Social Engineering

Cyberfahnder #3.1

Dem Social Engineering [1] hat Kevin Mitnick ein spannendes Buch gewidmet, das er „Die Kunst der Täuschung“ nennt [2]. Die Methoden des SE sind klassische Handlungsweisen der Detektive und Spione, die von der Hackerszene entdeckt und für die Penetration datenverarbeitender Systeme verfeinert wurden. Sie sind bereits begierig aufgenommen worden von den Informationsbrokern und den Industriespionen, die damit ihr Repertoire erweitert haben.

Mitnick ist ein verurteilter Hacker aus den USA und hat seinem Buch folgende Erklärung voran gestellt:

> *Social Engineering benutzt Techniken der Beeinflussung und Überredungskunst zur Manipulation oder zur Vortäuschung falscher Tatsachen, über die sich ein Social Engineer eine gefälschte Identität aneignet. Damit kann der Social Engineer andere zu seinem Vorteil ausbeuten, um mit oder ohne Verwendung von technischen Hilfsmitteln an Informationen zu gelangen.*

Die Wikipedia definiert SE als

> *die Kunst, Menschen mittels sozialer Kontakte zu Handlungen zu veranlassen, welche zum Nachteil der Zielperson oder Dritter führen.* [3]

Im Weiteren unterscheidet sie völlig zu recht zwischen

a) der (sozialpsychologischen) Erkundung und Verwendung vertraulicher Daten mit dem Ziel, diese zu missbrauchen [4], und
b) dem Einsatz von Manipulationsstrategien, um EDV-Anwender ohne persönliche Ansprache durch Online-Informationsträger zur Offenbarung vertraulicher Informationen (z.B. Phishing) oder zur unbedarften (z.B. Trojaner) oder heimlichen Installation von schädlichen Programmen (Crimeware) zu veranlassen [5].

Die Auseinandersetzung mit dem SE birgt die Chance, die Angreifbarkeit und Sicherheit von Unternehmen und Behörden insgesamt und unter Einschluss der technischen Sicherheit wahrzunehmen, zu bewerten und schließlich Sicherheitsmaßnahmen zu entwickeln.

Der Blick von außen

Die Staatsanwaltschaft liegt unweit des Hauptbahnhofs. Sie ist in einem L-förmigen Gebäude untergebracht, dessen südlicher Teil sieben Stockwerke über dem Erdgeschoss aufweist. Dieser Trakt ist leicht konkav gebogen, wie ein Hohlspiegel. Das Erdgeschoss wird durch ein großes vergittertes Tor unterbrochen, das den Blick zu einem begrünten Innenhof zulässt. Im Hintergrund sind weitere Gebäude erkennbar.

Es ist ein Nachmittag im späten Herbst. Der größere der Teil Fenster ist von innen in verschiedenen Stärken beleuchtet. Je zwei Fenster zeigen immer eine gleichartige Beleuchtung oder sind gar nicht beleuchtet, so dass sie zu jeweils einem Raum gehören. An verschiedenen Stellen reicht die gleichartige Beleuchtung auch über mehrere Fenster hinweg und man kann auch erkennen, dass einige Leuchtröhren rechts und links über einen Mauersturz hinweg reichen. Sie kennzeichnen größere Räume, in denen entweder mehrere Leute arbeiten oder Archive untergebracht sind.

Ich gehe um den Gebäudeteil links herum und betrachte seine Schmalseite. Es besteht aus massivem Mauerwerk, das in jeder Etage mittig von einem kleineren Fenster unterbrochen wird. Diese Fenster sind höhengleich mit den Fenstern an der Langseite. Sie liegen also am Ende von Mittelgängen, von denen beiderseits Räume abzweigen und ohne dass am Ende ein Treppenhaus eingebaut ist. Dies würde sich durch höhenversetzte Fenster oder erkennbare Treppenstrukturen zeigen.

