Organisationsinterne Sicherheitskommunikation

Beratungs- und Schulungsansätze

Dr. Johannes Wiele

Inhalt

Stand November 2002

1 Die Ausgangslage

Sicherheit in der Informationstechnik ist kein Zustand, sondern ein Prozess kontinuierlicher Anpassung. Er wird durch neue Entwicklungen und Bedrohungen außerhalb der Organisationen und durch Veränderungen der Kommunikationsstrukturen, Kommunikationsanforderungen sowie der technischen Infrastruktur innerhalb der Organisationen gleichermaßen in Gang gehalten. Akquisitionen und Kooperationen etwa können eine ebenso große Herausforderung an die Sicherheitsadministration darstellen wie klassische Hackerangriffe. Technik und menschliches Tun beeinflussen den Sicherheitsprozess gleichzeitig und mit der gleichen Wirkungskraft.

Eine Organisation, die ihre Sicherheit optimieren möchte, muss sich aus diesem Grund intern fortwährend über neue Bedrohungen, Risiken und Gegenmaßnahmen verständigen können. Gelingt es, funktionstüchtige Kommunikationsstrukturen und eine erfolgreiche Kommunikationspraxis einzuführen, fördert dies die Produktivität und Stabilität der jeweiligen Organisation:

- Organisationen, in denen es feste Ansprechpartner für IT-Sicherheitsfragen als Vertrauenspersonen und adäquate Informationsressourcen gibt, können ihre loyalen Mitarbeiter als interessierte Verbündete gegen externe und interne Bedrohungen der Informationssicherheit gewinnen.
- Organisationen, bei denen die interne Kommunikation über Sicherheitsfragen ein selbstverständlicher Teil der Unternehmenskultur ist, können im Krisenfall schneller und effizienter reagieren.
- Unternehmen, in denen sich Management, technische Administration und Mitarbeiter über Sicherheitsfragen verständigen, treffen eher die richtigen Investitionsentscheidungen für technische Sicherheitslösungen als Unternehmen, in denen diese Entscheidungen entweder nur vom Management oder nur von den Technikern bestimmt werden.
- Während technische Security-Lösungen überwiegend gegen bereits bekannte Angriffsformen wirksam sind, kann eine gut informierte und erfolgreich interagierende Belegschaft auch im Falle einer unerwarteten oder neuartigen Attacke sinnvolle Maßnahmen zum Schutz der IT-Infrastruktur und der gespeicherten Informationen ergreifen.
- Organisatorische und strukturelle Maßnahmen für die IT-Sicherheit kommen der Unternehmensbewertung ebenso zugute wie technische Security-Projekte.

Bisher gelingt allerdings nur den wenigsten Unternehmen der Aufbau einer angemessenen Kommunikationsstruktur für die Abwehr von Verletzungen der Informationssicherheit. Für diese Situation sind die folgenden Gründe verantwortlich.

1.1 Verständigungsprobleme zwischen Technik, Management und Anwendern

1.1.1 Kommunikationshindernisse zwischen Technikern und Management

Auf der Seite der technischen Administration:

- Management-Sprache ist nicht vertraut.
- Kein Training in der allgemeinverständlichen Präsentation technischer Lösungen
- Berichte ans Management werden als „Bürokram“ verstanden.
- Generell mangelndes Training in Kommunikationsaufgaben, die über die Grenzen der Fachabteilung hinausgehen – wie etwa das Verfassen verständlicher Sicherheitsregeln („Policies“) für Anwender ohne technisches Hintergrundwissen.
- Begrenzte Einbindung in unternehmerische Entscheidungen, die die IT-Infrastruktur beeinflussen (z.B. Merger und Akquisitionen)

Auf der Seite des Managements:

