

Running head: AWARENESS-FRAGEBOGEN FÜR UNTERNEHMEN

Ein Awareness-Fragebogen für deutsche Unternehmen

Stefan Egeler, Daniel Pandzic und Maxim Vinokurov

Ludwig-Maximilians-Universität München

Hausarbeit zum Seminar *Social Engineering in Informationssystemen*, im Sommersemester

2006 von Dr. Werner Degenhardt und Dr. Johannes Wiele veranstaltet

Verfasser:

Stefan Egeler

Matrikelnummer 2562589

Studiengang Psychologie (Diplom), 2. Semester

Daniel Pandzic

Matrikelnummer 2289108

Studiengang Psychologie (Diplom), 2. Semester

Maxim Vinokurov

Matrikelnummer 2358952

Studiengang Informatik (Diplom), 10. Semester

## Inhaltsverzeichnis

0	Abstract (Stefan Egeler, Daniel Pandzic & Maxim Vinokurov)	Seite 04
1	Einleitung (Daniel Pandzic)	Seite 05
2	Der Fragenkatalog	Seite 07
2.1	Aufbau des Fragenkatalogs (Stefan Egeler)	Seite 07
2.2	Themenblock Technik (Maxim Vinokurov)	Seite 08
2.3	Themenblock Recht und Intrusion (Stefan Egeler)	Seite 11
2.4	Themenblock Akteure, Intrusion & Engineering (Daniel Pandzic)	Seite 14
3	Wie gut eignet sich ein Fragebogen zur Schaffung von Awareness? (Maxim Vinokurov)	Seite 18
3.1	Ein 3-Schritt-Modell zur Aufrechterhaltung von Awareness (Stefan Egeler)	Seite 20
4	Zusammenfassung (Stefan Egeler, Daniel Pandzic & Maxim Vinokurov)	Seite 22
5	Literaturverzeichnis	Seite 23
6	Appendix: Fragenkatalog <sup>1</sup>	Seite 24

---

<sup>1</sup> Zusätzlich zum Fragenkatalog ist ein Beispiel des Fragebogens als letztes Blatt so angehängt, dass er ohne Umformatierungen direkt verwendet werden kann.

### Abstract

Die Autoren stellen einen für deutsche Unternehmen gestalteten Fragebogen zur Schaffung von Awareness vor. Sie diskutieren die Gestaltung und die gewünschten Auswirkungen jedes der insgesamt zwölf Items. Diese zielen vor allem darauf hin, ein vermeintliches Gefühl von Sicherheit zu erschüttern, um zu weiterem Nachdenken anzuregen. Die Autoren diskutieren außerdem die methodischen Vorzüge und Schwächen dieser Fragebogenkonstruktion, und bieten ein Modell für eine langfristig angelegte Security Awareness Kampagne an, in welcher der Fragebogen gewinnbringend genutzt werden kann.

## Einleitung

(Daniel Pandzic)

In wachsendem Maße rückt die Sensibilisierung der IT-Nutzer in den Fokus der Informationssicherheit. Zahlreiche Unternehmen haben Maßnahmen ergriffen, um ihre Mitarbeiter zu einem angemessenen Umgang mit den ihnen anvertrauten Informationen und der Informationstechnik anzuleiten und zu motivieren. Da diese Maßnahmen auf Einstellungs- und Verhaltensänderungen zielen, reichen isolierte Einzelaktionen in der Regel nicht aus – erst eine systematische Bündelung thematisch fokussierter Maßnahmen unter dem Dach einer "Security Awareness Kampagne" kann diesen Anspruch erfüllen. Fast alle bekannt gewordenen spektakulären Schäden sind von eigenen Mitarbeitern verursacht wurden, die versehentlich Schaden stiftende Software ins interne Netz einschleusten. Die Ursache solcher Sicherheitslücken ist in der Regel nicht in der Technik, sondern im oft leichtsinnigen Verhalten der IT-Nutzer zu finden.

Viele Unternehmen haben in den vergangenen Jahren intensiv in die Sensibilisierung ihrer Mitarbeiter investiert. Am wirkungsvollsten waren dabei umfassende Awareness Kampagnen, die Informationssicherheit im besten Fall als Professionalitäts- und Qualitätsmerkmal im Unternehmen zu verankern versuchten. Wichtig dabei war es, die Mitarbeiter auf unterschiedlichen Ebenen anzusprechen: Neben der sachlich-kognitiven Ebene zur Vermittlung des für die eigene Urteilsfähigkeit erforderlichen Grundwissens und der Schaffung von Verständnis für getroffene Maßnahmen und Regeln spielte die emotional-affektive Ebene eine zentrale Rolle: Durch Bilder, Videos, Trainingssoftware, Claims und Aktionszeichen wurde die Informationssicherheit emotional positiv besetzt. Mit dem von uns vorgestellten Fragebogen möchten wir Unternehmen ein potentiell effektvolles Tool an die Hand geben, das – im Gegensatz zu vielen seiner Alternativen – auch ohne größeren Aufwand zur Schaffung von Awareness einsetzbar ist.

Zudem stellt sich die Frage, wie der Erfolg von Awareness Kampagnen ermittelt werden kann. Es gibt zwei grundsätzliche Messkonzepte zur Evaluation von Sicherheitsbewusstsein, die aus der Verhaltens- und der Einstellungskomponente der Mitarbeiter resultieren: Die Beobachtung des sicherheitsbewussten Verhaltens und die Messung einer positiven Einstellung über Mitarbeiterbefragungen mit auf das Sicherheitsbewusstsein abzielenden Fragestellungen (vgl. Zerr, 2006). Der von uns vorgestellte Fragebogen hat den Vorteil, dass er über seine Eigenschaft als Awareness schaffendes Tool hinaus zur Messung der zweiten Komponente geeignet ist und damit evaluativ gebraucht werden kann; es ist mit ihm möglich, die Einstellung der Mitarbeiter vor und nach einer Kampagne zu messen und somit deren Erfolg zu ermitteln. Auf diese Weise werden Investitionen in das Sicherheitsbewusstsein „rechenbar“.