Etwas nach hinten versetzt schließt ein anderes und wahrscheinlich älteres Gebäude

1 Hier abgekürzt: SE.
2 Kevin Mitnick, William Simon, Die Kunst der Täuschung. Risikofaktor Mensch, Heidelberg 2002, 2006 (mitp).
3 Wikipedia – Social Engineering, Begriffserklärung.
4 Wikipedia – Social Engineering, Sicherheit.
5 Wikipedia – Social Engineering, Technik.

an. In diesem Anschlussbereich muss sich ein von außen nicht erkennbares Treppenhaus befinden, weil das die Bauvorschriften verlangen. Der Blick auf die Rückfront ist im wesentlichen verdeckt.

Aus einigem Abstand erkenne ich schließlich eine Richtfunkanlage auf dem Gebäudedach. Es handelt sich dabei um einen Zylinder, oder man kann auch sagen „Blecheimer", dessen flache Seite in Richtung Nordwesten ausgerichtet ist. Etwa in dieser Richtung befinden sich, wie ich im Stadtplan gesehen habe, eine größere Polizeibehörde und das Landeskriminalamt. Die Größe des „Blecheimers" zeigt, dass die Richtfunkanlage auf eine Entfernung bis zu etwa 20 Kilometer ausgelegt ist. Sie könnte also auch die Verbindung zu einem entfernteren Behördenteil, zu einer Nebenstelle oder zu einem Archiv herstellen. Um die Ausrichtung der Richtfunkanlage zu klären, müsste ich sie aus einer besseren Beobachtungsposition vermessen (genau gegenüber ist ein Hotel!) und mit genauem Kartenmaterial vergleichen.

Ich gehe zurück und zähle dabei meine Schritte. Der konkave Gebäudeteil ist etwa 70 Meter lang. An seinem „Knickpunkt", wo also das andere Teil des „L" anschließt, befindet sich ein rundläufiges Treppenhaus, wie man von außen ganz klar erkennen kann. Das anschließende Gebäudeteil ist gradlinig, knapp 100 Meter lang und weist nur fünf Etagen über dem Erdgeschoss aus. Die Raumanordnung entspricht dem, was ich auch am konkaven Gebäudeteil beobachtet habe. Nur eine Besonderheit ist zu sehen: In der ersten Etage führt nach etwa einem Drittel der Strecke eine gläserne „Beamtenlaufbahn", also eine umschlossene Personenbrücke zum gegenüberliegenden, wilhelminischen Gebäude des Amtsgerichts. In ihr bewegen sich vereinzelt Personen.

Am nördlichen Ende dieses Gebäudeteils schließt das offenbar etwas ältere Landgericht an. Die Anordnung der Fenster variiert etwas, so dass die Etagen beider Gebäude wahrscheinlich mit kleinen Treppen verbunden sind. Von außen ist im Bereich des Gebäudeanschlusses kein Treppenhaus erkennbar. Das muss innen liegen, weil es vom Baurecht vorgeschrieben ist. Auch dieser Gebäudeteil weist Innengänge auf mit beidseitig anschließenden Büroräumen, wie man sieht.

Am nächsten Vormittag stelle ich mich in besserer Alltagskleidung neben den Eingang rechts neben dem Tor zum Innenhof. Er besteht aus einer zweiflügeligen Glas-Schiebetür, die in einer gläsernen Personenschleuse mündet, die zwei Türen hat. Die linke, auch eine Schiebetür, öffnet sich automatisch. Hinter ihr befindet sich eine Pförtnerloge, die mit einem „formlos uniformierten" Menschen besetzt ist. Auf seinem Sweatshirt befindet sich die Aufschrift „Justiz".

Ich benehme mich unauffällig, wartend, rauche in Ruhe eine Zigarette. Würde mich jemand ansprechen, würde ich sagen: „Ich warte auf einen Kollegen." Dies ist ein öffentlich zugängliches Gebäude im Innenstadtbereich und deshalb auch ein üblicher Treffpunkt. Die Ausrede zieht immer.