- Techniker-Sprache ist nicht vertraut.
- Begrenzte Fähigkeit zur Einschätzung moderner Sicherheitstechnik aufgrund der schnellen Entwicklung und der technischen Komplexität dieses Bereichs
- Gleichzeitig soll Sicherheit aber Chefsache sein – eine Schere, die eine vertrauensvolle und enge Zusammenarbeit mit Fachabteilungen verlangt, die bisher eher als technische Dienstleister empfunden werden.
- Angst der Chefetage, Wissenslücken zu offenbaren und sich damit Blößen zu geben
- Unwille, sich den Sicherheitsregeln des Hauses selbst zu unterwerfen
- Unsicherheit, wie man im Ernstfall über den Ernstfall sprechen sollte (Krisen-PR, Kundeninformation etc.)
- Technische IT-Sicherheit wird als Möglichkeit gesehen, schwierige organisatorische Maßnahmen und komplexe Risikoabschätzungen zu umgehen.

1.1.2 Kommunikationshindernisse zwischen technischer Administration und Endanwendern

Auf der Seite der technischen Administration:

- Information der Belegschaft / Dialog wird nicht als Teil des Aufgabengebiets gesehen („Ich muss erst einmal dafür sorgen, dass die Technik läuft“, „Ich kann mich doch nicht um jeden Dummuser kümmern“)
- Realer Zeitmangel (Zeit für kommunikative Aufgaben wird in einer klassischen Administrationsabteilung nicht eingeplant)
- Generell mangelndes Training in Kommunikationsaufgaben (s.o.)
- Angst, eigene Wissenslücken zu offenbaren (Thema IT-Sicherheit ist komplex und erfordert ständiges Lernen, so dass zwangsläufig immer wieder Informationsdefizite ausgeglichen werden müssen)
- Unverständnis für die Bedürfnisse der Endanwender (Netzverwalter sehen PCs nicht als individuelle Werkzeuge für kreative Arbeit, sondern als Knoten im Netzwerk, und verstehen Kommunikation häufig als rein technischen Vorgang)

Auf der Seite der Belegschaft:

- Kein Verständnis für die Notwendigkeit restriktiver Maßnahmen, weil technisches Wissen fehlt und Richtlinien unverständlich formuliert oder gar nicht verbreitet werden.
- Deutung von Sicherheitsmaßnahmen als Kontroll- und Zensurmaßnahmen („Die da oben trauen uns ja sowieso nicht“)
- Administratoren werden nicht als Informationsquelle / Vertrauensstelle verstanden („Die kommen sowieso nicht“, „Ich blamiere mich“, „Mit den Freaks will ich gar nichts zu tun haben, die erklären nie etwas“)
- Weil der PC ein personalisierbares Werkzeug ist, bedeuten einschränkende Eingriffe für den Anwender einen spürbaren Kontroll- und Kompetenzverlust bei der individuellen Arbeit, der in geringere Produktivität und Kreativität münden kann. Anwender sehen Kommunikation übers Netzwerk als Variante der traditionellen Kommunikation, nicht als rein technischen Vorgang.

Die aufgelisteten Verständigungsschwierigkeiten und Reibungspunkte reduzieren den Grad an Sicherheit, den eine Organisation für ihre IT-Infrastruktur und für die gespeicherten Informationen erreichen kann. Angesichts des Stellenwertes, den Informationssicherheit und Datenschutz heute in der Öffentlichkeit, aber auch bei potenziellen Part-

nern und Investoren genießen, wirkt sich das Unvermögen zur internen Kommunikation somit auf die wirtschaftliche Lage oder den Entfaltungsspielraum einer Organisation aus.

Darüber hinaus neigen Organisationen, die das Problem erkennen, aber nicht lösen können, zu unüberlegten Investitionen in immer mehr Sicherheits- und Überwachungstechnik. Das Marketing der Anbieter macht sich diesen Trend und die Unsicherheit der Anwender zunutze, um die Verkäufe anzukurbeln. Viele Organisationen erreichen deshalb keinen vernünftigen Grad an Sicherheit oder schränken die Freiheit am Arbeitsplatz so sehr ein, dass die Effektivität und Kreativität der Arbeit leidet.

