

Soziale Manipulation

Auf den ersten Blick kaum gefährlich

Technische Sicherheitseinrichtungen, wie zum Beispiel Firewalls, Virtual Private Networks oder Virens Scanner, sind in jeder Kanzlei unerlässlich. Für Angreifer ist aber der Mitarbeiter die Informationsquelle Nummer eins. Die „soziale Manipulation“ (Social Engineering) ist eine Technik, mit der vertrauliche Daten von Mitarbeitern erschlichen werden.

Der Hacker Kevin Mitnick erläutert in seinem Buch „Die Kunst der Täuschung“ anhand fiktiver Beispiele, wie sich mit bestimmten Techniken vertrauliche Daten ausspähen lassen. Als er vor dem US-amerikanischen Kongress wegen tatsächlicher Angriffe auf fremde Daten danach gefragt wurde, wie er an sensible Unternehmensdaten gekommen sei, antwortete er, er habe nur danach gefragt. Fachleute bezeichnen diese Art des Datenklaus als soziale Manipulation (Social Engineering).

Das Grundmuster solcher Angriffe ist immer ähnlich. Im ersten Schritt benötigt der Angreifer Informationen über sein Angriffsobjekt. Geschäftsunterlagen, wie etwa Organigramme, Arbeitsanweisungen, Telefon- oder Mitarbeiterlisten, erscheinen Mitarbeitern als nicht schützenswert. Für Angreifer sind sie aber wertvoll. Sie holen sich die Informationen per Telefon, über öffentlich zugängliche

Quellen oder über den Papierabfall. Am ergiebigsten ist das persönliche Gespräch, da, wie aus der Psychologie bekannt ist, Menschen auf Verhaltensmuster reagieren. Dies nutzen Angreifer aus und erschleichen sich dadurch Daten, indem sie etwa autoritär auftreten oder versuchen, Zuneigung beim Gesprächspartner zu erzeugen.

Beispiel: Ein Unternehmen will sich aktuelle betriebswirtschaftliche Auswertungen (BWAs) eines Mitbewerbers verschaffen. Dazu muss es wissen, wo solche Daten vorliegen können. In diesem Beispiel kommen etwa die Geschäftsleitung, das Rechnungswesen, der Steuerberater und die Banken infrage. Der Steuerberater übermittelt, etwa im Rahmen des Prozesses Wirtschaftsberatung, auf Wunsch des Mandanten die BWAs direkt an das Unternehmen. Die Übermittlung erfolgt oft per E-Mail oder Fax. Da aber die Verschlüsselungssysteme zwischen Steuerberater und Mandant häufig nicht kompatibel sind, erfolgt die Übertragung meistens unverschlüsselt.

Angreifer gibt sich als autorisierter Mitarbeiter aus

Wenn der Angreifer weiß, welcher Steuerberater das Mitbewerberunternehmen betreut, ruft er dort als angeblich autorisierter Firmenmitarbeiter an. Er gibt sich etwa selbstbewusst als Assistenz der Geschäftsleitung oder Vertretung im Rechnungswesen aus. Aus einem vorgetäuschten Grund gibt er die Anweisung, die BWAs an das Unternehmen zu übermitteln. Er muss nur erreichen, dass die BWAs an eine bestimmte E-Mail-Adresse oder Fax-Nummer übermittelt werden.

Kanzleichefs sollten ihre Mitarbeiter über das Thema soziale Manipulation informieren, sie dafür sensibilisieren und ihr Sicherheitsbewusstsein entsprechend schärfen. Dies geschieht am effektivsten durch Schulungen, regelmäßige Aushänge, Erinnerungs-E-Mails, entsprechende Infozettel und Broschüren

» Serienplaner

Teil 3 – SteuerConsultant 3/09
Mobiles Arbeiten

Teil 4 – SteuerConsultant 4/09
Soziale Manipulation –
lernen von den Profis

Teil 5 – SteuerConsultant 5/09
VoIP – billig telefonieren,
teuer bezahlen

Abonnenten-Service

Abonnenten können im Internet unter www.steuer-consultant.de das Themenarchiv nutzen und unter anderem alle Teile der Serie „Datenschutz“ kostenlos nachlesen.



Stephan Rehfeld,

Diplom-Ökonom, ist Geschäftsführer der scope & focus GmbH, der IT-Tochter des Steuerberaterverbands Niedersachsen Sachsen-Anhalt e.V.

und externer Datenschutzbeauftragter.

E-Mail: info@scope-and-focus.com

www.scope-and-focus.com



Ralf Röhr,

Diplom-Ingenieur, ist Geschäftsführer der KRK Computer Systeme GmbH.

E-Mail: info@krk-computersysteme.de

www.krk-computersysteme.de

oder auch im Rahmen der jährlichen Zielvereinbarungsgespräche. Um den Erfolgsgrad der Sensibilisierung zu messen, empfehlen sich beispielsweise willkürliche Testangriffe. Schließlich kann nur ein entsprechend vorbereiteter Mitarbeiter einen solchen Angriff erkennen und auf ihn angemessen reagieren.

Auch die Weitergabe von Daten an Dritte sollte für die Mitarbeiter der Steuerberatungskanzlei im Rahmen einer Richtlinie klar geregelt sein. Im ersten Schritt ist sämtlichen Daten der Status „vertraulich“, „intern“ und „öffentlich“ zuzuordnen und mit den Klassifikationen auszuzeichnen.

Darüber hinaus müssen Regeln zur Datenweitergabe definiert werden. Es kann zum Beispiel geregelt werden, dass nur eine kleine Gruppe von Personen, wie die Geschäftsleitung oder das Rechnungswesen, vertrauliche und interne Daten abrufen darf und nur selbst an Dritte weiterleiten kann.