An mir ziehen Menschen vorbei, die sich in fünf Gruppen einteilen lassen.

Das sind zunächst die etwas „abgewrackt" wirkenden Leute mit nachlässiger Kleidung, die häufig auch ungepflegt aussehen. Sie haben fast immer einen Zettel in der Hand – eine Zahlungsaufforderung oder eine Ladung, wie ich vermute – wenden sich immer an den Pförtner und werden von ihm immer nicht ganz freundlich bedient, wie man an der Gestik und den Körperbewegungen sieht. Es handelt sich also um „Kundschaft", die zur Vernehmung, zum Strafantritt oder zu einem Gerichtstermin geladen ist und hier vermittelt wird.

Die zweite Gruppe zeichnet sich dadurch aus, dass sie meist einzeln, aber auch in Gruppen mit einem Pkw vorgefahren kommen und immer Akten in roten Aktenhüllen bei sich trägt. Die meisten dieser Leute sind zivil gekleidet und die anderen tragen Polizeiuniformen. Auch sie wenden sich immer an den Pförtner und werden von ihm offenbar freundlicher bedient. Schneller als bei der ersten Gruppe greift der Pförtner zum Telefon und sie verschwinden zu den beiden Fahrstühlen, die sie nach oben befördern.

Bei der dritten Gruppe handelt es sich offenbar um Mitarbeiter oder Vertraute. Sie gehen – meistens grüßend – am Pförtner – der zurück grüßt – vorbei und warten vor den Fahrstühlen, bis sie einsteigen können. Sie grü-

ßen auch andere Wartende und sprechen – gelegentlich vertraulich wirkend – mit ihnen. Ich vermute, dass diese Leute „Schlüsselgewalt“ haben und die Zugänge zu den Büroräumen verschlossen sind – sonst würden sich die „Polizisten“ nicht artig beim Pförtner melden – nicht alle.

Die vierte Gruppe ist interessant. Sie ist nicht elegant, aber geschäftsmäßig gekleidet. Alle ihrer Vertreter tragen eine mehr oder weniger große Aktentasche und fast alle warten nicht auf den Fahrstuhl, sondern besteigen gruß- und kontaktlos die Wendeltreppe in Richtung erstes Geschoss. Viel höher werden sie nicht steigen. Einerseits machen sie überwiegend einen gehetzten Eindruck (Termindruck? Erledigungsdruck?), andererseits scheinen sie mit den Räumlichkeiten und Anbindungen vertraut zu sein. Sie müssen offenbar keine verschlossenen Türen passieren und die Laufbrücke, die ich im Bereich der ersten Etage gesehen habe, zeigt, dass hier wahrscheinlich alle drei Behörden miteinander verbunden sind. Nur ganz wenige dieser Leute wenden sich an den Pförtner und lassen sich vermitteln.

Die letzte und kleinste Gruppe besteht aus jüngeren Leuten im Studentenalter, die grußlos (authistisch? unsicher?) und zielstrebig in den hinteren Bereich der Eingangshalle gehen, wo sich, wie ich jetzt sehe, der Eingang zur Bibliothek des Landgerichts befindet.

Ich habe mir Zeit gelassen und weiß jetzt einiges über diese Behörde, ohne einen Schritt in sie gesetzt zu haben:

Nach der Anzahl der Räume, ihrer Anordnung und dem Publikumsverkehr müssen hier mindestens 200, wahrscheinlich mehr als 250 Leute arbeiten.

Es ist eine öffentliche Behörde mit Durchgangs- und Publikumsverkehr. Ihr innerer Bereich ist wahrscheinlich durch verschlossene Flurtüren gesichert.

Sie hat drei Treppenhäuser, davon ein öffentlich zugängliches im „Knickbereich“ des L-förmigen Gebäudes und zwei weitere, die baurechtlich vorgeschrieben, aber von außen nicht direkt erkennbar sind.

