Grösstes Risiko – grösste Chance

Über 70 Prozent der Befragten einer Umfrage in London würden ihr persönliches Computer-Passwort für einen Schokoladenriegel bekanntgeben. Wo bleibt hier das Sicherheitsdenken und das Pflichtbewusstsein? Der Mensch ist das grösste Risiko überhaupt – vielleicht aber auch die grösste Chance?

VON WOLFGANG SIDLER

Der Mensch ist das schwächste Glied in der Informationssicherheitskette. Dieser Tatsache bedienen sich so genannte «Social-Engineering-Angriffe». Technische Sicherheits-Massnahmen bieten keinen Schutz vor nicht-technischen Angriffen.

Diverse Studien zum Thema Gefahrenbereiche belegen, dass die Befragten Irrtum und Nachlässigkeit eigener Mitarbeiter als grösstes Risiko einstufen. Da bleibt die Frage: Wofür wird investiert? Auch hier belegen verschiedene Studien, dass in den letzten zehn Jahren fast nur in die Technik investiert wurde. Investitionen in Awareness-Programme und Ausbildung der eignen Mitarbeiter wurde keine angemessene Beachtung geschenkt.

2004 hatte London-Taxi innerhalb von sechs Monaten 63 135 Handys, 4973 Notebooks und 5838 PDAs gefunden. Was für Daten und Informationen waren auf diesen Geräten gespeichert? Waren die Daten verschlüsselt? Welche Schäden hätten bei den betroffenen Unternehmen entstehen können? Es steht ausser Zweifel, dass nicht der Verlust der Hardware der eigentliche Schaden ist, sondern das Offenlegen vertraulicher Daten und ein möglicher Imageverlust.

Social-Engineering

Social-Engineering nennt man zwischenmenschliche Manipulation mit dem Ziel, unberechtigt an Dinge zu gelangen. Social-Engineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen falsche Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um Dinge wie geheime Informationen oder unbezahlte Dienstleistungen zu erlangen. Meist dient Social-Engineering dem Eindringen in ein fremdes Computersystem, um vertrauliche Daten einzusehen; man spricht dann auch von Social-Hacking.

Wolfgang Sidler
ist Master of Advanced Studies FHZ in Information Security, eidgenössischer Wirtschaftsinformatiker, BSI ISO 27001 Lead Auditor, ITIL Certified und MCSE. Seit 2006 ist er Senior Security Consultant bei InfoGuard AG und Security-Projektleiter EMEA bei der Crypto AG. Er ist zudem Mitautor des «Sicherheitshandbuches für die Praxis» (www.sihb.ch).

Kaum zu Glauben: Über 70 Prozent der Londoner würden ihr persönliches Computerpasswort für einen Schokoriegel bekannt geben.

Bild: Pixelio

Das Grundmuster des Social-Engineerings zeigt sich in fingierten Telefonanrufen: Der Social-Engineer ruft Mitarbeiter eines Unternehmens an und gibt sich als Techniker aus, der vertrauliche Zugangsdaten benötigt, um wichtige Arbeiten abzuschliessen. Bereits im Vorfeld hat er aus öffentlich zugänglichen Quellen oder vorangegangenen gescheiterten Telefonaten kleine Informationsfetzen über Verfahrensweisen, tägliches Bürogerede und Unternehmenshierarchie zusammengetragen, die ihm für die zwischenmenschliche Manipulation helfen. Der Angreifer verwirrt sein technisch ungebildetes Opfer mit Fachjargon, baut mit Smalltalk über scheinbar gemeinsame Kollegen Sympathie auf und nutzt Autoritätsrespekt aus, indem er droht, den Vorgesetzten stören zu müssen.