Wir stellen geeignete Fragen vor, die sich auf die technische, rechtliche und natürlich auch menschliche Ebene von Informationssicherheit beziehen und diskutieren die Gestaltung und gewünschten Auswirkungen jedes der insgesamt zwölf Items. Die Fragen sollen nicht nur Sicherheitsbewusstsein messen, sondern auch schaffen, indem der Befragte eigene Sicherheitslücken entdeckt und kritisch hinterfragt.

Über die möglichen Vorzüge und Schwächen eines Fragebogens zur Schaffung von Awareness gehen wir in der Diskussion ein. Danach stellen wir ein Modell für eine Security Awareness Kampagne vor. Uns ist bewusst, dass eine eingehende Überprüfung sowohl des Fragebogens, als auch des Modells noch ausstehen; diese war im Rahmen unserer Mittel bisher nicht möglich, und wir empfehlen sie nachdrücklich.

## Der Fragenkatalog

*Aufbau des Fragenkatalogs*

(Stefan Egeler)

Die folgenden zwölf Fragen sind in ihrem Aufbau an Katz (2005) angelehnt. Die Antwortmöglichkeiten sind, analog zu Katz:

- (a) Ich stimme völlig zu
- (b) Ich stimme zu
- (c) Ich stimme nicht zu
- (d) Ich stimme überhaupt nicht zu

Dabei haben wir diese Formulierungen auch aufgrund ihrer methodischen Vorzüge beibehalten: Die vier Antwortmöglichkeiten sind ausgeglichen und wir erwarten keinen Effekt extremer Formulierung (vgl. Stoffer, 2003). Durch die Abwesenheit einer neutralen Kategorie wird unserer Meinung nach einer vorschnellen Bejahungstendenz (vgl. Stoffer, 2003) entgegengewirkt. Aufgrund der zueinander passenden, dabei relativ extremen Antwortalternativen – (b) *ich stimme zu* und (a) *ich stimme völlig zu* anstelle von (b) *ich stimme eher zu* und (a) *ich stimme zu* – dürften die Formulierungen den Befragten zu verstärktem Nachdenken anregen.

Die bei Katz genannte Antwortalternative "(e) Not Applicable" haben wir dadurch vermieden, dass wir auf spezielle Arbeitssituationen, wie etwa in Katz' Frage 3 "I work in my own office [...]" (Katz, 2005), verzichtet haben.

Die Fragen sind durchgehend so gestellt, dass die im Bezug auf den Sicherheitsaspekt wünschenswerte Antwort (a) lautet. Dem Befragten wird dadurch das ideale Sicherheitsverhalten vor Augen geführt, was ihm die Möglichkeit gibt, sein eigenes Verhalten nachzukontrollieren. Eine zu befürchtende verstärkte Wahl dieser Möglichkeit aufgrund sozialer Erwünschtheit (vgl. Stoffer, 2003) halten wir aufgrund der Formulierung der Fragen

für eher unwahrscheinlich: Die Fragen erfordern ein intensives Nachdenken und geben dem Befragten oft die Möglichkeit, den Schuldigen (durchaus mit Recht) beim Management oder den Sicherheitsspezialisten zu sehen (etwa, weil der Befragte gar nicht ausreichend informiert wurde). Dies sollte eine eventuelle Motivation, das eigene Fehlverhalten nicht einzugestehen, einschränken.

Der Fragenkatalog ist in 12 der Reihe nach durchnummerierte Fragen aufgeteilt, die wir in drei Themenblöcke zu je vier Fragen untergliedert haben: *Technik, Recht und Intrusion*, sowie *Akteure, Intrusion und Engineering*.

#### *Themenblock Technik*

(Maxim Vinokurov)

*Frage 1: "Ich habe in der letzten Zeit mein Passwort nur verschlüsselt über das Internet/Firmennetzwerk übertragen (SFTP, SSH, Secure CVS oder POPS, IMAPS etc.)."*

Mit dieser Frage wird darauf angespielt, dass Passwörter mit einem Sniffer sehr leicht abgehört werden können. Dabei wissen die Befragten in den meisten Fällen nicht, wann eine Übertragung des Kennwortes im Klartext stattfindet.

Schon beim Einsatz von Netzwerkdiensten wie FTP, Telnet, CVS, etc. oder beim Abholen von Emails über POP und IMAP Protokolle, handelt der jeweilige Computernutzer sehr fahrlässig, denn dabei werden alle Daten, auch wenn diese als geheim oder privat eingestuft werden können, kurzzeitig im Datennetzen veröffentlicht.

Deswegen empfiehlt sich in solchen Fällen, möglichst schnell auf verschlüsselte Pendanten der genannten Dienste umzusteigen. Für das vorher angeführte Beispiel wären das die in der Frage genannten. Das im Protokollnamen zusätzlich hinzukommende "S" steht dabei meist für "Secure".

Die gestellte Frage ist nicht nur für Internetnutzer relevant. Auch in internen Firmennetzen muss darauf geachtet werden, dass die Daten nicht ungeschützt verschickt

werden. Nach einer erfolgreichen Attacke und Kontrollübernahme über einen internen Rechner oder einen Drucker mit Netzwerkfähigkeit werden nämlich in den meisten Fällen weitere elektronische Fallen im internen Netz aufgestellt, um möglichst viele Daten zu sammeln. Diese Frage spricht nicht nur Internetnutzer an, sondern auch Betreuer von Datennetzen und –diensten, denn allein der Wille des IT-Nutzers reicht alleine nicht aus, um auf sichere Alternativen umzusteigen. Dafür müssen diese zuvor installiert und angeboten werden, eventuell nicht einmal als Alternativen, sondern als einzig richtige Möglichkeit.

*Frage 2: "Ich überprüfe beim Online Banking vor der Eingabe von Kontonummer und PIN immer das Adressfeld des Browsers."*

Bei zahlreichen Spam-Mails hat es ein IT-Nutzer oft mit Fishing-Mails zu tun. Hierbei erhält der Benutzer eine täuschend echt aussende Email von einem Finanzinstitut. In der Email wird er aufgefordert, eine Internet-Seite aufzurufen und dort eine eigene Kontonummer, PIN oder TAN einzugeben. Der Link auf eine solche Seite wird dabei speziell präpariert, um dem gefälschten Internetauftritt möglichst ähnlich zu sein. Im schlimmsten Fall könnte nicht einmal ein Experte die Echtheit des Internetauftritts anzweifeln. Ein solches Szenario des Bankdatendiebstahls ist nicht sehr unwahrscheinlich, denn es erfordert keine sonderlich komplizierte technische Lösung. Deswegen bleibt oft das Adressfeld des Browser-Programms als einziges mehr oder weniger verlässliches Merkmal, anhand dessen man erkennen kann, ob der Browser sich gerade auf der Fishing-Seite befindet oder doch den originalen Internetauftritt darstellt. Die oben aufgestellte Frage bezieht sich genau auf dieses Problem und versucht, den PC-Benutzer dazu zu bewegen, vor der Eingabe wichtiger Daten in Datennetzen stets der URL der aktuellen Seite mehr Aufmerksamkeit zu schenken.