Eine Standard-Verkabelung für EDV-Anlagen kann keine Strecken von mehr als 100 Meter überbrücken. Die Flurlängen des Gebäudes zwingen dazu, dass irgendwo im Bereich des sichtbaren Treppenhauses die zentralen Komponenten der EDV zusammen laufen. Wahrscheinlich in der ersten Etage, weil das Erdgeschoss von der Bibliothek und linksseitig offenbar von einem Sitzungssaal eingenommen wird.

Die Richtfunkanlage ist auf hohe Leistung ausgelegt. Sie benötigt eine Wandlungs- und Steuerungsstation in dem Bereich zwischen den zentralen Komponenten und ihrem Standort, weil sonst die Strecke von 100 Metern überschritten wäre. Dazu dürfte ein eigener, zwar kleiner, aber wahrscheinlich abgeschlossener Raum verwendet werden.

Ich werde jetzt meine Aktentasche unter den Arm klemmen und grußlos zum Fahrstuhl gehen, dort werde ich die Taste für die erste Etage drücken, aber dann in den siebten Stock fahren. Zuerst werde ich danach schauen, ob die Flure wirklich verschlossen sind und ob es noch unverschlossene Nebenräume gibt, wo technische Komponenten oder andere interessante Einrichtungen abgestellt oder installiert sind. Dabei lohnt sich immer auch ein Blick auf Blechtüren im Mauerwerk, hinter denen sich häufig die Verteilerkästen für die Telekommunikation und die Datennetze befinden.

Von oben nach unten werde ich das Treppenhaus nutzen, das ist immer unauffällig, weil die meisten Leute mit dem Fahrstuhl nach oben fahren und eher gelassen das Treppenhaus nach unten benutzen. Ich liebe bequeme Leute, die eigentlich verschlossene Türen mit Keilen oder anderen Gegenständen geöffnet halten, um den Zugang zu den Fluren frei halten oder ihren Besuchern den Zugang zu ermöglichen, ohne ihnen einen Schlüssel geben zu müssen.

Besuchergruppen liebe ich sowieso. Ihr Leiter kennt die einzelnen Personen der Delegation in aller Regel nicht, so dass man sich der Gruppe einfach nur unauffällig anschließen muss, um in verschlossene Bereiche zu gelangen.

Unauffälligkeit und Smalltalk sind die wichtigsten Türöffner für geschlossene Bereiche, deren Sicherheit von Niemanden so richtig überwacht wird.

Risikofaktor Mensch

Mehr als 60 oder 70 Prozent aller Angriffe gegen Datenverarbeitungssysteme erfolgen nicht von außen, sondern von innen, also von den eigenen Mitarbeitern, die selten aus Böswilligkeit, sondern aus Unwissenheit, aus Unbekümmertheit oder aus Bequemlichkeit Betriebs- und Sicherheitsvorgaben missachten, umgehen oder aushebeln. Dasselbe gilt für Betriebs- und Unternehmensgeheimnisse, die nirgendwo so unüberlegt ausgeplaudert werden wie am Telefon oder in E-Mails an Geschäftspartner.

Auf dieser Erkenntnis fußend hat sich bereits in vielen US-amerikanischen Firmen eine Sicherheitsphobie entwickelt, die zu massiven (illegalen) Überwachungen des Telefon- und E-Mailverkehrs geführt hat [6]. Das größte Echo in der Öffentlichkeit erfuhr die interne Untersuchung bei Hewlett-Packard wegen Insiderinformationen aus dem Verwaltungsrat, die an Medien weitergegeben wurden [7].

Studien zur IT-Sicherheit sprechen davon, dass 2005 jeder zwölfte Angriff zum Totalausfall der Firmen-IT geführt hat (8,4 %) [8]. In 17,4 % der Fälle waren betriebskritische Anwendungen nicht verfügbar, traten finanzielle Verluste (5,3 %) oder eine Schädigung des Rufes oder der Marke ein (4,2 %).

