KMU im Fokus - Ein praxisorientierter Sicherheitsleitfaden zur Spionageabwehr

David Spuler

Eidg. dipl. Informatiker & Kantonspolizist
MAS Economic Crime Investigation Hochschule Luzern (MAS ECI 12)
CISA / CISM

David Spuler arbeitet seit September 2017 als Spezialist für Informationssicherheit bei der RONAL GROUP in Härkingen. Er verfügt über einen fundierten Informatik-Hintergrund mit Berufslehre bei der IBM Schweiz AG in Zürich und diversen Weiterbildungen im IT- und Informationssicherheitsbereich. 2006 absolvierte er die Polizeischule der Kantonspolizei Aargau und arbeitete im Anschluss im Innen- und Aussendienst mit Sonderfunktionen in Baden und Schafisheim. Im August 2009 übernahm er die stellvertretende Geschäftsführung der Wirtschaftsdetektei Business Control (Schweiz) AG in Zürich und leitete unter anderem Ermittlungseinsätze in Amerika, Syrien sowie vielen Teilen Europas. Mit dem MAS ECI Studium übernahm er eine Teilzeitstelle als Sicherheitsingenieur für Sonderprojekte bei der Securitas AG in Olten und übernahm später die Leitung des Kompetenzzentrums Schweizerisches Büro für integrale Sicherheit (SBIS), wo er 2015 den Fachbereich Informationssicherheit aufbaute.

Im Zeitalter der Interkonnektivität und dem daraus resultierenden Verlust des Perimeter-Schutzes für digitale Daten sind die Anforderungen an Unternehmen derart vielschichtig geworden, dass die Sicherheit von Daten speziell bei kleinen und mittleren Unternehmen oftmals nur ungenügend gewährleistet werden kann. Dabei hängt der Schutzbedarf in Bezug auf Industriespionage nicht primär von der Firmengrösse, sondern vielmehr von der wirtschaftlichen Attraktivität ab, welche sich aus der Betriebsart, der Produktepalette und dem Durchsatz, der technische Komplexität sowie der möglichen Gewinnspanne ergibt. Speziell technisch hochstehende Ingenieur- und Fertigungsbetriebe mit intensiven Forschungs- und Entwicklungsaufwänden gelten als stark gefährdet, wobei jedoch auch ein einfacher Handelsbetrieb aufgrund einer attraktiven Kundendatenbank zum Ziel eines Spionageangriffs werden kann. Auch Kleinstbetriebe können durch einzigartige Ideen, Produkte und Dienstleistungen, gefragtes „Know-How“ oder andere wertvolle betriebliche Geheimnisse schnell Geschädigte eines illegalen Datenabflusses werden. Bei neu gegründeten Betrieben und Kleinunternehmen fehlen zudem oft finanziellen Ressourcen für Aufträge an externe Spezialisten, um den benötigten Schutzgrad zu erreichen. Auch strategisch liegt der Fokus eher auf Wachstum und Wirtschaftlichkeit, anstatt auf der Rekrutierung von Sicherheits-Fachleuten. Eine aufwendige Zertifizierung im Sinne des Risikomanagements (ISO 31000-Reihe) oder IT-Sicherheit (ISO 27000-Reihe) wird zudem meist erst auf Verlangen der Kunden in Betracht gezogen.

Ein Datenverlust oder Diebstahl von Kundendaten, vertraulichen Produkteinformationen oder teuren Entwicklungsunterlagen kann ein kleines oder mittleres Unternehmen existenziell schädigen, sei es durch die Flutung des Marktes mit identischen, billigeren Produkten oder durch Imageschäden, wenn bekannt wird, dass Kundendaten oder andere vertrauliche Informationen an die Öffentlichkeit gelangen. Unternehmen müssen sich in der heutigen Zeit nicht mehr die Frage stellen, ob und wann sie Opfer einer Cyberattacke werden, sondern ob bereits erfolgte Angriffe erkannt und abgewehrt werden konnten. Dabei ist die gezielte Konkurrenzspionage nur für einen Bruchteil der Angriffe verantwortlich. Neben dem technischen Aspekt nimmt die Thematik «Social Engineering» immer eine bedeutendere Rolle ein. Mittels geschickten Täuschungen und fundierten Legenden werden vertrauliche Informationen gestohlen, Zutritte zu geschützten Bereichen erschlichen sowie Personen unterschiedlichster Funktionen gezielt beeinflusst. Statistisch gesehen ist die Schwachstelle Mensch mit Abstand die grösste Sicherheitslücke in jedem Unternehmen. Neben der unbewussten Preisgabe von vertraulichen Informationen mittels Social Engineering können auch unzufriedene Mitarbeiter, eingeschleuste Praktikanten oder ehemalige Angestellte mit bestehendem Datenzugriff, vertrauliche Informationen gegen Bezahlung preisgeben. Dies zeigt die Notwendigkeit von organisatorischen Prozessen zur Wahrung der Unternehmenssicherheit, welche unter anderem die Einstellung, die periodische Überprüfung wie auch die Entlassung von Personal behandeln. In der Praxis werden Social Engineering-Techniken oft auch nur zu Vorbereitungszwecken verwendet, um im Anschluss einen IT-Angriff zu starten oder gezielt technische Abhörgeräte einzusetzen. Nur wer die Spionagemethoden kennt, hat eine Chance einen Angriff zu erkennen und entsprechend zu reagieren. In diesem Sinne werden im Hauptteil der Arbeit die gängigsten Methoden bei Spionageangriffen aufgezeigt und mit organisatorischen, personellen, baulichen und technischen Massnahmen zur Abwehr dieser Gefahren verknüpft. Im Falle eines erfolgten Angriffes fällt es oftmals schwer, den entstandenen Schaden zu eruieren, geschweige denn zu beziffern. Das Einschalten der Strafverfolgungsbehörden deckt nur bedingt die unternehmerischen Ziele ab und birgt Risiken. Das letzte Kapitel behandelt folglich die Vor- und Nachteile entsprechender Aufklärungsmethoden. Diese Arbeit soll Unternehmen vor Schäden von zukünftigen Spionageangriffen schützen sowie notwendige Massnahmen zur effizienten Steigerung des individuellen Sicherheitslevels aufzeigen.

Hochschule Luzern - Wirtschaft
Institut für Finanzdienstleistungen Zug IFZ
Grafenauweg 10
Postfach 7344
CH-6302 Zug
+41 41 757 67 67
ifz@hslu.ch