*Frage 3: "Ich antworte nicht auf per Email zugeschickte Forderungen meiner Bank zur Herausgabe persönlicher Transaktionsdaten und benutzte ebenfalls keine Software, die mir meine Bank per Email zugeschickt hat."*

Diese Frage soll den Befragten ebenfalls auf das Problem hinführen, wie leicht Bankdaten durch Fishing-Attacken gestohlen werden können. In den meisten Betrugsfällen führt die Sorglosigkeit der Bankkunden dazu, dass die Opfer ihre sensiblen Daten selbst preisgeben. Trotz häufiger Warnungen durch die Geldinstitute wird immer öfter auf Betrugsmails geantwortet. Dabei sind die Bankkunden oft sehr nachlässig. Sie zweifeln auch dann nicht an der Echtheit des Textes, wenn die Betrüger allein durch seine Dreistigkeit auffallen sollte. So werden Anforderungen beantwortet, bei denen mit der Sperrung des Kontos oder gar dem Verlust des ganzen Guthabens gedroht wird, sollten die gewünschten Informationen nicht preisgegeben werden.

Selbst wenn die gefälschte Mail der echten Mail nur darin ähnelt, dass sie das richtige Banklogo trägt, wird es oft für bare Münze genommen.

Ein weiteres Problem in diesem Kontext sind Anhänge in Fishing-Mails, die als Updates für Online-Banking Software getarnt werden. Falls sie angeklickt werden, installiert sich prompt ein Spionage-Programm, das vom Rechner unbemerkt ausgeführt wird und auf die Eingabe der Bankdaten wartet.

All das betrifft nicht nur Privatkunden. In letzter Zeit häufen sich Fälle, in denen Buchhaltungsabteilungen von Organisationen und Unternehmen derartigen Betrugsfällen zum Opfer fallen.

*Frage 4: "Ich habe die automatischen Update-Funktionen meines Betriebssystems aktiviert bzw. überprüfe selbst regelmäßig, ob neue Sicherheitspatches für von mir benutzte Computerprogramme vorliegen."*

Mit der Frage wird auf ein grundlegendes Problem eingegangen. Es handelt sich um das Problem der massenhaften Ausnutzung von Sicherheitslücken in Software-Produkten durch diverse Computer-Viren und -Würmer. Heutzutage verbessert der größte Teil der Software-Patches weniger die Programmfunktionalität oder bügelt semantische und syntaktische

Programmierfehler aus. Vielmehr werden zumeist Sicherheitsschwachstellen korrigiert. Dabei ist jedoch nicht das Eingestehen und die Korrektur von Programmierfehlern durch den jeweiligen Hersteller notwendig, sondern vielmehr das rechtzeitige Einspielen von bereitgestellten Patches. Dadurch, dass Kunden eines solchen Herstellers nicht unverzüglich die Korrekturen übernehmen, wird erst das Einnisten von Computer-Schädlingen möglich. Ignoranz vieler Anwender gegenüber Warnungen seitens der Hersteller hat beispielsweise dazu geführt, dass im August 2003 der Virus *W32.Blaster* durch rasante Verbreitung Schlagzeilen machte. Später hat diesen Erfolg ein anderer Virus namens *Sasser* wiederholt. Dabei könnten solche elektronischen Katastrophen oft allein dadurch verhindert werden, dass zumindest einige der zahlreichen Betroffenen den Patch installieren. In den beiden obigen Fällen wurde dieser etliche Wochen vor dem Computer-Virusausbruch veröffentlicht. Vor allem sollte für das rechtzeitiges Aktualisieren netzwerkfähiger Software-Produkte gesorgt werden.

Am häufigsten werden Betriebssysteme betroffen, weil sie ein hoch-komplexes Programmierprodukt darstellen, das aus mehreren Millionen Codezeilen besteht. Es gibt jedoch Fälle, in denen sich ein populäres und weit verbreitetes Tool als Träger durchsetzt, wie dies mit Apache-Webserver (etwa 60% Marktanteil) passierte, als der Computer-Wurm *Slapper* ein Sicherheitleck (das übrigens im Vormonat bereits entdeckt wurde) in einem Modul der Software ausnutzte, um sich auszubreiten.

#### *Themenblock Recht und Intrusion*

(Stefan Egeler)

*Frage 5: "Ich verlasse meinen Arbeitsplatz auch bei kurzer Abwesenheit immer so, dass keine sensiblen Daten abrufbar sind (passwortgeschützter Screensaver, Schränke abgesperrt, Büro abgesperrt)."*

Der Mensch ist das schwächste Glied in der Kette der Angriffsziele. Während technische Sicherheitslücken durch Patches, Updates und neue Versionen mit enormem Aufwand verschlossen werden, wird die Sicherheitslücke Mensch von vielen Programmierern und Technikern nicht näher betrachtet.

Diese Frage soll in diesem Sinne auf wichtige Fehler in der täglichen Routine hinweisen: Keine technische Sicherung der Welt kann verhindern, dass offenliegende Daten abgerufen werden. In Verbindung mit dem Begriff der *sensiblen Daten* wird dem IT-Nutzer aufgezeigt, dass er durch unbequeme Tätigkeiten, wie einen Screensaver mit Passwort einzurichten, einen ebensolchen Abruf von Unbefugten verhindern kann. Ebenso wird ihm dieses Verhalten als wichtig suggeriert, immerhin handelt es sich um *sensible Daten*.