2 Beratungsansatz

2.1 Kurzfristiger Ansatz

Unternehmen müssen zunächst erkennen, dass Kommunikationsprobleme im Sektor IT-Sicherheit ein Risikofaktor sind. Der Nachweis, dass in diesem Bereich Fehlinvestitionen zu befürchten sind, lässt sich argumentativ anhand der Schwierigkeiten erbringen, Sicherheitslösungen passend zu den jeweiligen Businessprozessen auszuwählen und zu implementieren. Weitere Punkte, die angesprochen werden sollten:

- Die Bedeutung des „Faktors Mensch“ in der IT-Sicherheit
- Die Gefahr von Sicherheitsverletzungen durch Fehlbedienungen, wenn Mitarbeiter unzureichend informiert sind oder Richtlinien nicht verstehen
- Die Gefahr der Gleichgültigkeit gegenüber Angriffen von innen und außen, wenn Mitarbeiter in Sicherheitsmaßnahmen nicht eingebunden sind

Da echte Wissens- und Ausbildungslücken eine große Rolle spielen, kann die Situation nicht durch ein Regelwerk oder Anweisungen allein verbessert werden. Stattdessen müssen zunächst folgende Elemente im Vordergrund stehen, die zugleich die Ad-hoc-Maßnahmen definieren:

- Klärung von Zuständigkeiten
- Aufbau einer Kommunikationsstruktur für die IT-Sicherheit
- Entwicklung einer Praxis der Sicherheitskommunikation
- Aufdecken von versteckten Potenzialen zur Verbesserung der Sicherheit

- Bildung von Sicherheitsteams, die Wissenslücken und fehlende Fähigkeiten bei einzelnen Verantwortlichen ausgleichen
- Wecken von Verständnis für die unterschiedlichen Sichtweisen der IT-Infrastrukturen bei Administration und Anwendern

Für IT-Sicherheit muss eine Person oder ein Team ausdrücklich zuständig sein. Wer diese Position einnimmt oder im Team die Aufgabe des Ansprechpartners für die Belegschaft, sollte für alle Personen in der Organisation eine Vertrauensperson sein, die außerhalb der Unternehmenshierarchie steht. Ein Mitarbeiter etwa, der befürchtet, selbst aus Unachtsamkeit zu einer Verletzung der Informationssicherheit beigetragen zu haben, sollte mit keinen negativen Konsequenzen rechnen müssen, wenn er den Vorfall mit dem IT-Sicherheitsbeauftragten bespricht.

In der Kommunikationsstruktur muss festgelegt sein, wer mit wem im Falle von Sicherheitsmaßnahmen oder im Krisenfall Kontakt aufnimmt und wo sich welche Person im Unternehmen selbst informieren kann.

Zur Praxis könnte es gehören, durch regelmäßige Maßnahmen das Sicherheitsbewusstsein zu stärken und zu erhalten. Meetings und interne Newsletter beispielsweise können dazu beitragen, dürfen aber nur zu einem gewissen Maß Routine werden.

Ein besonderes Potenzial bietet die Teambildung, für die die Beratung Anstöße geben muss. Fachleute aus dem Marketing oder der Presseabteilung etwa, die in der Aufbereitung komplexer Inhalte für Nichttechniker geübt sind und wissen, wie man für wichtige Mitteilungen Aufmerksamkeit schafft, können Technikern bei der Verbreitung und Durchsetzung von Policies und im Krisenfall zur Hand gehen.

