Wirtschaftsspionage in der Schweiz: Sind unsere KMUs bedroht?

Mit der Globalisierung haben sich die Bedrohungen für Schweizer Firmen vergrössert. Illegaler Wissenstransfer und Verlust von sensiblen Daten können die Existenz eines Unternehmens gefährden.

Wolfgang Sidler

Das Bundesamt für Verfassungsschutz in Deutschland schätzt das jährliche Schadenspotenzial, das der deutschen Wirtschaft durch Wirtschaftsspionage entsteht, auf ein Volumen von bis zu 50 Mrd. Euro. Gehen wir davon aus, dass Deutschland 10-mal grösser als die Schweiz ist, entsteht der Schweizer Wirtschaft ein Schaden von 5 Mrd. Euro bzw. 7,5 Mrd. Schweizer Franken. Ein eigentlicher «Wirtschaftskrieg» hat den militärischen und politischen Wettbewerb des Kalten Krieges abgelöst.

Die Schweiz ist vermehrt im Visier fremder Nachrichtendienste – 2008 erhielten darum 21 (im Jahr 2007 8) Osteuropäer Einreiseverbot. Hauptauftraggeber sind Russland und China. Laut dem Dienst für Analyse und Prävention (DAP) hat «das Interesse ausländischer Nachrichtendienste an der Schweiz als Standort von Forschungseinrichtungen und Unternehmen der Spitzentechnologie nicht abgenommen». Diese Art der Beschaffung von Wirtschaftsinforma-

tionen ist in Russland und China legitimiert und offizieller Aufklärungsschwerpunkt. Dabei bedienen sich die Spione der Social Engineering Methode, um an die sensiblen Informationen zu kommen. Social Engineering ist eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch «Aushorchen» zu erlangen. Beim Social Engineering werden menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Dadurch können Mitarbeiter so manipuliert werden, dass sie unzulässig handeln.
Unter Spionage versteht man die Gesamtheit von Handlungen zugunsten eines Staates, einer Firma oder einer Person, zwecks Beschaffung von geschützten oder geheimen Informationen aus den Bereichen Militär, Politik, Wirtschaft, Wissenschaft und Technologie, die zum Nachteil eines Landes oder einer Firma führt. KMUs und wissenschaftliche Institute stellen wegen ihrer innovativen Forschungs- und Entwicklungsvorhaben und ihres Knowhows häufig interessante Ausspähungsziele dar. Besonders beliebt sind auch Messen, wie beispielsweise die CeBIT in Hannover. Hier sind Spione gezielt am Werk und greifen offen auf Informationen zu, die nicht selten in Joint Ventures münden.

Wir unterscheiden die folgenden externen Bedrohungen:

a) Delikte durch Einzelpersonen an der Firma
Einbruch, Drohung, Nötigung, Betrug, Erpressung durch Kunden als «Verhandlungsstrategie»

b) Wirtschaftsspionage
Konkurrenzausspähung, abhören, kopieren, fotografieren an Messen usw.

c) Cybercrime
Diebstahl geistigen Eigentums von Produktions- und Marketingplänen, Geschäftsstrategien, Rezepte, Patente durch spezielle Trojaner und Spyware, welche durch E-Mails (SPAM) unbemerkt auf den Firmen-Computern installiert werden.

Es gibt zwei Arten der Informationsbeschaffung:

1. Die offene Beschaffung
Auswertung von Veröffentlichungen, Internet und Datenbanken, Besuch von öffentlichen Veranstaltungen (Messen, Kongresse, Symposien usw.), die Teilnahme an Studiengängen oder wissenschaftlichen Projekten (Praktikanten, Gast-/Austauschwissenschaftler), Abschöpfung im Gespräch mit der Social Engineering Methode.

2. Die geheime Beschaffung
Einsatz von Agenten, Überwachung von Telekommunikation und das Eindringen in Informationssysteme (Hacking), welches strafbar ist.

2008 wurden der KOBIK (Koordinationsstelle zur Bekämpfung der Internetkriminalität) 440 Wirtschaftsdelikte gemeldet.

