

## Sicherheitsrisiko Nummer 1 ist der Mensch

Mit Methoden des „Social Engineering“ können Datendiebe die Sicherheitssysteme von Unternehmen überwinden. Unterstützung bei diesen Angriffen bekommen Sie von arglosen, hilfsbereiten Mitarbeitern des angegriffenen Unternehmens.

„Unser Netzwerk ist sicher“, verkünden IT-Verantwortliche landauf landab. Durch Firewall, Virenschutz, Intrusion Detection und weitere Systeme sind die Daten vor einem Angriff durch Hacker gut geschützt. Das ist gut und richtig. Die oben zitierte Aussage stimmt jedoch nur, wenn der Angriff von Außen erfolgt. Gegen einen Angriff von Innen schützen die Systeme nicht. Social Engineering wird eine Methode genannt, mit der die technischen Sicherheitsbarrieren von Firmen durch Kommunikation überwunden werden können. Dazu zählen „Phishing-Mails“ ebenso, wie andere, noch weitaus effizientere Angriffsvarianten. Alle haben eines gemeinsam: Angriffsziel ist der Mitarbeiter. Unterm Strich ist deshalb jeder nicht auf solche Situationen vorbereitete Angestellte ein Sicherheitsrisiko.

Drei von vier Unternehmen halten das Sicherheitsniveau ihrer IT-Systeme auf aktuellem Stand. Regelmäßige Wartung, Support und Investitionen in die Technik sind die meistgenutzten Mittel. Das hat das Marktforschungsinstitut MR&S in einer Umfrage bei mittelständischen Unternehmen herausgefunden. Mitarbeiterschulungen nutzen nur 16 Prozent. Diese Zahlen belegen deutlich, wo ein Angriff auf die Firmendaten am einfachsten wäre: Bei den Mitarbeitern. Genau diese Sicherheitslücke nutzt ein Social Engineer.

Immer wieder machen Meldungen Schlagzeilen in denen über Datenklau durch entlassene Mitarbeiter berichtet wird. Das Risiko ist bekannt und meistens werden die notwendigen Schutzmaßnahmen eingesetzt. Doch gerade der zufriedene, motivierte Mitarbeiter kann bei einem Angriff durch einen Social Engineer zur Gefahrenquelle für das Unternehmen werden. Anhand der folgenden Szenarien wird hier das Gefahrenpotential skizziert.

### **Szenario 1 – Schwachstelle Hilfsbereitschaft**

Ein sympathischer, gut gekleideter Mann betritt gegen Mittag den Eingangsbereich eines Unternehmens. Er erkundigt sich nach einem führenden Mitarbeiter mit dem er angeblich zum Essen verabredet ist. Nennen wir diesen Manager: Maier. Herr Maier ist in einer Besprechung und der Besucher beschließt, im Foyer zu warten. Nach einer ¼ Stunde fragt er wieder nach Herrn Maier, der aber immer noch in einer Besprechung ist. Der Besucher zieht sich nochmals in die Sitzecke zurück, klappt sein mitgebrachtes Notebook auf und beginnt zu arbeiten.

Wieder 15 Minuten später fragt er erneut erfolglos nach Herrn Maier. Jetzt verbindet er diese Frage mit einer weiteren: Ob es nicht in der Nähe eine ruhigeren Besprechungsraum gäbe, in dem er warten und währenddessen arbeiten könnte. Nicht jeder Mitarbeiter am Empfang wird ein solches, freundlich vorgetragenes Ansinnen mit einem klaren „Nein“ beantworten. Denn gerade für das Personal am

Empfang ist „Hilfsbereitschaft“ eine Selbstverständlichkeit. Bei einem „Ja“ hat der Besucher gewonnen. Oder können Sie garantieren, dass in jedem Besprechungsraum die Netzwerkzugänge einem Angriff standhalten? Bedenken Sie bei Ihrer Antwort: Der Angreifer ist innerhalb des Unternehmens. Es gibt also kaum noch technische Hindernisse, die überwunden werden müssten.

„Frechheit siegt“ heißt es. Und genau auf dieser Überlegung basiert dieser Angriff. Wenn Sie in einen Besprechungsraum eines Unternehmens eindringen wollen: Weshalb fragen Sie nicht einfach, ob man Ihnen diesen Zugang nicht freiwillig gewährt?

### **Szenario2 – Soziale Bestätigung**

Das Telefon in der Marketingabteilung klingelt. Am Apparat ist ein Marktforschungsinstitut. Der Anrufer gibt an, dass er diesen Anruf mit dem – überraschenderweise heute nicht anwesenden Abteilungsleiter – besprochen hat. Dieser hat Sie als Ansprechpartner benannt. Können Sie da „Nein“ sagen? Das ist eher unwahrscheinlich. Und die Umfrage beginnt: Wie viele Mitarbeiter hat die Firma? Wie viele davon arbeiten am PC? Welches Betriebssystem haben die PCs? Gibt es eine Firewall bzw. Antivirenschutz? Wie lautet die Benutzerkennung? Wie viele Zeichen hat Ihr Passwort? (Hinweis des Anrufers: Sagen Sie auf keinen Fall Ihr Passwort, sondern nur die Anzahl der Buchstaben!) Wie entsorgen Sie Müll? Was machen Sie mit alten CDs und Disketten? Welche Telefonanlage nutzen Sie? Und noch ein paar weitere Fragen zu Öffnungszeiten und anderen banalen Sachen.