*Frage 6: "Ich weiß, wie in meinem Unternehmen sensible Daten und Texte behandelt werden, und kann zu dieser Frage einiges sagen."*

Gemäß den Richtlinien des Datenschutzgesetzes muss ein Arbeitgeber unter anderem zwei Vorgaben erfüllen: Erstens muss er einen Datenschutzbeauftragten ernennen, zweitens sind persönliche Daten seiner Mitarbeiter für alle außer den direkten Bearbeitern tabu (vgl. open beware!). Zudem hat er großes Interesse daran, wenn vertrauliche Daten nicht an die Öffentlichkeit oder an Unbefugte innerhalb der Firma gelangen. Werden Mitarbeiter im Umgang mit vertraulichen Daten und Texten geschult, und arbeiten sie täglich mit solchen, ist das ein großer Schritt hin zu notwendiger Awareness, führt es den Mitarbeitern doch regelmäßig vor Augen, dass es Information gibt, die nicht einfach so weitergegeben werden dürfen. Allein die Existenz von Vertraulichkeitsklassen zeigt dabei in der alltäglichen Benutzung das Thema Sicherheit auf und hält es so im Bewusstsein.

Dieser ideale Nährboden für Awareness ist nicht in jedem Bereich jeder Firma gegeben. Dennoch haben die meisten Mitarbeiter eines Unternehmens ständig mit Information zu tun, die mehr oder minder sicherheitsrelevant ist, selbst, wenn es sich nur um Organigramme

handelt, die ein Angreifer nutzen kann, um "internes Wissen" vorzutäuschen. Idealerweise führt diese Frage zu verstärktem Nachdenken auf Seiten der Mitarbeiter und zu einigen Nachfragen bei den Sicherheitsspezialisten, welche Daten überhaupt als vertraulich gelten und wie das Unternehmen mit solchen Daten umgeht.

*Frage 7: "Ich kenne alle anderen Mitarbeiter in meinem Unternehmen und alle Zulieferer und kann deshalb Eindringlinge von hier arbeitenden Menschen unterscheiden."*

Selbst in einem Kleinunternehmen mit wenigen festen Mitarbeitern ist möglich, dass man den einen oder anderen Zulieferer noch nie gesehen hat. In einem mittelgroßen oder einem Großunternehmen ist es noch viel unwahrscheinlicher, wirklich alle Menschen zu kennen, die sich dort aufhalten dürfen. Diese Frage soll den Befragten vor Augen führen, dass sie sie eben nicht mit "Ja" beantworten können, und oftmals mit Menschen zu tun haben, von denen sie nur annehmen, dass sie Teil der Firmenstruktur sind.

Es ist durch die drei vorhergehenden Fragen auch ein Kontexteffekt (Stoffer, 2003) zu erhoffen: Der Befragte hat sich zuvor zu vertraulichen Daten Gedanken gemacht, nun geht es um Eindringlinge; das ist eine Kombination, die jeder Mitarbeiter als Bedrohung empfinden dürfte.

*Frage 8: " Ich weiß, wie ein Angreifer selbst einfache Organigramme benutzen kann, um so zu tun, als wäre er ein Mitarbeiter einer anderen Abteilung."*

Wie zu Frage 6 erwähnt, können selbst Organigramme sicherheitsrelevant sein. Ein Angreifer, der Informationen über interne Abläufe erhalten hat, kann mit diesen schnell als vermeintliches Mitglied des Unternehmens gelten – wer sonst, kann sich der Mitarbeiter fragen, kennt die Organisationsstruktur der Firma auswendig? Hier ist der Begriff des *blinden Vertrauens* bedeutsam: Ein Mitarbeiter darf und soll anderen Personen Vertrauen entgegenbringen, aber er soll sein Vertrauen zugleich durchdenken und kritisch reflektieren. Tut er das, wird ihm schnell auffallen, dass allgemeines Wissen über interne Abläufe ein nicht

schwer zu beschaffendes Gut sind und er sich nicht sicher sein kann, ob die Person, mit der er sich gerade unterhält, wirklich Mitglied des Unternehmens ist. Vorsicht ist bei einer solchen Strategie dennoch geboten: Es sollte nicht vergessen werden, dass ein übermäßiges Maß an gefühlter Bedrohung zu einem Arbeitsklima des gegenseitigen Misstrauens führen kann, das wohl kaum als wünschenswert anzusehen ist.

In Verbindung mit den beiden vorhergehenden Fragen zielt diese Frage darauf, den Mitarbeiter zu verunsichern. Die Frage, die er sich stellen soll, ist: Wenn nun Sicherheit einerseits notwendig, aber andererseits auch übertrieben werden kann, was ist dann richtig? Im komplexen Feld der Informationssicherheit ist darauf tatsächlich keine einfache Antwort zu finden. Es ist erforderlich, dass sich Menschen, die mit diesem Feld zu tun haben, eine eigene Antwort bilden. Ohne weitere Information ist dies allerdings kaum möglich. Deswegen ist einerseits darauf zu hoffen, dass der Fragebogen den Wissensdurst der Befragten aktivieren kann, andererseits auf weitere Maßnahmen zur Ausbildung von Awareness zu bauen.

*Themenblock Akteure, Intrusion & Andere*

(Daniel Pandzic)

*Frage 9: "Ich erlebe oft Situationen, in denen die Arbeit der Systemspezialisten nur durch die Mitarbeit der IT-Nutzer erfolgreich werden kann."*

Selbst wenn die Mitarbeiter in einem Unternehmen über die technischen Maßnahmen (Firewalls, Anti-Virus Programme) zur Abwehr von Hackern und anderen Angreifern informiert sind, fühlen sie sich in den meisten Fällen zu sehr in Sicherheit, was einige Studien und Befragungen gezeigt haben. Diesem zufolge gehen Arbeiter oft sehr unbedenklich mit ihrem Arbeits-PC um, was sich zum Beispiel dadurch äußert, dass 60% von ihnen persönliche Daten auf dem Arbeits-PC speichern (Gutachten von McAfee 2005). Die meisten Mitarbeiter haben folgende Einstellung: „Ach, der Systemspezialist wird es schon richten, wenn etwas