Dem SE geht es um die Informationsbeschaffung und nicht zwingend darum, die Datenverarbeitung zu stören. Ihr Arsenal besteht aus allen Methoden der Manipulation und Suggestion: „Täuschung, Bestechung, Erpressung, Einschüchterung, Bedrohung, Appellieren an die Hilfsbereitschaft oder Ausnutzen der Arglosigkeit des Opfers“ [9].

6 Wolf-Dieter Roth, Sicherheitsrisiko Mitarbeiter, Telepolis 12.06.2006;
Peter Mühlbauer, Trojaner vom Chef, Telepolis 04.04.2006;
ders., Anonymisieren oder Pseudonymisieren, Telepolis 18.04.2006.

7 Jüngste Meldung bei heise online (mit weiteren Verweisen): Beschuldigungen gegen Ex-HP-Verwaltungsratsvorsitzende aufgegeben, heise online 15.03.2007.

8 Zahlen aus der Studie "IT-Security 2005", zitiert nach tecchannel, Angriffe auf IT-Sicherheit: Störfälle nehmen zu, 06.10.2005.

9 Christoph Baumgartner, Social Engineering – trau schau wem, computerworld.ch 05.08.2005.

Fünf unwichtige Informationen ergeben eine sensible

Sven Vetsch [10] beschreibt das Vorgehen beim SE in sechs typischen Schritten:

1.) **Informieren**
Informationen über das Ziel der Social Engineering Attacke sammeln, z.B. Im Internet oder per „Dumpster diving“, also das Durchwühlen von Abfällen auf der Suche nach betriebsinternen Informationen wie Organigramme, Telefonverzeichnisse, persönliche Aufzeichnungen. Andere öffentliche Quellen sind z.B. Bibliotheken, Patentschriften, Museen und öffentliche Auftritte auf Messen.

2.) **Kontakt aufbauen**
Anruf, persönlicher Besuch, Brief, E-Mail, Newsgroup, Weblog.

3.) **Vortäuschung einer Identität**
In eine andere Rolle schlüpfen, z.B. als Vorgesetzter der Kontaktperson, als Endanwender, als Kunde oder als Interviewer bei einer Telefonumfrage.

4.) **Zielinformationen erarbeiten**
Sich durch verschiedene Fragen an die Zielinformationen herantasten. Beispiele:
a) Ich bin neu in der Systemverwaltung und muss Ihre Anwenderdaten überprüfen. Wie war noch Ihre Zugangskennung? Und das Passwort?
b) Hier arbeitet doch die Frau Sowieso (Information aus einem Organigramm aus dem Vorjahr). Arbeitet die hier gar nicht mehr?
c) Hier Meier, PI Garbsen. Ich habe von meinem Kollegen den Vorgang wegen des Verkehrsunfalls (dort und dort) übernommen. Ist der Vorgang mit dem Führerschein schon bei Ihnen?

5.) **Wenn man die Zielinformationen hat, den Kontakt möglichst nicht “verlieren“**
Die Kontaktperson darf nicht merken, dass sie sensible Daten an einen Social Engineer weitergegeben hat. Gute Kontakte kann man immer wieder verwenden. Der Zugang zu ihm ist leichter, weil man auf die zurücklie-

10 Sven Vetsch, Social Engineering, Präsentation, www.disenchant.ch 2005.
Die sechs Schritte folgen Vetsch' Darstellung. Die Erklärungen wurden überarbeitet und ergänzt.

genden Kontakte Bezug nehmen kann und die Kommunikation bereits vertraut ist. Der geschickte Angreifer lässt dabei auch immer wieder persönliche Informationen einfließen, die er bei den früheren Kontakten gesammelt hat.