Unter Umständen hat der Mitarbeiter sogar tatsächlich technische Hilfe angefordert und erwartet bereits einen derartigen Anruf. Eine bekannte und unpersönliche Variante des Social-Engineerings ist das Phishing: Fingierte E-Mails mit vertrauenswürdiger Aufmachung fordern den Empfänger auf, auf einer präparierten Webseite geheime Zugangsdaten wie Passwörter für Online-Banking preiszugeben. Das Grundmuster ist ähnlich dem fingierten Telefonanruf, denn auch hier gibt sich der Social-Engineer in der Regel als technischer Mitarbeiter aus, der zur Datenüberprüfung oder -wiederherstellung die Geheiminformation benötigt. Anders als dort verfügt der Angreifer hier über nicht viel mehr als die E-Mail-Adresse des Empfängers, was die Attacke weniger persönlich und damit auch weniger wirkungsvoll macht.

Die sechs typischen Schritte einer Social-Engineering-Attacke sind:

► Informationen beschaffen (Internet, Google, Adressverzeichnisse)
► Aufbauen eines vermeintlichen Vertrauens (Insider, Gewohnheiten)
► Gezielte Manipulation von Personen, um an die gewünschten Informationen zu gelangen (Lieferanten, Techniker, Journalist)

► Ausnutzen von menschlichen Eigenschaften, um das Opfer zu bestimmten Aktionen zu verleiten (um Hilfe fragen, Auskunft verlangen)
► Angriffe auf IT-Systeme oder Diebstahl von Daten und Passwörtern über Menschen (Bestechung, Erpressung)
► Personen ohne Fachwissen zu Sicherheitsgefährdenden Aktionen bewegen

Die Social-Engineering-Attacken werden immer raffinierter und nehmen zu. Ein gekonntes und autoritäres Auftreten mit der richtigen «Ver-Kleidung» macht es möglich. Besonders so genannte kommerzielle Spionage-Software (Spyware, Trojaner) beziehungsweise Überwachungsprogramme werden heute in Kombination mit Social-Engineering-Attacken eingesetzt. Viele dieser Spionage-Programme werden von den Antiviren-Scannern nicht erkannt. Einige Beispiele aus der Praxis: Mitlaufen mit einer Gruppe Mitarbeiter, welche das Gebäude betreten, beschäftigt telefonierend in den Aufzug marschieren und warten bis dieser von jemandem in ein oberes Stockwerk gerufen wird, beschäftigt telefonierend an anderen Zu- oder Ausgängen wartend bis jemand die Tür öffnet und diese dann für den unberechtigten Zutritt benutzt. Auch als Getränke-Lieferant getarnter Mitarbeiter kann man sich Zugang verschaffen. Oder die Variante: «Guten Tag Herr Meier, hier ist Frau Müller von der IT. Wir haben gerade ein grosses Systemproblem und brauchen unbedingt Ihre Hilfe. Wie lautet Ihr Passwort?» Oder beim Personaleingang: «Entschuldigen Sie, ich habe meinen Badge vergessen.» Ein Social-Engineer wartet in der Toilette, bis die Belegschaft in ihren wohl verdienten Feierabend geht. Und dann noch die Version des Reinigungspersonals: «Entschuldigen Sie, ich habe meine Aktenkoffer im Büro liegen gelassen und den Schlüssel im Auto.»

Erfahrungen aus der Praxis zeigen, dass Social-Engineering-Attacken sehr erfolgreich bei ungenügender Sensibilisierung der Mitarbeitenden sind. Für Passwort-Phishing per E-Mail liegt die Erfolgsquote zwischen 30 und 50 Prozent. Für Passwort-Klau per Telefon sogar 50 bis 80 Prozent. Zutritt in gesicherte Räume sind in 50 Prozent der Fälle erfolgreich.

Tipps

Seien Sie kritisch und haben Sie ein gesundes Mass an Misstrauen. Begleiten Sie eine externe Person an den Bestimmungsort. Fragen Sie eine Ihnen nicht bekannte Person freundlich nach Name, Kontaktperson und Auftrag. Alle Mitarbeiter und Besucher sollen einen Badge sichtbar tragen. Achten Sie darauf, dass Sie keine vertraulichen Dokumente auf Ihrem Arbeitsplatz unbeaufsichtigt liegen lassen (Clear Desk).