passiert. Dafür ist er ja da.“ Dies sollte so sein, aber selbst Spezialisten legen häufig zu wenig Wert auf Sicherheit, vielleicht sind sie sogar gar keine Profis, oder sie sind einfach machtlos, wenn das schwächste Glied in der Kette, nämlich der Mitarbeiter selbst, reißt. In der Frage wird sowohl auf den Systemspezialisten, als auch auf den Mitarbeiter eingegangen, da viele Personen auf beiden Seiten dazu neigen, Verantwortung abzugeben und sich als unwissend und unschuldig darzustellen. Damit soll die 9. Frage den Leser verunsichern und ihn dazu anregen, sich seiner eigenen Verantwortung dem Unternehmen gegenüber bewusst zu werden. Er sollte verstehen, dass er zwar ein kleiner, jedoch sehr wichtiger Teil der Organisation ist, unabhängig davon, ob er Fließbandarbeiter oder Abteilungsleiter ist. Er muss seine eigene Verantwortung erkennen und den Wert einer Information verstehen, um verantwortungsbewusst und eigenständig mit dem Thema Informationssicherheit umgehen zu können. Den Zusammenhang zwischen Verantwortung und Wertgefühl möchte ich in der nächsten Frage erläutern.

*Frage 10: "Wenn ich an wichtigen oder sensiblen Daten arbeite, bin ich über die Konsequenzen, die drohen, falls sie in falsche Hände geraten, angemessen informiert."*

Diese Frage greift im Sinne eines Aktualisierungseffekts (Stoffer, 2003) die Thematik der Frage 6 wieder auf, nämlich diejenige der „sensiblen Daten“. Sie soll Aufschluss darüber geben, ob die Angestellten überhaupt selbst genügend über „die Daten“ informiert wurden. Außerdem möchte ich mehr auf den Aspekt des Schadens nach einem Angriff eingehen.

Ein großes Problem, das sich in vielen Unternehmen stellt, ist, dass die Mitarbeiter sich oft nur als Befehlsempfänger fühlen. Sie werden zwar in den meisten Fällen darauf hingewiesen, dass sie sich sicher(er) zu verhalten haben, haben aber nicht immer ein angemessenes Wissen darüber, wie die ihnen zur Verfügung gestellten Daten richtig zu verstehen und zu schätzen sind.

Das allein ist jedoch noch nicht ausreichend. Ein Mitarbeiter, der weiß, wie wichtig und weshalb bestimmte Daten überhaupt wichtig ist, versteht zwar, wie er damit umzugehen hat. Trotzdem unterschätzen viele die möglichen Gefahren, auch wenn sie über diese Bescheid wissen. In den meisten bekannt gewordenen Fällen von Industriespionage wurde bevorzugt reagiert und nicht agiert. Das heißt, dass das Management erst nach einem Angriff zur Tat schritt. Zu diesem Zeitpunkt war es jedoch schon zu spät.

Um diesen Effekt zu vermeiden, wäre eine sinnvolle Awareness Maßnahme, den Angestellten von Angriffen auf andere Unternehmen zu berichten, die entweder gelungen oder abgewehrt worden sind.

Frage 10 könnte neben diesen Aspekten die Befragten auch darauf aufmerksam machen, welchen Schaden als unwichtig eingeschätzte Daten in den falschen Händen verursachen kann, ähnlich Frage 8, die am Beispiel der Organigramme eben dieses Szenario nahelegt. Viele Mitarbeiter kommen nicht auf die Idee, dass die Herausgabe einiger Telefonnummern an einen netten Anrufer, der vermeintlich vom Support ist, später einmal zu einem Desaster führen kann. Neben den enormen finanziellen Schäden muss zum Beispiel bei geknackten Netzwerkpasswörtern das ganze Netzwerk neu aufgesetzt werden, da sich dort nicht auffindbare Schadsoftware befinden kann. Kunden kündigen unter Umständen ihre Verträge auf, und es schwindet nicht nur deren Vertrauen gegenüber dem Unternehmen, sondern auch das der Mitarbeiter.

*Frage 11: "Ich kenne sowohl den Unterschied, als auch den Zusammenhang zwischen Hacking und Social Engineering."*

Diese Frage greift wohl am allgemeinsten und deutlichsten das Problem der Informationssicherheit auf. Erst seit einigen Jahren richtet sich der Fokus vermehrt von rein technischen auch auf menschliche Sicherheitslücken, wobei noch sehr viel Aufklärungsbedarf nicht nur seitens der Mitarbeiter im Unternehmen, sondern aller IT-Nutzer besteht. Gerade der

IT- Nutzer sollte aber am Meisten über die verschiedenen Angriffsarten bescheid wissen, um sich ausreichend immunisieren zu können. Die Frage soll den Leser in erster Linie auf den Zusammenhang von Angriffen auf technische und menschliche Schwachstellen hinweisen, denn Attacken von Hackern können ohne die Naivität der Opfer meist gar nicht erfolgreich durchgeführt werden. Ein Beispiel dafür sind Phishing Mails und Webseiten (vgl. Frage 2 und 3).

In dieser Frage geht es nicht primär darum herauszufinden, ob der Mitarbeiter den Unterschied zwischen Hacking und Social Engineering tatsächlich kennt, sondern sie soll ihn zum Nachdenken anregen. Er sollte selber auf einige Beispiele kommen, mit denen er wahrscheinlich täglich beim surfen im Internet konfrontiert wird. Lästige PopUps - wer kennt sie nicht - springen auf und geben vor, dass man bei irgendeiner Verlosung, bei einem Gewinnspiel oder Sonstigem gewonnen hat. Lässt man sich davon beeindruckt, so führt der Weg meist zu einem Formular, in dem man seine persönlichen Daten eintragen soll und dann nur den kleinen Submit-Button betätigen muss, um den großen Gewinn geliefert zu bekommen. Das wird höchst wahrscheinlich bei keiner dieser PopUp Meldungen der Fall sein, aber mit Sicherheit fallen viele Menschen auf solche „verlockenden Angebote“ herein (vgl. Dhamija, 2006). Erschreckend wird dabei die Vorstellung, dass sich Angreifer immer ausgefeiltere und komplexere Methoden ausdenken, um das vermeintliche Sicherheitsschloss Mensch zu knacken.