2.2 Langfristiger Ansatz

Die Forschung stellt in verstreuten Fachgebieten durchaus konkret anwendbares Wissen für die IT-Sicherheitskommunikation bereit: Ergebnisse der Verständlichkeitsforschung und Pädagogik etwa können auf die Aufbereitung technischer Zusammenhänge für Nichttechniker bezogen werden. Die Arbeitspsychologie gibt Hinweise für die maß- und sinnvolle Anwendung und Durchsetzung von Regeln am Arbeitsplatz und liefert Modelle für Hierarchie-übergreifende Kommunikation. Die Kommunikationswissenschaft befasst sich mit der Entschärfung schwieriger Verständigungssituationen, Juristen können das Datenschutzrecht auf die korrekte Implementierung von Überwachungsmaßnahmen anwenden. Erkenntnisse zum allgemeinen Krisenmanagement lassen sich auf den Umgang mit Verletzungen der Informationssicherheit übertragen.

All diese Ressourcen stehen bereits zur Verfügung, wurden aber bisher kaum auf den Anwendungsfall „IT-Sicherheit“ bezogen und zu diesem Zweck zusammengetragen. Diese Möglichkeit sollte in Zusammenarbeit mit Hochschulen und ähnlichen Institutionen mit dem Ziel erforscht werden, die Vorschläge für eine praxisgerechte Sicherheitskommunikation in Unternehmen auf eine immer sicherere Grundlage zu stellen.

3 Schulungsansatz

3.1 Seminare für Techniker

Struktur:

Das Problem erkennen

- Dialog mit dem Management: Entscheidungsprozesse, Sprache und Denkweise, Erwartungen, Schwächen und Stärken der Gegenseite
- Dialog mit den Endanwendern: Sicht der IT-Infrastruktur als Medium „natürlicher“ Kommunikation, Erwartungshaltung an die IT-Administration, Schwächen und Stärken der Kommunikationspartner, die Folgen fehlender Richtlinien und Informationsquellen
- Rolle der Techniker aus der Sicht der anderen

Pflichten und Rechte der Administration

Berührungspunkte zum Datenschutz

Eigene Position finden

- Position zum Management: Eigenen Bedarf klar definieren. Verdeutlichen, welche Leistung die Technik für das Unternehmen erbringt. Autorität beweisen, nicht einfordern.
- Position zu den Endanwendern: Eigene Rolle erklären. Autorität beweisen, nicht einfordern. Verbündete finden. Support auf das Thema „Sicherheit“ ausdehnen.

Security-Teams bilden

- „Security-Marketing“ nach innen aufbauen
- Task Forces für den Ernstfall bilden

Klare Richtlinien schreiben

3.2 Seminare für Manager

Struktur:

Das Problem erkennen

- Dialog mit der Technik: Eigene Autorität auf Geschäftsebene zeigen, technische Autorität anerkennen, keine Angst vor Wissenslücken
- Entscheidungsprozesse für Investitionen überprüfen
- Die Rolle der Kommunikation für die Risiko-Analyse
- Unterschiedliche Sichtweisen im Unternehmen erkennen
- Die Tricks der Hersteller durchschauen

Pflichten und Rechte der Geschäftsführung

Die Bedeutung von Sicherheits-Kommunikationsstrukturen für die Unternehmensbewertung

Strategien

- Security-Wissen im Unternehmen lokalisieren
- Heterogene Teams und Task Forces fördern
- Informationsquellen schaffen
- Kommunikationsstrukturen für den Ernstfall bilden
- Die Strukturen definieren
- Weiterbildung
- Die Ergebnisse dokumentieren, Engagement honorieren

3.3 Seminare für Kommunikationswissenschaftler

Kommunikationswissenschaftler können die Problematik (Fachsprachen, Hierarchie, Psychologie) selbst leichter durchschauen als Techniker und Manager, müssten aber Grundkenntnisse in IT-Sicherheitstechnik erlernen und über die Bedeutung der IT und der IT-Sicherheit für moderne Unternehmen unterrichtet werden.

