Wirtschaftsspionage 2.0

Spionage im Wandel der Zeit

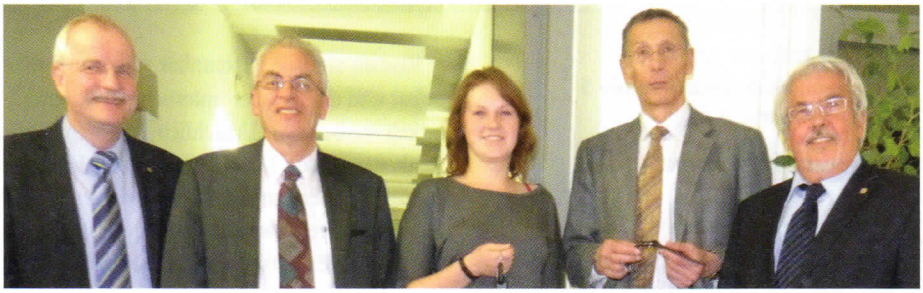

Foto: privat

Hr. Proschko, Leiter Spionageabwehr LfV (2. v. re.) mit den Leitern der BG Erlangen und des AK EKV.

Viele sind der Meinung, dass mit dem Fall des Eisernen Vorhangs die Bedrohung für die deutsche Wirtschaft durch Spionage und andere Gefährdungen abgenommen hat. Doch das Gegenteil ist der Fall. Die Anzahl der Spionageangriffe hat sogar zugenommen, was in erster Linie durch die offenen Grenzen, die zunehmende Vernetzung der Unternehmen, die modernen Kommunikationsdienste und Unkenntnis vieler Geheimnisträger begünstigt wird. Herr Proschko, Leiter der Abteilung Spionageabwehr im Bayerischen Landesamt für Verfassungsschutz LfV, hatte am 14. März der VDI-Bezirksgruppe Erlangen und dem VDI-Arbeitskreis Entwicklung-Konstruktion-Vertrieb einen kleinen Einblick in die Bedrohung und in geeignete Abwehrmaßnahmen gegeben.

Ziele der Wirtschaftsspionage

Im Fokus des ausspähenden Landes oder Unternehmens sind meist Unternehmensstrategien und F&E-Ergebnisse zukunftssichernder Hochtechnologien. Mittels Angriffe auf Computernetze und durch zwischenmenschliche Beeinflussung wird versucht, unberechtigt Informationen und Zugriff auf die technische Infrastruktur zu erhalten. Damit sollen Kosten und Zeit gespart werden mit dem Ziel, noch vor dem eigentlichen Innovator Produkte und Dienstleistungen auf den Markt zu bringen und dies zu niedrigen Kosten.

Methoden der Wirtschaftsspionage

Sind Sie schon einmal ausgespäht worden? Dies werden Sie höchst wahrscheinlich verneinen. Jedoch die Wahrscheinlichkeit, dass auch Sie bereits Ziel eines Ausspähers waren, ist sehr hoch. Denn Spionageangriffe werden zunächst nicht bemerkt und somit wiegen sich die betroffenen Personen in falscher Sicherheit. Laut Statistik sind mehr als 50% der Bevölkerung von Cyberattacken betroffen, täglich kommen ca. 100.000 neue Schadprogramme ins Netz und im Durchschnitt greifen drei Schadprogramme pro Sekunde Ihren Computer an. Eine stark eingeschränkte Performance Ihres PCs wird oft fälschlicherweise technischen Ursachen zugeschrieben. Selbst wenn nach einem Einbruch in einem Unternehmensgebäude nur ein einziger PC fehlt, wird dies vermeintlich der Beschaffungskriminalität zugeschrieben, jedoch leider nicht das LfV verständigt und um Aufklärung gebeten. Wenn Sie Ihre Kontaktdaten, den Namen Ihres Arbeitgebers und sogar Ihre Funktion in Ihrem Unternehmen in sozialen Netzwerken, wie XING oder Facebook, veröffentlicht haben, dann ersparen Sie feindlichen Unternehmen oder Ländern das aufwändige Ausspähen Ihrer Daten, sodass diese sehr schnell identifizieren können, ob Sie ein potenzieller Geheimnisträger sein könnten oder nicht. Wenn Sie unerwartet Kontaktanfragen über Internetportale von Unbekannten erhalten, dann sollte in Ihrem Kopf eine gelbe Ampel aufleuchten. Ganz zu schweigen von Einladungen zu Urlaubsreisen, die vom Einladenden bezahlt werden. Hier sollte die rote Ampel aufleuchten, denn Social-Engineering, wie es von Spionageorganisationen betrieben und genannt wird, ist in diesem Fall schon sehr weit vorangekommen.