*Frage 12: "Ich kenne und erkenne einige Social Engineering Angriffsarten."*

Die meisten Leute gehen davon aus, sie könnten erkennen, wenn sie jemand manipulieren oder ihnen etwas vortäuschen will. So werden sie irgendwann einmal zu einem Opfer einer Spionageaktion, da der Social Engineer die Schwächen des Menschen auszunutzen versucht, indem er z.B. ihr Vertrauen gewinnt oder auch die kleinsten Informationsteilchen ergattert, die dem Einzelnen vielleicht gar nicht als wichtig erscheinen,

aber bei Zusammenfügen zu einem vollständigen Puzzle mit hohem Informationsgrad werden können. Hier ein paar Methoden eines Social Engineers, an denen man erkennen kann, dass für einen erfolgreichen „Angriff“ hohe schauspielerische Fähigkeiten gefragt sind:

- Vertrauensgewinnung des Opfers
  - Kommunikation im Fachjargon des Unternehmens
  - Vortäuschen eine Autoritätsperson zu sein
  - Vortäuschung von verschiedenen Stimmungslagen (hektisch, ärgerlich, freundlich)
- usw.

Um Manipulationsversuche rechtzeitig zu erkennen, ist es mit Sicherheit sinnvoll, mit einem gewissen Maß an Misstrauen nicht nur fremden, sondern gerade eben auch bekannten Personen gegenüberzutreten. Denn laut einer Studie der Unternehmensberatung KPMG stammen über 80 Prozent aller Angriffe aus dem Unternehmen selbst, doch im Gegensatz zu externen Attacken bleiben diese meist unbemerkt. Umso wichtiger ist es, dass Mitarbeiter z.B. in Seminaren lernen, manipulierendes Verhalten zu erkennen und angemessen darauf zu reagieren. Eine erfolgreiche Abwehr bei Telefonanrufen ist z.B., einfach die Nummer des Anrufers zu verlangen, um ihn zurückrufen zu können. Dieser weigert sich meistens oder erfindet irgendwelche Ausreden, womit er sich aber als Angreifer entlarvt.

Wie gut eignet sich ein Fragebogen zur Schaffung von Awareness?

(Maxim Vinokurov)

Im Laufe des Seminars sind wir auf die Idee gestoßen, dass man einen Fragenbogen für Awareness-Zwecke einsetzen kann. Folgende Punkte sprachen dafür, dass die Methode unsere Erwartungen erfüllen dürfte.

Durch das Beantworten von Fragen werden Teilnehmer an einer Awareness-Kampagne in eine Situation gebracht, in der sie sich zwangsläufig überlegen müssen, ob die

Aktionen, die täglich routiniert durchgeführt werden, mit genügend Rücksicht auf Sicherheit erledigt wurden. In dem Fragebogen sollten auch demensprechende Frage gestellt werden. Das heisst, es werden tägliche Abläufe angesprochen, die einen verantwortungsvollen Umgang benötigen und bei denen man stets kritisch sein muss. Zusätzlich werden die befragten Personen darauf hingewiesen, welche Abläufe das sind. Eventuell wird es für den einen oder anderen neu sein, das man einige der beschriebenen Situationen als gefährlich einstufen muss.

Ferner sehen wir diese Art von Awareness als eine gute Abwechslung zu anderen bereits angewendeten Methoden. Ein Fragebogen sollte vor allem nicht viel Zeit für die Bearbeitung in Anspruch nehmen und somit auch nicht langweilig sein, wie manche lange Aufklärungstexte. Es lohnt sich also weniger, wieder und wieder dieselbe Security Guidelines zum Lesen zu verteilen, die ab einer bestimmten Wiederholungsrunde wohl einfach ignoriert werden. Eine kleine und schnelle Umfrage könnte hierbei die wichtigsten Eckpunkte einer Awareness-Aktion effizienter zur Erinnerung bringen. Zielpersonen bekommen auf diese Weise gleichzeitig mehr Spielraum zum Handeln, denn in einem Fragebogen werden keine festen Regeln vorgeschrieben, wie dies in den meisten firmeneigenen Sicherheitsrichtlinien gefordert wird. Vielmehr sollte sich ein Fragenbogen auf das Sicherheitsbewusstsein der Umfrageteilnehmer auswirken und sie möglichst dazu bewegen, ihr bisheriges Handeln zu analysieren.

Es gibt natürlich auch einige Argumente, die gegen dem Einsatz von Fragebogen sprechen. Zuerst muss gesagt werden, dass bei einigen Fragen der gewünschte Lerneffekt ausbleiben kann, weil eine Frage nicht verstanden wird. Es ist auch möglich, dass Antworttendenzen aufgrund sozialer Erwünschtheit (vgl. Stoffer, 2003) nicht gewählt werden; etwa, dass man sich nicht bloßstellen möchte, indem man gesteht, zum Beispiel ein simples

Kennwort gehabt zu haben, oder, dass das eigene Passwort im Büro gerade auf einem Zettel geschrieben auf dem Monitor klebt.

Es kann auch dazu kommen, dass Awareness Eigenschaften eines Fragebogens gar nicht als solche wahrgenommen werden und dass der Fragebogen im Sinne einer Bejahungstendenz (Stoffer, 2003) einfach durchgekreuzt wird, auch, weil die meisten Befragungen dieser Art anonymisiert durchgeführt und ausgewertet werden. Deswegen sollten Awareness-Eigenschaften vorher angekündigt werden, weshalb wir dies auch in unseren Vorschlag eines Fragebogens implementiert haben.

Alles in allem fordert ein Fragebogen eine aktive Mitarbeit an der Awareness-Kampagne. Der Befragte sollte zum Nachdenken bewegt werden. Ausserdem vergeht eine solche Aktivität nicht spurlos, wenn nach der Auswertung mit einem Feedback weitere Maßnahmen begonnen werden. Wie ein solches Konzept einer allgemeinen Security Awareness Kampagne aussehen könnte, behandelt der nächste Beitrag.

#### Ein 3-Schritt-Modell zur Aufrechterhaltung von Awareness

(Stefan Egeler)

Der von uns präsentierte Fragebogen, den wir auf Basis des Fragebogens von Katz' *Security Survey* (2005) erstellt haben, dient als erste Verstärkung von Security Awareness. Technische, aber auch menschliche Schwachstellen werden dem Mitarbeiter aufgezeigt; es ist zu erwarten, dass er sich in der Folgezeit mehr Gedanken zu seinem persönlichen Sicherheitsverhalten machen wird. Soll diese Bewusstseinsänderung anhalten, ist eine nachhaltige Verstärkung notwendig. Hierzu sei folgendes Modell einer Security Awareness Kampagne vorgeschlagen.