Wichtig für den IT-Bereich: Speichern Sie vertrauliche Informationen auf mobilen Geräten immer verschlüsselt ab. Transportieren Sie vertrauliche Daten nur geschützt. Senden Sie vertrauliche e-Mails nur verschlüsselt. Wählen Sie ein komplexes Passwort von mindestens acht Zeichen und behalten Sie es für sich. Sprechen Sie nie in der Öffentlichkeit (Zug, Tram, Bus, Restaurant, Raucherecke, Toilette) über geschäftsinterne und vertrauliche Angelegenheiten. Lassen Sie andere nicht mithören! Schliessen Sie keine USB-Sticks mit unbekannter Herkunft an Ihren Computer an. Schliessen Sie Ihren USB-Stick nicht an einen Ihnen unbekannten Computer an. Legen Sie keine CD-Rom ein, von der Sie nicht wissen, woher sie stammt. Installieren Sie keine Gratissoftware mit unbekannter Herkunft. Viele Gratis-Programme sind getarnte Spionage-Programme.

Zudem: Lassen Sie Notebook, Handy oder PDA nie unbeaufsichtigt. Das gilt auch für Aktentaschen oder Papier-Agenden. Lassen Sie keine vertraulichen Dokumente auf dem zentralen Drucker/Fax/Kopierer liegen. Entsorgen Sie Datenträger und vertrauliche Dokumente sicher (Schredder). Entfernen Sie nach jeder Sitzung die Skizzen und Notizen auf dem Whiteboard und entfernen Sie die Flip-Chart-Notizen.

Den wichtigsten Beitrag zur Bekämpfung von Social-Engineering-Attacken liefert das Opfer selbst, indem es Identität und Berechtigung des Ansprechenden zweifellos sicherstellt, bevor es weitere Handlungen vornimmt. Bereits die Rückfrage nach Name und Telefonnummer des Anrufers kann schlecht informierte

Angreifer enttarnen. Auch scheinbar geringfügige und nutzlose Informationen sollten Unbekannten nicht offen gelegt werden, denn sie könnten in folgenden Kontaktaufnahmen zum Aushorchen anderer missbraucht werden oder zusammen mit vielen anderen für sich genommen nutzlosen Angaben zum Abgrenzen eines grösseren Sachverhalts dienen.

Wichtig ist eine schnelle Warnung aller potenziellen weiteren Opfer; erste Ansprechpartner sind die Sicherheitsabteilung des Unternehmens, die Kontaktadresse des E-Mail-Providers und Mitmenschen und Institutionen, deren Angaben zur Vorspiegelung falscher Tatsachen missbraucht wurden.

Social-Engineering-Audit

Im Rahmen eines Social-Engineering-Audit stellt man fest, wie es um das Sicherheitsbewusstsein der Mitarbeiter steht. Durch den persönlichen Kontakt werden dem Mitarbeiter vertrauliche Informationen entlockt – meist eine User ID und ein Passwort. Der Social-Engineer als Angreifer täuscht dem Mitarbeiter eine bestimmte glaubwürdige Identität vor, um an die gewünschten Informationen zu gelangen. Ein solches Audit basiert auf den bekannten Angriffsmethoden des Social-Engineerings. Die einzelnen Angriffsarten können je nach Kundenbedürfnis beliebig kombiniert werden.

Ziele, die in einem solchen Audit verfolgt werden, sind:

► Überprüft das Sicherheitsbewusstsein der Mitarbeiter effektiv
► Erkennt Schwachstellen im Sicherheitsverständnis und Sicherheitsdispositiv
► Liefert erprobte und praxisnahe Ansätze zur Risikominimierung
► Eine wirkungsvolle Art die Effektivität einer Awareness-Kampagne zu messen. Sinnvoll ist ein Audit vor und nach der Awareness-Kampagne.