Beispiele einiger Spionagefälle:

a) 2005: Grossunternehmen in Israel horchten sich mit individualisierten trojanischen Pferden aus (Mobilfunkprovider, Satelliten-TV-Anbieter, Auto-Importeure).
b) 2007: Angriff auf interne E-Mails der PNOS-Parteileitung.
c) 2005: Valéo, ein französischer Automobilteile-Hersteller in Gyancourt, entdeckte, dass eine chinesische Praktikantin namens Li Li Whuang in ihr Computersystem eingedrungen war und dort Daten über neue Konzepte kopiert hatte. Seit drei Jahren in Frankreich, galt sie als brillant und hatte Universitätsdiplome in Mathematik und Physik. Die Polizei fand bei ihr zuhause mehrere Computer und Festplatten mit enormen Speicherkapazitäten, die sie angeblich nur für ihre Arbeit bei Valéo benutzte.
d) 1994: Wurden bei Airbus die Faxe und Telefonate durch den amerikanischen Geheimdienst NSA abgehört. Ziel war, Informationen über die Verhandlungen zwischen Airbus und der saudi-arabischen Fluglinie an den US-amerikanischen Konkurrenten Boeing und McDonnel-Douglas weiterzugeben. Die Folge war, dass das 6 Mrd. US-Dollar-Projekt an den Konkurrenten Boeing ging.
e) 1996: Wurden Informationen über die Verhandlungen über Importquoten für US-Wagen auf dem japanischen Markt durch das Eindringen (Hacking) in die Computersysteme des japanischen Handelsministeriums beschafft. Ziel war, dass der US-Unterhändler Mickey Kantor beim niedrigsten Angebot einwilligen soll. Schliesslich nahm er das niedrigste Angebot an.
f) 2007: Eine Delegation liess sich in einem deutschen Unternehmen eine neue Anlage vorführen. Die Steuerung des Verfahrens erfolgte über ein älteres Notebook. Dies bewahrte der zuständige Ingenieur in seinem Büro im Schreibtisch auf. Die Täter drangen wenige Tage nach der Präsentation in das Gebäude ein und entwendeten das ältere Notebook aus dem Schreibtisch. Hierbei liessen sie ein neues Notebook samt Netzgerät ausser Acht, das auf dem Schreibtisch stand.

Es ist also zu erwarten, dass sich heute Spione (Studenten) aus China und anderen Staaten unter dem Denkmantel «Praktikant oder Trainee» von Firmen anstellen lassen, damit sie an die vertraulichen Daten gelangen. In vielen Fällen wurde zunächst nur wegen Einbruch oder Einbruchdiebstahls ermittelt und erst nach einer Sensibilisierung durch die Sicherheitsspezialisten die tatsächliche Zielrichtung – der Angriff auf das Firmen-Knowhow – erkannt. Die Beteiligung fremder Nachrichtendienste an solchen Sachverhalten ist zwar oft schwierig zu belegen, vor allem dann, wenn bereits einige Zeit seit der Tat vergangen ist. Aber gerade deshalb ist es wichtig, einen Sicherheitsspezialisten so früh wie möglich beizuziehen. Denn häufig sind an diesen Straftaten auch sogenannte Innentäter beteiligt, sodass weitere Verluste von sensiblem Firmen-Knowhow zu befürchten sind.
Wie wird heute spioniert? Fremde Staaten können E-Mails, Faxe, Telefone durch Satelliten abhören und Wanzen installieren oder können durch IT-Angriffe via Trojaner in ein IT-System eindringen und dort meistens unbemerkt Informationen sammeln und weiterleiten (z. B. unbemerktes Weiterleiten aller E-Mails).
Wer kennt es nicht? Sie besuchen eine Messe und bekommen auf den Unternehmensständen nach Abschluss eines Gesprächs kleine Werbegeschenke angeboten. Darunter ist auch ein USB-Speicherstick mit einer Kapazität von einigen Gigabytes. Obwohl gerade ein USB-Speicherstick ein hochwertiges «Give-away» ist, ist bei solchen Geschenken Vorsicht

geboten! USB-Speichermedien dieser Art gelten nur sekundär als Werbegeschenke. Primär verfolgen die Absender das Ausspionieren der Adressaten. In einigen Fällen ist ein solches Speichermedium mit einem Trojaner infiziert, der den Datenverkehr ausspioniert und diesen kontinuierlich an den Verursacher leitet.
Wie können Sie feststellen, ob Ihr Unternehmen ausgehorcht wird? Erhalten Sie zum Beispiel auf Ihre Offerten über Monate hinweg keine Aufträge mehr – sondern Ihr Mitbewerber gewinnt die Aufträge – könnte es sein, dass Ihre E-Mails mit den Offerten unbemerkt an Ihren Mitbewerber gesendet werden.

Wie können Sie sich schützen?