Im ersten von drei Schritten wird der Fragebogen präsentiert. Er zeigt den Befragten grundlegende Schwächen auf und vermittelt ihnen dadurch die Notwendigkeit weiterer Maßnahmen.

Der zweite Schritt ist eine Informationsveranstaltung, in der die Inhalte des Fragebogens erläutert und vertieft werden. Die Veranstaltung findet einige Tage nach dem Fragebogen statt. Dieser Zeitabstand hat zwei Vorteile: Erstens haben die Mitarbeiter die Möglichkeit, sich selbst Gedanken zu machen, zweitens können bei der Veranstaltung sogleich die Ergebnisse präsentiert werden. Der Fragebogen ist für die Informationsveranstaltung also eine Art "Einstieg" – indem er den Befragten ihre Schwachstellen aufzeigt, wird ihnen die Notwendigkeit der Veranstaltung noch einmal vor Augen geführt. Fragebogen und Informationsveranstaltung gemeinsam demonstrieren den Mitarbeitern, dass es sich bei Sicherheitsproblemen nicht um Bagatellen handelt und verhindern, dass die vielseitigen virtuellen und menschlichen Angriffsmöglichkeiten als "Kleinjungenstreiche" oder Ähnliches in Intensität und Häufigkeit unterschätzt werden.

Der dritte Schritt schließlich ist eine nach den ersten beiden Schritten dauerhaft implementierte Phase, mit der das gewünschte Level von Awareness aufrecht erhalten wird. Nun soll der Mitarbeiter, dem die Brisanz der Thematik in der vorherigen Phase klar geworden ist, in seinem alltäglichen Verhalten am Arbeitsplatz positiv verstärkt werden. Dies wird auf zwei unterschiedliche Arten ausgeführt: Erstens wird, wie es in der Softwarefirma SAP wegweisend eingeführt wurde, bei unregelmäßigen, aber nicht zu seltenen Kontrollen nach Unsicherheitsfaktoren am Arbeitsplatz gesucht, wie sie in Frage 5 auftauchen. Die Kontrollen finden dabei außerhalb der Arbeitszeit statt. Die betroffenen Mitarbeiter erhalten einen schriftlichen Hinweis auf den Fehler, direkte Konsequenzen auf das Arbeitsverhältnis gibt es jedoch nicht. Zweitens werden in größeren Zeitabständen Scheinangriffe von dazu beauftragten externen Firmen geführt. Es ist zu beachten, dass die Scheinangriffe nicht von den Sicherheitsspezialisten selbst ausgeführt werden, da zu befürchten ist, dass dies das Verhältnis zwischen Sicherheitsspezialisten und anderen Mitarbeitern belasten könnte. Der Fragebogen wird in dieser Phase als in regelmäßigem Turnus verteiltes Evaluationsinstrument

benutzt, um den Sicherheitsspezialisten Rückmeldung über den Erfolg ihrer Tätigkeiten zu geben; zugleich ruft er den Befragten die Inhalte wieder ins Gedächtnis.

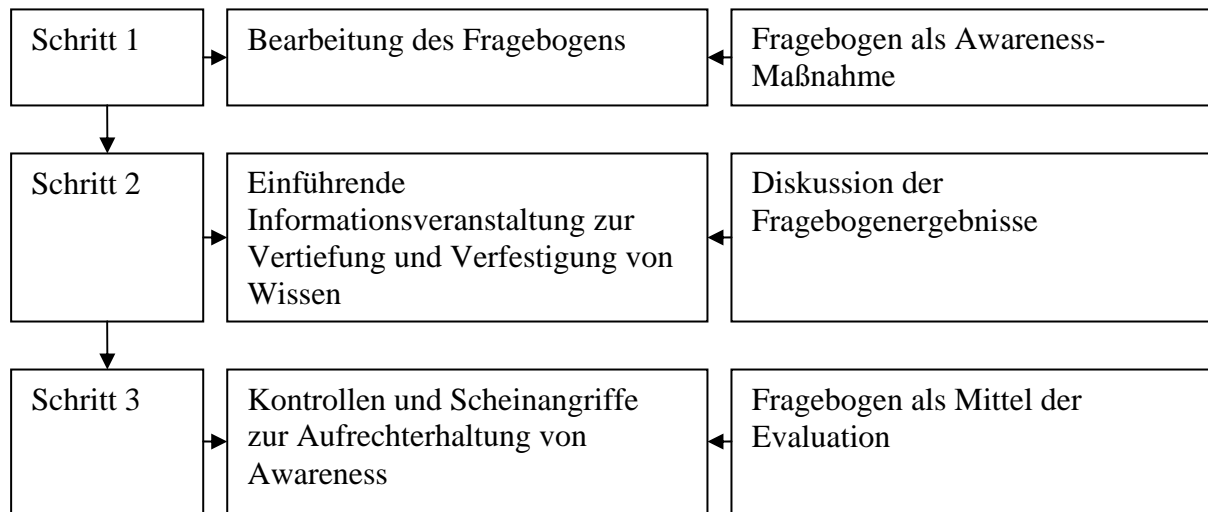


Abbildung 1: Schaubild für das 3-Schritt-Modell zur Aufrechterhaltung von Awareness

#### Zusammenfassung

(Stefan Egeler, Daniel Pandzic & Maxim Vinokurov)

Unserer Meinung nach kann ein Awareness-Fragebogen als sehr einfach durchzuführende Maßnahme einen Grundstein für Awareness legen. Wir gestalteten eine Auswahl an Items, die für diesen Zweck geeignet sein sollte und die nach methodischen Gesichtspunkten angeordnet wurde. Eine Überprüfung des Fragekatalogs steht dabei noch aus. Wir empfehlen, den Fragebogen zusammen mit weiteren Maßnahmen in ein allgemeines Awareness-Programm zu implementieren, um seine Vorzüge vollständig ausnutzen zu können.

