Michael Bechtel

TÜV Media

Der IT-Sicherheitsbeauftragte als Kommunikator

TÜVRheinland
Genau. Richtig.

TÜVRheinland®
Genau. Richtig.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie. Detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-8249-1895-9

Gesamtherstellung: TÜV Media GmbH, Köln 2015

Den Inhalt dieses E-Books finden Sie auch in dem Handbuch „Information Security Management“, TÜV Media GmbH, Köln.

Der IT-Sicherheitsbeauftragte als Kommunikator

Zum Inhalt

Für den IT-Sicherheitsbeauftragten ist gute Kommunikation eine Schlüsselaufgabe. Gelingt es nicht, dessen Anliegen und Fragestellungen dem Management wie den Mitarbeitern zu vermitteln, wird eine echte Sicherheitskultur in der Organisation nicht entstehen. Dazu muss der Systembeauftragte seine Anliegen versprachlichen und mit Kommunikationsprozessen und Medien umgehen können.

Das E-Book zeigt, wie er Kommunikationsmaßnahmen, die den unterschiedlichen Zielgruppen gerecht werden, bei seiner ganzen Arbeit stets mitbedenken muss. Darüber hinaus liefert er Tipps zum professionellen Umgang mit Sprache und Texten.

Autor: Michael Bechtel
E-Mail: info@michael-bechtel.de

Ausgangslage

Der moderne Mensch akzeptiert die Technik und verwendet sie, ohne sie letztlich zu begreifen. So neigt er dazu, ihr Vertrauen entgegenzubringen – dem Auto, dem Fahrstuhl und natürlich dem Computer. Sich um Sicherheit zu kümmern ist die Aufgabe von Spezialisten. Technischen Lösungen schirmen uns vor Risiken ab. Dieses Verhalten ist gerade bei der IT nachvollziehbar. Die technischen Voraussetzungen für Angriffe aus dem Netz sind für normale Anwender kaum verständlich und nicht nachvollziehbar. Dies ist das Know-how weniger Experten, die entweder als Hacker tätig sind oder als Analysten und Programmierer die Hacker bekämpfen.

Faktor Mensch

Die IT ist aber so komplex, dass sich immer neue Sicherheitslücken ergeben, mit denen niemand rechnen kann. Da versagt technische Sicherheit, es bräuchte den sensiblen Anwender, der richtig reagiert. Doch je aufwändiger und teurer die Sicherheitstechnik, desto leichtfertiger der Anwender. Das ist beim Auto nicht anders als beim Computer, und so kommt es, dass nicht Malware-Schreiber und

Hacker für die IT-Sicherheit am gefährlichsten sind, sondern Otto Normalanwender. Gegen Malware und Hackerattacken helfen Virenschutz, Firewall, konsequentes Patching, Intrusion-Prevention-Systeme, Datenverschlüsselung und Mehrweg-Authentisierung relativ verlässlich – gegen die Kreativität und den Leichtsinn der Menschen vor dem Computer ist noch keine Soft- oder Hardware erfunden.

Falsches Verständnis

Die Sicht der Anwender auf IT Security ist geprägt durch Missverständnisse: Potenzielle Opfer sind immer die anderen, ich verfüge über keine wichtigen Daten und bin kein Angriffsziel. Hacker sind pubertierende Jugendliche, die Schabernack treiben. Alle Risikoaussagen sind übertrieben, um mehr Security-Produkte zu verkaufen. Die Security-Technik ist mächtig und wird mich gegen jede Attacke schützen.

Security Awareness ist der Schlüsselfaktor

Solange dieses Denken vorherrscht, ist jedes Bemühen um Security Awareness zum Scheitern verurteilt, weil der Einzelne keine Veranlassung sieht, sich mit IT-Sicherheit zu beschäftigen. Presseberichte sind oft zu abstrakt und an abseitigen, sensationsheischenden Beispielen aufgehängt, so dass sie das reale Bedrohungspotenzial gerade in der Geschäftswelt nicht vermitteln. Aber nur wenn allen Beteiligten die korrekte Ist-Situation bekannt ist, kann man mit Aussicht auf Erfolg Security Awareness betreiben.