6.) **Informationen zusammensetzen**
Die Teilantworten müssen sinnvoll miteinander kombiniert werden. Meistens hat man nur nach Teilinformationen gefragt und auch nur solche erhalten. Sie mögen noch so banal erscheinen, können jedoch häufig zu sensiblen Informationen verbunden werden.

Erfahrungsgemäß ergeben fünf unwichtige Informationen eine sensible.

Der Blick von innen

Kurz vor zwölf Uhr. Mittagszeit. Kolleginnen und Kollegen treffen sich und machen sich auf den Weg zur Kantine. Ich grüße – freundlich und zurückhaltend – und schließe mich der Gruppe an. Man hält mir die Tür auf und schon bin ich in dem „verschlossenen" Flur. Die Gruppe biegt zu einem innen liegenden Treppenhaus ab (wie ich von außen vermutet hatte!) und ich gehe ein paar Schritte weiter. Schon bin ich wieder unauffällig von der Gruppe getrennt.

Ich gehe zurück zu der Tür, aus der Mann kam, der sich zuletzt der Gruppe anschloss. Sein Name steht auf einem Schild neben der Tür, „Müllermann", aber die Tür ist verschlossen. Ich klopfe an der Nachbartür und trete ein. Das Zimmer ist besetzt. „Entschuldigen Sie, ich bin mit Herrn Müllermann verabredet." „Der müsste gerade zu Tisch sein", lautet die freundliche Antwort. Auch die beiden nächsten Türen sind verschlossen. Eine weitere systematische Untersuchung könnte bei dieser Tageszeit zu auffällig sein.

Ich schlendere den Flur zurück. Fast an seinem Ende führt ein dicker aufgeschraubter Kabelschacht quer an der Decke über den Gang. Hier laufen also die Datenleitungen für die Büros des Flures zusammen. Wie ich vermutet hatte befindet sich der zentrale Raum für die Datenverarbeitung in der Nähe des zentralen Treppenhauses.

Die Flurtüren lassen sich von innen mit einem Türgriff öffnen. Zwei Etagen tiefer habe ich Glück. Die Flurtür ist unverschlossen, weil sie nicht richtig ins Schloss gefallen ist.

Auch hier treffen sich Kolleginnen und Kollegen zum Mittagessen. Eine von ihnen vergisst, ihre Bürotür abzuschließen. Kaum ist die Gruppe aus meinem Blick, bin ich in ihrem Büro. Ich habe jetzt etwa zwanzig Minuten Zeit. Der PC ist eingeschaltet und der Bildschirmschoner oder eine andere Zeitschaltung sind noch nicht aktiv. Ich komme jetzt an alle Informationen, zu denen auch die unvorsichtige Mitarbeiterin Zugang hat.

Organisationssicherheit

Die Geschichten über die Blicke von innen und außen zeigen, dass ein geschickter Angreifer allein mit seinen Beobachtungen, mit öffentlichem Allgemeinwissen und überlegten Kombinationen sensible Informationen über eine fremde Organisation, ihren Aufbau und ihren inneren Abläufen sammeln und erschließen kann. Der Erzähler hat erst etwas Illegales getan als er die verschlossenen Bereiche betrat und schließlich die Daten ausgespähte, auf die er es abgesehen hat.

In Mitnicks Berichten über das SE werden Szenen beschrieben, wie mit belanglosen internen Informationen Vertrauen geschafft und die Gesprächspartner dazu gebracht werden, weitere vertrauliche Informationen bis hin zu personenbezogenen Daten und echten Geheimnissen zu offenbaren. Er beschreibt den Einsatz von Keyloggern, die am PC installiert werden, um die Tastatureingaben zu protokollieren, wie ungesicherte Datensteckdosen zum Eindringen in das EDV-System verwendet und wie die Zugangsdaten von Mitarbeitern missbraucht werden können. Für den Angreifer, der es auf die EDV abgesehen hat, ist es besonders wichtig, einen Zugang mit Administratoren-, also mit vollen Zugriffsrechten zu erlangen, mit denen er auf alle geschützten Informationen zugreifen kann.