Personensicherheit: Vor jeder Neuanstellung, speziell für sensible Bereiche, empfehle ich Ihnen die Identität und Referenzen des Bewerbers zu überprüfen. Achten Sie aber auch darauf, wenn Sie Hilfskräfte (z. B. Reinigungspersonal) einstellen. In einem Unternehmen sollten alle Mitarbeiter inkl. Management sichtbar einen Ausweis (Badge) tragen. Nur so können die Mitarbeiter in einem grösseren Unternehmen interne von externen Mitarbeitern unterscheiden. Externe Mitarbeiter (Handwerker, temporäre Mitarbeiter) müssen einen speziell markierten Ausweis sichtbar tragen. Begleiten Sie Handwerker in die Räumlichkeiten. Verfügt Ihr Unternehmen über eine Entwicklungsabteilung, verbieten Sie digitale Kameras oder andere Mobilgeräte mit einer eingebauten Kamera während einer Führung durch diese Räumlichkeiten.

Verschlüsselung: Schützen Sie Ihr Firmen-Knowhow durch eine geeignete Verschlüsselung der Notebook-Festplatte. Wenn Sie vertrauliche Dokumente via E-Mail versenden, verschlüsseln Sie den E-Mail und dessen Inhalt. Nur mit einer angemessenen Verschlüsselung können Sie die Vertraulichkeit wahren.

Passwörter: Verwenden Sie jeweils starke Passwörter und geben Sie Ihr Passwort nie bekannt. Keine Passwortliste unverschlüsselt speichern oder ausdrucken.

USB-Sticks: Schliessen Sie keine USB-Sticks mit unbekannter Herkunft an Ihr Notebook an. Überprüfen Sie vertrauensvolle USB-Sticks und CDs nach Viren, bevor Sie diese verwenden. Speichern Sie vertrauliche Firmendaten nur verschlüsselt auf einem USB-Stick. Schliessen Sie Ihren USB-Stick an keinen unbekannten PC oder Notebook an, denn die Daten auf dem USB-Stick können schnell, unbemerkt und ohne Spuren zu hinterlassen auf den PC kopiert werden.

Handy und PDA: Vorsicht mit dem Umgang der PDAs (iPhone, Blackberry usw.). Nehmen Sie solche elektronische Geräte bei wichtigen und vertraulichen Verhandlungen nicht ins Sitzungszimmer. Auch ein angeblich ausgeschaltetes Handy kann mit einem speziellen Handy-Trojaner alles im Raum aufnehmen oder das Gespräch live übertragen.

Öffentlichkeit: Behandeln Sie geschäftliche Themen und Informationen in der Öffentlichkeit vertraulich während einer Bahn- oder Flugreise oder im Restaurant. Lassen Sie andere nicht mithören und lassen Sie sich nicht aushorchen.

Büro: Schliessen Sie vertrauliche Unterlagen weg. Verlassen Sie Ihren Arbeitsplatz jeweils aufgeräumt (Clear Desk). Werfen Sie keine Datenträger (CDs) und Dokumente mit sensiblem Inhalt ungeschreddert in den Papierkorb. Wenn Sie Ihren Arbeitsplatz auch nur für kurze Zeit verlassen, aktivieren Sie Ihren Bildschirmschoner.

E-Mail: Versenden Sie vertrauliche E-Mails nur verschlüsselt und überprüfen Sie den oder die Empfänger vor dem Senden genau. Senden Sie wenn möglich keine Word-Dokumente (DOC) in einer E-Mail. Senden Sie nur PDF-Dokumente als Anhang in einer E-Mail. Denn Word-Dokumente beinhalten viele Informationen (Meta-Daten), welche Sie in kompromittierende Situationen bringen könnten.

Software: Installieren Sie keine unbekannte Software. Vorsicht bei Freeware-Software. Stellen Sie sicher, dass die Quelle vertrauenswürdig ist. Es gab Fälle, wo Spyware in den Gratisprogrammen eingebaut war. Halten Sie Ihren Virenschutz und Ihre Programme inkl. Betriebssystem auf dem aktuellsten Stand.

Informatik: Vor der Entsorgung von Computern ist die Festplatte «sicher zu löschen». Dasselbe gilt vor dem Verschenken oder Verkaufen von Computern. Löschen oder deaktivieren Sie alle Benutzer-IDs von Mitarbeitern, welche Ihr Unternehmen verlassen haben.

Recht: Bestehen Sie darauf, dass Ihre Mitarbeiter bei der Anstellung eine Vertraulichkeitsvereinbarung (Geheimhaltungs-, Sorgfaltspflicht- und Treuepflicht) unterschreiben, welche auch nach dem Austritt Gültigkeit hat.

Weisungen: Stellen Sie sicher, dass alle Mitarbeiter die internen Firmenweisungen in Bezug auf die Nutzung der Informatikmittel kennen. Ich empfehle Ihnen eine Sicherheitspolitik erstellen zu lassen, welche die generellen Ziele der Informationssicherheit und die Informationssicherheits-Organisation definiert.