Zur Person

Studium:

- Wintersemester 1983/84 bis 1988 Germanistik, Philosophie und Politikwissenschaft mit Magister-Artium-Abschluss
- 1995/96 Promotion zum Dr. Phil. Doktorarbeit: „Vergangenheit als innere Welt. Historisches Erzählen bei E.T.A. Hoffmann.“ Europäische Hochschulschriften, Reihe I: Deutsche Sprache und Literatur. Bd. 1554. Frankfurt am Main, Berlin, Bern 1996

Berufliche Laufbahn:

- 1988-1995 Fachautor, Redakteur und Testredakteur für Computer-Fachzeitschriften sowie Autor von Handbüchern, Online-Dokumentationen und Software-integrierten Hilfesystemen
- 1995 Presales-Beratung für Microsoft
- 1996 in temporär angelegter Stellung Produktmanager für IT-Fachbücher bei Microsoft Press in München
- 1996 Buchlektor für den IT-Fachverlag bhv in Kaarst
- 1997-1998 bis zur Auflösung des Buchprogramms Lektor für IT-Fachbücher beim TLC Tewi-Verlag in München
- 1998-2000 Fachredakteur bei der Computer Reseller News in Poing, Spezialisierung auf IT-Sicherheit
- Seit 2001 Fachredakteur bei der NetworkWorld im Computerwoche Verlag. Zum Aufgabengebiet gehört die inhaltliche Planung von IT-Security-Veranstaltungen.

Buchveröffentlichungen im IT-Bereich:

- PC Tuning. Korschenbroich 1996
- Co-Autor der „Handbücher“ zu Microsoft Word 2000/2002. Unterschleißheim 2000 und 2001
- „Content-Filter als persönliche Assistenten“, in: Trust. Das Prinzip Vertrauen. Beiträge zum internationalen Kolloquium „Vertrauen. Das 21. Jahrhundert und darüber hinaus“. Herausgegeben von Mihai Nadin in Zusammenarbeit mit Lutz Becker und Thomas Eicher. Heidelberg 2001, S. 207-226

- „IT-Sicherheit als Sache des Managements“, in: NetworkWorld-Jahrbuch 2002: Kommunikationsnetze. Herausgegeben von Heiko Rössel. München 2002, S. 279-320

Links zu Fachartikeln in der NetworkWorld und Computer Reseller News:

http://www.wiele.com/johannes/articles.htm

http://www.wiele.com/johannes/oldessays.htm

Vorträge (Auszug):

- Der Linux-Markt (IBM Fachhandelskonferenz Köln 1999)
- Content Security (Euroforum Hamburg 2000)
- Filtertechnik zwischen Schutz und Zensur (Kolloquium Westfälische Wilhelms-Universität Münster 2001)
- Sicherheit verlangt Vertrauen (Novell/Azlan IT-Security-Seminar 2001)
- Aspects of the German and European Security Market (RSA Conference San Francisco 2001)
- Sicherheitstrends (NetworkWorld Netzwerktage München 2001)
- Navigating Multinational Privacy Standards (RSA Conference Europe Online 2001)
- Sicherheitskommunikation (Azlan IT-Security-Seminar 2002)
- Content Security (EICAR-Konferenz International Berlin 2002)
- Content Filtering und Content Security (Rechtsfallen für IT-Sicherheitsbeauftragte, Euroforum Freising 2002)

Sonstiges Engagement:

- Vorschlagspapier für die Überwindung von Kommunikationsproblemen bei IT-Sicherheitswarnungen an Unternehmen und andere Organisationen im Rahmen der „Cyberworld Awareness and Security Enhancement Structure“ (CASES)
- Mitarbeit am Aufbau eines Network-Forensics-Tracks für die Konferenz 2003 des „European Institute for Computer Antivirus Research“ (EICAR)
- Mitarbeit an Koordination/Moderation der Podiumsdiskussion „Die Netze der Zukunft – bedroht oder endlich sicher?“ (Kooperation NetworkWorld, EICAR, RSA Security), geplant für den 14. März 2003 während der CeBIT in Hannover

- Arbeitsgruppenleitung zum Thema Internet-Schutzsoftware während der Fachtagung „Letz netz!“ der Gleichstellungsstelle für Frauen der Landeshauptstadt München, 23.02.2003