Social-Engineering-Audit in fünf Schritten:

Informationsbeschaffung und Planung: Mit dem Kunden wird ein Anforderungsprofil (Einsatzgebiet, Audit-Umfang, Vorgehen) definiert und daraus ein Drehbuch erstellt. Hintergrundinformationen sind vom Kunden und durch Recherchen vor Ort erhältlich.

Design der Werkzeuge und des Angriffsdrehbuchs: Es folgt die Ausarbeitung der benötigten Werkzeuge (E-Mails, Website) und der Aufbau der benötigten Infrastruktur für die Online-Angriffe. Anschliessend wird ein genauer Angriffsplan ausgearbeitet und mit dem Kunden abgestimmt.

Test und Abnahme: Vor dem «Audit-Ernstfall» erfolgt die Abnahme des Angriffsdrehbuchs und der entsprechenden Werkzeuge. Allfällige Korrekturen werden umgehend vorgenommen.

Durchführung des Social-Engineering-Audits: Das Audit wird gemäss dem abgestimmten Drehbuch durchgeführt.

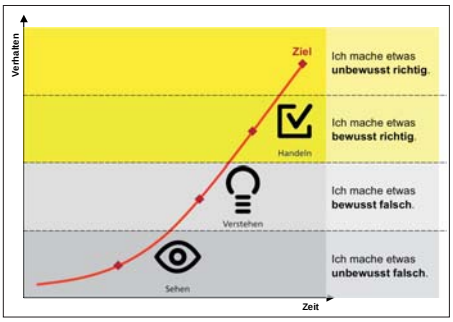
Analysierung und Dokumentierung der Ergebnisse: Alle Resultate werden ausgewertet, analysiert und in einem Bericht festgehalten. Die Erkenntnisse werden mit dem Kunden diskutiert. Thematisiert wird im Besonderen ein konkreter, praxiserprobter Sensibilisierungs-Massnahmenkatalog, um das Sicherheitsniveau unternehmensintern nachhaltig zu verbessern.

Entwicklung einer Sicherheitskultur

Wie im Strassenverkehr ist der Mensch für die Informationssicherheit von zentraler Bedeutung. Mit seinem Verhalten trägt er Verantwortung, die er nicht delegieren kann. Die Sicherheit im Strassenverkehr hängt somit wesentlich vom persönlichen, verantwortungsvollen und aufmerksamen Verhalten jedes Einzelnen ab, und davon, was Sicherheit für ihn bedeutet, beziehungsweise was er darunter versteht.

Im Vordergrund steht für die Mitarbeiter der optimalste und bequemste Weg zur Leistungserbringung. Sicherheitsmassnahmen hemmen die bekannten Abläufe und stören die Effizienz der Arbeit, so die gängige Meinung. Die Stärkung des Sicherheitsbewusstseins verbessert die Akzeptanz der Informationssicherheit und führt damit zum Wachstum der Sicherheitskultur im Unternehmen, so dass die Informationssicherheit zu einer Selbstverständlichkeit und zum Bestand-

teil der Firmenkultur wird. Es geht letztlich darum, das Verhalten der Mitarbeiter bleibend zu verändern. In Banken und Versicherungen ist dies im Bereich der physischen Sicherheit bereits seit Jahren der Fall.



Entwicklungsstufen der Sicherheitskultur (Quelle: InfoGuard AG)

Um das Sicherheitsbewusstsein der Mitarbeiter und den hohen Stellenwert der Informationssicherheit innerhalb des Unternehmens zu fördern, sollte ein umfassendes, organisationsweites Sensibilisierungsprogramm durchgeführt werden. Ziel eines solchen ist, die Informationssicherheit zu einem integrierten Bestandteil der täglichen Arbeit zu machen. Es gibt verschiedene Ansätze, wie man eine Sicherheitskultur aufbauen und prägen kann. Für einen nachhaltigen Erfolg ist in jedem Fall eine zielpublikumsorientierte Kommunikation wichtig und dass es sich dabei um einen kontinuierlichen und mehrjährigen Prozess handelt. Sensibilisierung ist eine permanente Aufgabe.