Sensibilisierung: Sensibilisieren Sie Ihre Mitarbeiter mit einfachen aber wirkungsvollen Präsentationen und Publikationen. Besonders Mitarbeiter im Verkauf, Marketing, in der Entwicklung und als Filialleiter im In- und Ausland.

Zutritt: Schützen Sie Ihre Büroräumlichkeiten und Computer-Räume vor unbefugtem Zutritt.

Risiko-Analyse: Führen Sie mithilfe eines Sicherheitsspezialisten eine Risiko-Analyse in Ihrem Unternehmen durch. Dabei geht es darum, die Unternehmenswerte zu identifizieren, damit die Risiken und Gefahren explizit richtig eingeschätzt werden können. Ermitteln Sie die möglichen Szenarien mit den entsprechenden Gegenmassnahmen.

Verhaltenstipps bei Geschäftsreisen

- Vor Reiseantritt möglichst genaues Bild vom Gastland erarbeiten, allgemeine Gefährdungs- und Sicherheitslage eruieren und mit den Gebräuchen und Gesetzen des Landes vertraut machen.
- Lassen Sie Ihr Notebook, Handy, PDA und sensible Firmenunterlagen nie unbeaufsichtigt liegen. Dies gilt insbesondere auch für die Aufbewahrung in Fahrzeugen, Seminarräumen und Hotelzimmern.

- Vermeiden Sie, Ihr mobiles Gerät auf irgendeine Weise mit Ihrer Firma in Verbindung zu bringen und verzichten Sie auf das Anbringen von Logos, Klebern usw. sowie auf die Aktivierung entsprechender, eindeutiger Bildschirmschoner.
- Tragen Sie Ihr Notebook und andere Mobilgeräte bei Flugreisen ausschliesslich im Handgepäck. Dies gilt auch für wichtige Unterlagen. Verstauen Sie alle Geräte, wenn immer möglich und für Sie gut einsehbar, unter dem vorderen Sitz.
- Setzen Sie Passwörter, Virenschutz- und Verschlüsselungsprogramme zum Schutz Ihres PCs und Notebooks ein.
- Seien Sie besonders aufmerksam, wenn Sie Ihr Notebook am Flughafen durchleuchten lassen müssen. Legen Sie es erst auf das Förderband, wenn Sie selbst durch den Metalldetektor gehen. Sollten Sie durch Anstehen aufgehalten werden, dann behalten Sie Ihr Notebook im Auge und achten Sie dabei auf verdächtige Personen, die es in der Zwischenzeit vom Band nehmen können.
- Nutzen Sie für sensible Kommunikation nur gesicherte Wege (Vorsicht insbesondere bei Fax-, E-Mail- und Telefonverkehr von unterwegs).
- Berücksichtigen Sie bei Telefongesprächen vom Mobiltelefon, dass diese ohne grossen technischen Aufwand abzuhören sind.
- Vernichten Sie nicht mehr benötigte Unterlagen. Ihr Abfall kann für andere wertvolle Informationen enthalten.
- Seien Sie misstrauisch, wenn Sie sich ungewöhnlich stark ausgefragt fühlen – nicht jeder Gesprächspartner hat das gemeinsame Geschäft im Sinn. Niemals Gespräche mit Fremden über Reisezweck und Arbeitgeber führen.
- Analysieren Sie in der Gesprächsvorbereitung, welche Informationen Ihre Gesprächspartner zu Ihrem Nachteil verwenden könnten.
- Sitzen Sie in der Bahn oder in einem Flugzeug, verwenden Sie für Ihr Notebook einen speziellen Sichtschutzfilter. So kann der Nachbar nicht mitlesen.
- Sind Sie vorsichtig beim Eröffnen von Filialen und Produktionsstätten in allen Ländern, die den Patent- und Markenschutz nicht respektieren oder nicht durchsetzen.
- Wenn Sie Ihre neuen Produkte auf internationalen Ausstellungen präsentieren, achten Sie darauf, dass während der Ausstellung kein Firmen-Knowhow gestohlen wird.

Fazit

Wirtschaftsspionage ist eine Realität! Durch die wachsende Komplexität und Vernetzung der IT-Systeme und die Globalisierung ergeben sich neue Herausforderungen an den Schutz der Daten und Informationen. Schützen Sie Ihr Firmen-Knowhow mit Ihren Möglichkeiten und lassen Sie sich wenn nötig von einem Sicherheitsspezialisten beraten. Befolgen Sie die hier beschriebenen Tipps und Empfehlungen, die dazu beitragen werden, Ihr Firmen-Knowhow angemessen zu schützen. ■