Der Mitarbeiter antwortet auf die Fragen, weil ja schließlich sein Vorgesetzter ihn genau dafür ausgewählt hat. Die Hoffnung: Je besser die Mitarbeit, umso größer die Anerkennung. Wie viele Mitarbeiter würden bei diesen guten Aussichten die Antwort verweigern? Aus einer gut strukturierten Umfrage können eine Vielzahl an Informationen heraus gezogen werden. Wichtig ist, dass brisante Fragen in ein möglichst allgemeines Umfeld eingebettet werden. Technisches Know-how ist hier nicht unbedingt erforderlich. Der Anrufer muss nur gut reden können.

### **Szenario 3 – Eine technische Variante**

Eine Führungskraft hat ein Notebook mit Wireless-LAN (WLAN). Damit der Manager auch zu Hause arbeiten kann, richtet er sich privat ein WLAN ein. Das WLAN wird nur unzureichend gesichert. Es ist dadurch für einen Datendieb ein Leichtes alle drahtlos übertragenen Daten „mitzulesen“, z.B. E-Mails, Office-Dokumente u.ä. Dehnen Sie dieses Szenario auf die „Hot-Spots“ von Flughäfen, Bahnhöfen und Hotels aus, die in der Regel ohnehin unverschlüsselt arbeiten, dann wird das Gefahrenpotential noch offensichtlicher.

Diese simple Geschichte zeigt, mit welcher einfachen technischen Mitteln ein Datendiebstahl möglich wird, wenn der Mitarbeiter die vorhandene Sicherheitstechnologie nicht richtig einsetzt, oder sie vielleicht im privaten Bereich sogar für überflüssig hält. Der Angreifer braucht nicht viel Know-how, um eine solche Sicherheitslücke auszunutzen: Ein WLAN-Notebook, die Adresse des Managers und ein wenig kostenlose Software reichen schon aus. Dieser Angriff stellt auch Laien nicht vor große Probleme. Bei einer halbstündigen „Testfahrt“ durch Hamburg fand der Autor mehr als zehn ungeschützte WLAN-Zugänge.

Das waren drei einfache Szenarien. Mit ein wenig Phantasie kann sich jeder Manager weitere Varianten ausmalen. Das gefährliche an den Angriffen ist, dass sie oft gar nicht als solche erkannt werden und deshalb jederzeit wiederholt werden können. Das macht aus jedem Mitarbeiter ein dauerhaftes Sicherheitsrisiko.

Natürlich kommt auch ein Social Engineer nicht ganz ohne den Einsatz von Technik aus. Doch die Rahmenbedingungen sind andere, als bei einem Hackerangriff. Denn die wenigsten Firmennetzwerke sind darauf ausgelegt, einen Angriff von Innen abzuwehren. Hinzu kommt, dass freundliche und hilfsbereite Mitarbeiter den Social Engineer tatkräftig dabei unterstützen, die wenigen vorhandenen Schranken zu überwinden.

### **Was ist zu tun?**

Die Angriffe eines Social Engineers finden im Unternehmen statt. Sie nutzen die größte Schwachstelle – den Mitarbeiter – für den Angriff aus. Gegen einen so organisierten Datendiebstahl schützen die gängigen Sicherheitssysteme kaum. Dennoch: Firewall und andere technische Sicherheitssysteme sind wichtig und müssen immer topaktuell sein. Doch mindestens genauso wichtig sind Sicherheitsleitlinien, die die Sicherheitslücke „Mensch“ schließen.

Wichtig ist, dass beim Aufbau der Sicherheits-Leitlinien die Kreativität, die Hilfsbereitschaft, der Teamgeist nicht auf der Strecke bleiben. Es muss deshalb genau abgewogen werden, welche Maßnahmen letztlich notwendig sind und welche den reibungslosen Arbeitsablauf zu stark einschränken. Deshalb sollte am Anfang ein kurzes „Sicherheitstraining“ für alle Mitarbeiter stehen. Jeder vom Hausmeister bis zum Vorstand sollte die Risiken und Methoden eines Social Engineering-Angriffs kennen lernen. Auf dieser Basis werden dann die Sicherheits-Leitlinien entwickelt. Diese müssen genauso wie die Antiviren-Software regelmäßig aktualisiert werden. So können neue Mitarbeiter das Sicherheitssystem kennen lernen und alte Mitarbeiter ihr Wissen auffrischen. Durch die richtige Kombination aus technischen Abwehrmaßnahmen und Kommunikationsregeln kann die Sicherheit im Unternehmen deutlich gesteigert werden.

Ralph Dalibor

Bielefeld, Januar 2006

Der Artikel ist erschienen im Artikeldienst des Deutschen Industrie- und Handelskammertages (DIHK) und steht allen IHK-Magazinen zur Verfügung.