Die Sicherheit der Informationstechnik beginnt bei der einfachen Physik. Serverräume müssen verschlossen, klimatisiert und brandgeschützt sein. Verteilerkästen für Datenleitungen müssen abgeschlossen sein; wenn nicht, lässt sich womöglich mit einem Nagelknipser die EDV in mehreren Etagen

so sabotieren, dass eine neue Verkabelung installiert werden muss. Datensicherungsbänder gehören in einen Stahlschrank, der sich möglichst in einem anderen Gebäude befindet. Nur dann ist bei einem fatalen Störungsfall (Feuer, Hochwasser, Sabotage) sicher gestellt, dass die Daten mit neuer Technik wieder hergestellt werden können.

Die heutigen Methoden zur technischen IT-Sicherheit sind so verfeinert, dass einfache Angriffe scheitern müssen. Das beginnt bei Datensteckdosen, die nur auf ein bestimmtes Endgerät reagieren, das dort mit seinen individuellen Merkmalen angemeldet ist, und endet bei strikten Regelwerken, die die Installation von fremder Software und damit auch von schädlicher Crimeware am Arbeitsplatz rigoros verhindern. Das Bundesamt für Sicherheit in der Informationstechnik – BSI [11] – hat hierzu ein Regelungswerk geschaffen und verschiedene Studien veröffentlicht, die kaum Lücken offen lassen und neben einem „Grundschutz“ [12] auch „kritische“ Datenverarbeitungsvorgänge [13] im hohen Maße sichern.

Die IT-Sicherheit wird häufig nur als technische Sicherheit angesehen. Die Diskussion um das SE zeigt hingegen, dass die IT-Sicherheit immer eingebettet ist in die allgemeine Organisationssicherheit. Die Korruptionsbekämpfung oder die Abwehr von Spionen beschränken sich deshalb heute nicht mehr auf die klassischen Betrachtungsweisen, sondern müssen sich auch den Besonderheiten der Informationstechnik stellen und sie in ihre Konzepte einbinden.

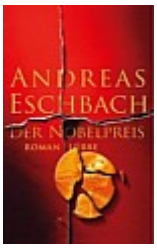
Das Wichtigste bei allen Sicherheitsfragen ist die Ausbildung und die gelebte Sensibilität der Mitarbeiter. Sie lassen sich mit Dienstanweisungen unterstützen, aber nicht ersetzen. Die Mitarbeiter müssen erkennen lernen, wo Unsicherheitsquellen sind und wo ihnen ungewöhnliche oder sensible Informationen abgefragt werden – und sie brauchen Handlungsanleitungen und eine Ansprechstelle, an die sie ihre Beobachtungen und Befürchtungen vorbehaltlos melden können.

SE und Crimeware

Die Überredungstechniken, die das SE prägen, haben längst Eingang in andere kriminelle Techniken gefunden. Am deutlichsten wird das im Zusammenhang mit der Verbreitung von Crimeware durch Anhänge an unverlangt eingehenden E-Mails (Spamming, Phishing). Die meisten dieser Crimeware-Programme müssen von dem Empfänger aktiviert werden, indem er die angebotenen Anhänge mit einem Doppelklick öffnet. Anstelle eines Dokuments mit Informationen, das der Empfänger erwartet, wird damit die Installation eines schädlichen Programms gestartet, das die Daten oder Verarbeitungsvorgänge des befallenen Computers ausspähen oder ihn sabotieren soll [14].