Die Entwicklung einer Sicherheitskultur kann grob in die drei Phasen «Verständnis schaffen», «Verhalten ändern» und «zur Gewohnheit werden» aufgeteilt werden. In der ersten Phase soll das Verständnis für die Thematik geschaffen werden. Die Mitarbeiter werden mit ausreichenden Hintergrundinformationen versorgt, damit sie verstehen, welche für sie relevanten Sicherheitsmassnahmen und -regelungen im Unternehmen bestehen, sowie einzuhalten sind – und vor allem wozu sie dienen. Die Kenntnis darüber allein genügt jedoch nicht. Die Mitarbeiter müssen dazu gebracht werden, im Modell die Phase zwei, das Gelernte in der Praxis auch wirklich anzuwenden.

Dies ist der eigentliche Kernpunkt einer Sicherheitskultur und damit eines Sensibilisierungsprogramms. Denn für erzwingbare Sicherheitsmassnahmen, wie beispielsweise die Badge-Nutzung für den Gebäudezutritt, benötigt es grundsätzlich keine Sensibilisierung. Dass man beim Eintritt darauf achten soll, dass nicht noch eine unberechtigte Person durch die offene Türe eintritt, hingegen schon. Ebenfalls kann man Mitarbeiter nicht dazu zwingen, ein virenverseuchtes e-Mail nicht zu öffnen. Genau in solchen Bereichen setzt ein Sensibilisierungsprogramm an.

Die dritte Phase bezweckt das automatische oder unbewusste Anwenden von Sicherheitsmassnahmen. Eine erfolgreiche Sensibilisierung führt letztendlich zu einer nachhaltigen Verhaltensänderung der Mitarbeiter. Sie müssen immer wieder mit dem Thema Informationssicherheit konfrontiert werden, damit diese zum selbstverständlichen Bestandteil der täglichen Arbeit wird. Um eine bleibende Verhaltensänderung zu bewirken, sollten die Informationen regelmässig aufgefrischt und aktualisiert werden.

Diverse Möglichkeiten der Mitarbeitersensibilisierung sind einzeln oder in Kombination denkbar. Hier sind einige Beispiele genannt: Ausbildungen, wie beispielsweise Einführungsschulung, Schulungen zu einzelnen Massnahmen, wie Virenschutz, «Clear Desk», Verhalten im Notfall, Workshops (aktive Mitarbeit), Notfallübungen, Demonstrationen oder Videos über Sicherheitsvorfälle, Computer/Web Based Training.

Weitere Massnahmen sind: Schriftliche Informationen, wie Abgabe der Sicherheitspolitik bei der Einstellung, Publikation in der Hauszeitung, Informations-CD-Rom mit Booklet inklusive einem aktuellen Viren-Scanner. Weiter: Merkblätter, Plakate, Kurznachrichten zur Erinnerung am Bildschirmschoner oder in Form von Werbeartikeln, wie Mausmatten, Tassen/Gläser, Post-it, Kugelschreiber, Schlüsselanhänger sowie Sicherheitswettbewerbe und Umfragen.

Gehör verschaffen

Da die Sicherheitskultur nicht erzwungen werden kann und Informationssicherheit immer noch als Störfaktor und Verhinderer empfunden wird und weniger als unternehmensstrategischer Erfolgsfaktor, ist es mit einer reinen Informationskampagne nicht getan. In der heutigen Informations- und Regulationsflut kann die Wichtigkeit des Themas Informationssicherheit schnell untergehen. Als ein kritischer Erfolgsfaktor hat sich in der Praxis das Erkennen der Notwendigkeit, sowie das Kennen der effektiv vorhandenen Risiken bei jedem einzelnen Mitarbeiter herauskristallisiert.