Literaturverzeichnis

- Dhamija, Rachna (2006). *Why phishing works*, April 22-27, 2006, Montréal, Québec, Canada.
- Katz, F. H. (2005). The Effect of a University Information Security Survey on Instruction Methods in Information Security. Tagungsbeitrag von *Information Security Curriculum Development (InfoSecCD) Conference '05, September 23-24, 2005, Kennesaw, GA, USA*.
- open beware! *Security Awareness Training*. (kein Datum). Abgefragt am 8. September 2006, von <http://www.bdg.de/beware/>
- Stoffer, T. (2003). *Skript der Vorlesung "Forschungsmethoden, Teil 2: Quantitative Methoden"*. Abgefragt am 8. September 2006, von <http://www.paed.uni-muenchen.de/~allg1/lehrveranstaltungen/forschmethWS04/Skript.pdf>
- Zerr, Konrad (2006). *Security-Awarenes bei IT-Systems. Ein sozialwissenschaftlicher Ansatz zur Messung des Sicherheitsbewusstseins*.

Anhang

Fragenkatalog

Die Antwortmöglichkeiten sind:

- (a) Ich stimme völlig zu
- (b) Ich stimme zu
- (c) Ich stimme nicht zu
- (d) Ich stimme überhaupt nicht zu

Die Fragen lauten:

Frage 1: Ich habe in der letzten Zeit mein Passwort nur verschlüsselt über das Internet/Firmennetzwerk übertragen (SFTP, SSH, Secure CVS oder POPS, IMAPS etc.).

Frage 2: Ich überprüfe beim Online Banking vor der Eingabe von Kontonummer und PIN immer das Adressfeld des Browsers.

Frage 3: Ich antworte nicht auf per Email zugeschickte Forderungen meiner Bank zur Herausgabe persönlicher Transaktionsdaten und benutzte ebenfalls keine Software, die mir meine Bank per Email zugeschickt hat.

Frage 4: Ich habe die automatischen Update-Funktionen meines Betriebssystems aktiviert bzw. überprüfe selbst regelmäßig, ob neue Sicherheitspatches für von mir benutzte Computerprogramme vorliegen.

Frage 5: Ich verlasse meinen Arbeitsplatz auch bei kurzer Abwesenheit immer so, dass keine sensiblen Daten abrufbar sind (passwortgeschützter Screensaver, Schränke abgesperrt, Büro abgesperrt).

Frage 6: Ich weiß, wie in meinem Unternehmen sensible Daten und Texte behandelt werden, und kann zu dieser Frage einiges sagen.

Frage 7: Ich kenne alle anderen Mitarbeiter in meinem Unternehmen und alle Zulieferer und kann deshalb Eindringlinge von hier arbeitenden Menschen unterscheiden.

Frage 8: Ich weiß, wie ein Angreifer selbst einfache Organigramme benutzen kann, um so zu tun, als wäre er ein Mitarbeiter einer anderen Abteilung.

Frage 9: Ich erlebe oft Situationen, in denen die Arbeit der Systemspezialisten nur durch die Mitarbeit der IT-Nutzer erfolgreich werden kann.

Frage 10: Wenn ich an wichtigen oder sensiblen Daten arbeite, bin ich über die Konsequenzen, die drohen, falls sie in falsche Hände geraten, angemessen informiert.

Frage 11: Ich kenne sowohl den Unterschied, als auch den Zusammenhang zwischen Hacking und Social Engineering.

Frage 12: Ich kenne und erkenne einige Social Engineering Angriffsarten.

# Fragebogen zur Computersicherheit

Der folgende Fragenkatalog soll Ihnen dabei helfen, Ihr Wissen über sicherheitsrelevante Themen zu überprüfen und kritisch zu reflektieren. Er wird außerdem anonym ausgewertet und dient Ihrem Sicherheitspezialisten als Tool, die durchschnittlichen Sicherheitskenntnisse aller Befragten zu ermitteln.

Bitte beantworten Sie alle Fragen so ehrlich wie möglich und machen sie ein Kreuz bei derjenigen Antwort, mit der Sie Ihre Einstellung am besten repräsentiert finden.

	Ich stimme völlig zu	Ich stimme zu	Ich stimme nicht zu	Ich stimme überhaupt nicht zu
<b>Themenbereich Technik</b>				
Ich habe in der letzten Zeit mein Passwort nur verschlüsselt über das Internet/Firmennetzwerk übertragen (SFTP, SSH, Secure CVS oder POPS, IMAPS etc.).				
Ich überprüfe beim Online Banking vor der Eingabe von Kontonummer und PIN immer das Adressfeld des Browsers.				
Ich antworte nicht auf per Email zugeschickte Forderungen meiner Bank zur Herausgabe persönlicher Transaktionsdaten und benutzte ebenfalls keine Software, die mir meine Bank per Email zugeschickt hat.				
Ich habe die automatischen Update-Funktionen meines Betriebssystems aktiviert bzw. überprüfe selbst regelmäßig, ob neue Sicherheitspatches für von mir benutzte Computerprogramme vorliegen.				
<b>Themenbereich Recht und Intrusion</b>				
Ich verlasse meinen Arbeitsplatz auch bei kurzer Abwesenheit immer so, dass keine sensiblen Daten abrufbar sind (passwortgeschützter Screensaver, Schränke abgesperrt, Büro abgesperrt).				
Ich weiß, wie in meinem Unternehmen sensible Daten und Texte behandelt werden, und kann zu dieser Frage einiges sagen.				
Ich kenne alle anderen Mitarbeiter in meinem Unternehmen und alle Zulieferer und kann deshalb Eindringlinge von hier arbeitenden Menschen unterscheiden.				
Ich weiß, wie ein Angreifer selbst einfache Organigramme benutzen kann, um so zu tun, als wäre er ein Mitarbeiter einer anderen Abteilung.				
<b>Themenbereich Akteure, Intrusion &amp; Engineering</b>				
Ich erlebe oft Situationen, in denen die Arbeit der Systemspezialisten nur durch die Mitarbeit der IT-Nutzer erfolgreich werden kann.				
Wenn ich an wichtigen oder sensiblen Daten arbeite, bin ich über die Konsequenzen, die drohen, falls sie in falsche Hände geraten, angemessen informiert.				
Ich kenne sowohl den Unterschied, als auch den Zusammenhang zwischen Hacking und Social Engineering.				
Ich kenne und erkenne einige Social Engineering Angriffsarten.				