mittelständischen Unternehmen ein allgegenwärtiges Phänomen. Mehr als jedes zweite deutsche Unternehmen wurde bereits Opfer von Datendieben. Der wirtschaftliche Schaden beläuft sich laut einer aktuellen Bitkom-Studie auf circa 51 Millionen Euro jährlich.

Dabei kann von geheimen Konstruktionsplänen bis zur täglichen Geschäftskommunikation alles ins Visier der Spione geraten. Hochsaison haben Spione dabei vor allem in der Vorweihnachtszeit, weiß Sicherheitsexperte Marcus Lentz von der bundesweit agierenden Wirtschaftsdetektei Lentz: „Die bevorstehende Adventszeit öffnet potenziellen Angreifern mit kleinen Aufmerksamkeiten in vielen Betrieben Tür und Tor.“

Alle Jahre wieder

Jedes Jahr tauschen Unternehmen in der Weihnachtszeit Werbegeschenke aus, um sich für die erfolgreichen Geschäftsbeziehungen im vergangenen Jahr zu bedanken. Immer häufiger versteckt sich in der netten Aufmerksamkeit aber ein hinterhältiger Spionageangriff. Der Einfallsreichtum der Spione ist dabei so unbegrenzt wie das Angebot an Werbegeschenken. Vom teuren Kugelschreiber, der mittels Wanze alle Aktivitäten des Chefs überwacht, bis zur Designer-Kaffeekanne im Konferenzraum, die als gut getarnter Lauschangriff wichtige Geschäftsentscheidungen an die Konkurrenz übermittelt – dem Einsatz der heutigen leistungsstarken Überwachungstechnik im Miniaturformat sind höchstens noch kreative Grenzen gesetzt. „Zu den beliebtesten spionierenden Werbegeschenken gehören weiterhin digitale Geräte wie USB-Sticks oder MP3-Player“, erläutert Marcus Lentz, Geschäftsführer der Wirtschaftsdetektei Lentz. Nachdem diese Geräte an einen Computer angeschlossen wurden, installiert sich unbemerkt eine Schadsoftware, die den PC oder – via Netzwerk – sogar ein ganzes Unternehmen nach interessanten Daten durchforstet und diese per Internetverbindung den Angreifern frei Haus liefert.

Bedrohliche Technik

Das Abhören von Telefonanlagen, der Einsatz von winzigen Wanzen oder Minikameras in beliebigen Alltagsgegenständen oder die „feindliche Übernahme“ eines Smartphones durch die Installation von sogenannten Spy Apps – die technischen Möglichkeiten sind vielfältig, um sich unbefugten Zugriff auf firmeninterne Daten zu verschaffen. „Dabei sinken auch die technischen, finanziellen und letztlich auch moralischen Hürden für die Anwendung immer weiter“, warnt Lentz. Längst sind es nicht mehr nur professionelle Spione und Hacker, die Spähangriffe starten. Der Konkurrenzdruck führt dazu, dass auch kleine und mittelständische Unternehmen sich immer häufiger gegenseitig bespitzeln. Die überall frei verfügbaren Instrumente – sei es Hardware oder Software – werden zudem immer leistungsfähiger, günstiger und lassen sich meist schon mit einfachen Anwenderkenntnissen bedienen: „Die technische Bespitzelung funktioniert heute oft schon nach dem ‚Plug-and-Play‘-Ansatz“, so der Wirtschaftsdetektiv. Der wirtschaftliche Schaden durch diese Entwicklung ist immens. „Für kleine und mittelständische Betriebe kann sich ein Datenleck rasch zur existenzbedrohlichen Krise ausweiten“, weiß Marcus Lentz. Eine Sicherheitslücke, durch die wichtige Unternehmensinformationen wie Konstruktionspläne, Kalkulationen, Kundendaten oder Angebote an die Konkurrenz abfließen, kann zu massiven Auftragseinbrüchen und – bei Bekanntwerden der Betriebsspionage – zu einem nachhaltigen Vertrauensverlust führen.

Risikofaktor Mensch

Sicherheitsexperten wissen: Die größte Gefahr für die Datensicherheit ist der Faktor Mensch. Oft ist er die schwächste Stelle im System. „Ein Geschenk wird eigentlich immer positiv angenommen, kaum jemand vermutet hinter dieser netten Geste eine böse Absicht. Und so werden Mitarbeiter zu ahnungslosen Mithelfern, wenn sie den praktischen USB-Stick am Arbeitsplatz benutzen“, erklärt Sicherheitsexperte Marcus Lentz. „Diese Unwissenheit und Nachlässigkeit sind häufig die größten Gefahren für sensible Unternehmensdaten.“ Selbst viele Verantwortliche unterschätzen noch immer die Bedrohung durch digitale Wirtschaftsspionage. „Aufklärung ist daher die erste und wichtigste Maßnahme zum Datenschutz“, meint Lentz und rät Unternehmern wie Mitarbeitern deshalb, auch in der beschaulichen Weihnachtszeit ein gesundes Misstrauen an den Tag zu legen. „Am sichersten ist es, Weihnachtsgeschenke nicht im Betrieb zu verwenden!“, so Lentz.

Grundlagen der Spionageabwehr

Wirksamer Schutz gegen Datenklau und seine oft existenzbedrohlichen Folgen muss grundsätzlich vorbeugend erfolgen. Dazu sollten in jeder Firma einige grundlegende Maßnahmen ergriffen werden. „Der Einsatz von Firewalls und Antivirenprogrammen zum Schutz der IT-Systeme sollte inzwischen selbstverständlich sein“, meint Sicherheitsexperte Marcus Lentz. Darüber hinaus sollten in jedem Betrieb verbindliche Regeln zum Umgang mit vertraulichen Geschäftsdaten gelten. Dazu gehören zum Beispiel klar geregelte Zugriffsrechte und feste Richtlinien für den Umgang mit externen Datenträgern wie USB-Sticks. „Wenn trotzdem der Verdacht besteht, dass ein Unternehmen Opfer von Betriebsspionage ist, müssen die Verantwortlichen schnellstmöglich handeln und sich professionelle Hilfe zur Spionageabwehr suchen“, rät der erfahrene Wirtschaftsermittler. Diskretion ist dabei für Wirtschaftsdetektive das oberste Gebot, da vielen Unternehmen zum Datenverlust auch ein Imageschaden droht. Die Sicherheitsexperten können mit technischem Know-how und professionellen Ermittlungsmethoden meist nicht nur rasch den Spähangriff abwenden, sondern auch die Angreifer identifizieren.

Weitere Informationen zum Thema Lauschangriff finden Sie unter http://www.lentz-detektei.de/wirtschaft/abhoeraktionen.

Pressekontakt:

Marcus R. Lentz
E-Mail: medienstelle@lentz.de

Unternehmen

Detektei Lentz & Co. GmbH
Hanauer Landstraße 126-128
60314 Frankfurt am Main

Internet: www.lentz-detektei.de

Pressekontakt:

Daniela Werner
Telefon: 089/998 461-13
Fax: 089/998 461-20
E-Mail: detektei-lentz@hartzkom.de

Unternehmen

Hartzkom GmbH
Anglerstraße 11
80339 München

Internet: www.hartzkom.de