Die Nachrichten, die dazu verwendet werden, versuchen einen „Nerv“ des Empfängers zu treffen, also ein persönliches Interesse, eine Neigung oder eine Gewohnheit anzusprechen. Besonders deutlich wurde das, als seit Ende 2006 gefälschte Bestätigungs-Mails in den Umlauf kamen, die eine „Rechnung“ als Anlage hatten. Dabei handelte es sich aber nicht um ein Textdokument (Rechnung.doc) oder um ein PDF-Dokument (Rechnung.pdf), sondern um einen Trojaner (Rechnung.exe), der sich zu installieren versuchte [15]. Auch erfahrene und in EDV-Fragen vertraute Leute, die mit Beschaffungen betraut sind, haben versucht, die Anlagen zu öffnen, und sogar die E-Mails beantwortet, weil sie die angekündigten Geräte gar nicht bestellt hatten.

11 Website des Bundesamtes für Sicherheit in der Informationstechnik.
12 BSI - Grundschutzhandbuch.
13 BSI – kritische Infrastrukturen – KRITIS.
14 Über die Einzelheiten und die Eigenschaften von Botnetzen wird der Cyberfahnder an anderer Stelle berichten.
15 Überblick über die verschiedenen Varianten bei heise online (Suchworte „Trojaner“ und „Rechnung“).



Industriespionage

Andreas Eschbach lässt einen klassisch handelnden Industriespion [16] zu Wort kommen:

„Hacker - also Leute, die sich über Datennetze in fremde Computersysteme einklinken, um dort auf die Suche nach interessanten Daten zu gehen - gibt es wie Sand am Meer. Sie mögen ihre Daseinsberechtigung haben; auf jeden Fall verkörpern sie das Bild, das sich die Öffentlichkeit von einem Industriespion macht. Ich jedoch begebe mich vor Ort, ich weiß, was ich tue, und ich kann einschätzen, was ich zu sehen bekomme. Das ist mein persönlicher Wettbewerbsvorteil.

Denn was ist, wenn sich die interessanten Daten in Computern befinden, die an kein Netz angeschlossen sind? Was, wenn die Unterlagen, auf die es ankommt, überhaupt nicht in digitaler Form vorliegen, sondern als Papiere, Pläne, handschriftliche Notizen? In solchen Fällen schlägt meine Stunde. Ich komme nicht durch ein Kabel, ich komme durch die Tür. Ich knacke keine Passwörter, ich knacke Schlösser. Ich bin nicht darauf angewiesen, dass es einen Zugang gibt zu den Informationen, die meine Auftraggeber interessieren, ich bahne mir meinen Zugang selbst.“

Der Einsatz von Crimeware ist eine Massenerscheinung. Mit geschickt formulierten Anschreiben soll damit eine bestimmte Zielgruppe angesprochen werden (Raiffeisenbanken / Volksbanken, Bestellungen bei der Firma Dell usw.), die damit dazu gebracht werden sollen, eine bestimmte Seite im Internet aufzurufen, wo ihre Kontodaten abgefragt werden (Phishing), oder ein als Anlage mitgeführtes Programm zu starten.

Eine neue Erscheinungsform ist die individualisierte Crimeware. Sie greift ganz gezielt bestimmte Personen [17] an, um ihre persönlichen Daten auf dem PC auszuforschen, oder konkurrierende Unternehmen [18]. Um sie einzusetzen muss man entweder einen physikalischen Zugriff auf das Zielsystem bekommen oder die Zielperson mit den Mitteln des SE dazu überreden, das präparierte Programm zu installieren. Wie bei der üblichen Crimeware auch kann es in PDF-Dokumenten (und vielen anderen Formaten) oder in ein Demo-Programm eingebunden sein, das man unter Geschäftspartnern zu Werbezwecken oder zur Vertragsanbahnung übermittelt.

Im Zusammenhang mit der Online-Durchsuchung dürften keine anderen Angriffstechniken zum Einsatz kommen.

16 Andreas Eschbach, Der Nobelpreis, Bergisch Gladbach (Lübbe) 2005, S. 160.

17 Alfred Krüger, "L wie Lüge" - Spionage via Unikat-Trojaner, Telepolis 07.03.2006.

18 Trojaner spionierte israelische Unternehmen aus, heise online 30.05.2005.