Schutz vor Wirtschaftsspionage

Aufklärung und Information über die Methoden der Wirtschaftsspione ist zunächst der erste Schritt. Des Weiteren sollte ein professionelles Virenschutzprogramm auf Ihrem PC installiert sein und automatisch aktualisiert werden. Sie sollten sich auch bewusst sein, dass ein Smart-Phone kein Telefon, sondern ein PC ist, über was Sie Zugriff auf Ihr Unternehmensnetz haben. Somit sollte auch auf diesem ein Virenschutzprogramm installiert sein. Ein weiterer Klassiker ist das Passwort Ihres PC, das eventuell als Maßnahme gegen Vergessen auf Ihrem Bildschirm notiert oder aus den Namen Ihrer Frau und Ihrer Kinder abgeleitet worden ist. Durch Untersuchungen wurde festgestellt, dass selbst ein 8-stelliges Passwort mit Groß- und Kleinbuchstaben und Sonderzeichen im Durchschnitt bereits nach 37 Minuten durch einen Profi geknackt werden kann. Um ein sorgfältig ausgedachtes Passwort mit 10 Zeichen zu entschlüsseln, benötigt ein Profi hochgerechnet dagegen mehrere Jahre. Wenn Sie einen USB-Stick irgendwo finden sollten, dann gucken Sie bitte nicht nach, was darauf gespeichert ist, um festzustellen, wem der Stick gehören dürfte. Stattdessen werfen Sie den Stick besser in den nächsten Mülleimer, wenn sich der Eigentümer nicht finden lässt. Vorsicht ist auch zu walten mit technischen Dingen, wie Kfz-Schlüssel, die jemand scheinbar absichtslos auf den Tisch legt und mit denen man keine Autos öffnen kann, sondern die sich als Stimmenrecorder entpuppten, mit Uhren, mit denen man fotografieren kann, und mit gebrauchten Telefonen, in denen eine Handyplatine mit aktiver Sim-Karte installiert sein könnte. Wenn Sie meinen, Sie sollten Ihrem Chef von öffentlichen Plätzen aus, wie Wartehallen in Bahnhöfen oder Flughäfen, über den erfolgreichen Geschäftsabschluss mit einem wichtigen Kunden berichten, dann ist Ihnen zu raten, damit zu warten, bis Sie Ihrem Chef in seinem Büro gegenüber sitzen. Auch sollten Sie sich bewusst sein, dass in manchen Ländern ein Hotel-Safe alles andere als safe ist. Ansonsten ergeht es Ihnen vielleicht wie einem Ingenieur aus einem westlichen Land, der für seinen Besuch in China eine kleine Webcam in seinem Koffer installierte. Er war sehr überrascht, dass mehrere Personen seine persönlichen Sachen und seinen Hotel-Safe-Inhalt untersuchten, während das Zimmermädchen das Zimmer aufräumte. Schutz gegen Wirtschaftsspionage sollte nicht nur eine Aufgabe des IT-Beauftragten in Ihrem Unternehmen sein, sondern sollte als eine wichtige Managementaufgabe betrachtet werden. Laut einer Untersuchung, handelt es sich bei 80% der Unternehmens-Daten um nicht schützenswerte, bei 15% um wichtigere und nur bei 5% um höchst schützenswerte Daten. Diese 5% der Daten, die Kronjuwelen, gilt es zu identifizieren und mittels besonderer Maßnahmen gezielt zu sichern.

Unterstützung ist nur einen Telefonanruf entfernt

Das Bayerische Landesamt für Verfassungsschutz LfV steht Ihnen mit Aufklärung und Schutz vor Know-how-Verlust kostenfrei zur Verfügung. Sie können es per Telefon über 089/31201-500 oder per E-Mail wirtschaftsschutz@lfv.bayern.de erreichen.

Günter Schmid
VDI-AK Entwicklung-Konstruktion-Vertrieb