Erst wenn dies erreicht ist, werden die Sensibilisierungsinformationen bewusst aufgenommen und in korrektes Sicherheitsverhalten umgesetzt. Über das Erzeugen einer gewissen Verunsicherung kann der Mitarbeiter zur Einsicht und anschliessend zum Ziel, dem Soll-Verhalten, geführt werden. Diese Verunsicherung kann ausgelöst werden, indem beispielsweise von tatsächlichen Sicherheitsvorfällen berichtet wird oder durch Demonstration von Risiken, wie das Knacken eines Passwortes, das Fälschen eines e-Mails oder der Einfachheit einer Vireninfektion.

Weitere kritische Erfolgsfaktoren einer erfolgreichen Sensibilisierung sind:

Unterstützung durch das Management: Das Top-Management muss den Prozess spürbar und aktiv unterstützen, damit eine gute Wirkung erzielt werden kann.

Fokussierung auf das Zielpublikum: Die Sensibilisierung und die gewählte Sprache muss der Zielgruppe angepasst sein. Das Management muss beispielsweise auf eine andere Art und Weise sensibilisiert werden als die Techniker. Kunden sowie Neueintretende sind nicht zu vergessen.

Positive Aussagen: Die Aussagen und Mitteilungen sollen stets auf ein positives Ziel ausgerichtet sein. Sicherheit soll als positiv empfunden werden. Alle Informationen im Zusammenhang mit der Informationssicherheit sollen ein einheitliches und einprägsames Erscheinungsbild besitzen. Ein eigenes Logo kann hierbei gute Dienste leisten.

Geduld und Stetigkeit: Die Mitarbeiter dürfen nicht überfordert werden. Angemessenheit der Sicherheit zum Tagesgeschäft ist wichtig.

Anreizsystem: Sicherheit könnte beispielsweise ein Teil der persönlichen Leistungsbewertung mit dem Vorgesetzten beziehungsweise bonusrelevant sein.

Den Mitarbeitern soll ein allgemeines Verständnis für die Bedeutung der Sicherheit vermittelt werden. Dies führt dazu, dass Informationssicherheit als Bestandteil einer umfassenden, der so genannten integralen Sicherheit gesehen wird.

Fazit

Diverse Rezepte haben in der Praxis gezeigt, dass die Sicherheitskultur durchaus positiv beeinflusst werden kann. So genannte Aha-Effekte bei Zuhörern sind langen Erklärungen über Sinn und Zweck vorzuziehen, da sie wesentlich besser und nachhaltiger aufgenommen werden. Beispielsweise das Knacken eines Passwortes, eines Notebooks oder das Fälschen eines e-Mails während einer Sensibilisierungs-Präsentation zum Beispiel in Form eines Info-Lunch zeigen die Risiken eindrücklich auf.

Der Hinweis auf eine mögliche, ja sogar sinnvolle Nutzung der Verhaltenshinweise auch im Umgang mit dem privaten PC, erhöht die Aufmerksamkeit des Publikums merklich. So hat sich die Verknüpfung der Informationen mit privatem Nutzen als erfolgsversprechend erwiesen: Im Rahmen einer unternehmensweiten Informationssicherheit-Awareness-Aktion wurde eine CD «Vertrauen ist gut, Kontrolle ist besser! Wie Sie Ihren Home-PC schützen können» mit einem Virus-Scanner und anderen Tools inklusive Booklet mit Internet-Tipps allen Mitarbeitern abgegeben, damit sie zu Hause ihren PC sicher und kontrolliert betreiben können.

Besonders heute mit der Verwendung von USB Memory-Sticks ist das Risiko einen Virus oder andere schädliche Programme einzuschleusen sehr hoch. Das Feedback der Mitarbeiter war durchwegs positiv, zumal sie einen aktuellen Viren-Scanner mit Update-Abo und Tipps für das korrekte Verhalten im Internet kostenlos bekommen haben. Ziel ist, das Verhalten aller Mitarbeiter nachhaltig in Bezug auf die Informationssicherheit zu ändern. ■