Security Awareness ist so der eigentliche Schlüsselfaktor für den Erfolg der IT-Sicherheit: Die Mitarbeiter müssen Spielregeln beachten und sicherheitsbewusst arbeiten, wenn die Security-Strategie greifen soll. Dafür sorgen soll der IT-Sicherheitsbeauftragte, der – wie im Maßnahmenkatalog des IT-Grundschutz-Katalogs und in ISO 27001, Kap. 5.2.2 umrissen – die „abgestimmte IT-Sicherheitsleitlinie allen betroffenen Mitarbeitern des Unternehmens bekannt

macht“. Er hat Sensibilisierungs- und Schulungsmaßnahmen zum Thema IT-Sicherheit zu koordinieren. Dass sich hierfür der Begriff Awareness-Maßnahmen eingebürgert hat, wirft ein Licht darauf, wie weit die Verantwortlichen von den Menschen entfernt sind, um die es geht.

Man spricht nicht die Sprache der Mitarbeiter

Man spricht nicht einmal die Sprache der Mitarbeiter, deren Bewusstsein für Belange der IT-Sicherheit man schärfen, die man aktiv in die Security-Architektur einbinden möchte. Wie will man sie dann dazu bringen, IT-Sicherheit ernsthaft zu leben? Dazu braucht es eine komplexe Kommunikationsstrategie, die Zeit und Geld kostet, die, weil der Erfolg nie sofort eintritt, einen langen Atem, vor allem aber Know-how und Kompetenz in Sachen Kommunikation erfordert.

1 Sensibilisierung des Managements

Unternehmenslenker von neuen Software- oder Hardware-Investitionen zu überzeugen ist oft leichter. Fehlverhalten des eigenen Personals gilt zwar längst als eine der größten Schwachstellen der IT-Sicherheit, was sich auch in den Chefetagen herumgesprochen hat. So setzen mittlerweile 40–60 Prozent der Unternehmen auf Awareness-Maßnahmen und Schulungen – mit steigender Tendenz. Dass einmalige Schulungen oder kurzatmige Informationskampagnen kaum Einstellungs- und Verhaltensänderungen bewirken, ist Spitzenmanagern dennoch nicht unbedingt klar – ebenso wenig, dass es kontraproduktiv sein kann, allzu sehr auf Drohung mit arbeitsrechtlichen Konsequenzen zu setzen.

Treiber und Vorbilder

Die in M 3.44 beschriebene Sensibilisierung des Managements muss die Bedeutung des menschlichen Faktors in den Fokus setzen und allem anderen voranstellen. Hinreichende

Unterstützung der Leitung für den Sicherheitsprozess wird es nur geben, wo die Einsicht da ist: Langfristige Verhaltensänderungen der Mitarbeiter sind nur in einem langen und kontinuierlichen Prozess erreichbar. Und damit dies gelingt, müssen die Mitglieder der Unternehmensleitung als Treiber und Vorbilder eine große Rolle spielen.

2 Es geht um ein integriertes Kommunikationsprogramm

Jeder Mitarbeiter ist Teil des Erfolgs

Die in der Maßnahme M 2.312 „Konzeption eines Schulungs- und Sensibilisierungsprogramms zur Informationssicherheit" läuft auf ein integriertes, auf personale wie mediale Kommunikation gestütztes Kommunikationsprogramm hinaus, das durchaus Züge eines Change-Prozesses hat. Eine Sicherheitskultur muss aufgebaut und ein Sicherheitsbewusstsein gebildet werden. Jeder Mitarbeiter muss verinnerlichen, dass Informationssicherheit ein wesentlicher Teil des Erfolgs seiner Organisation ist und er persönlich nicht das schwächste Glied in der Kette sein darf.

IT-Sicherheitsbeauftragter als Kommunikator

Dazu muss der IT-Sicherheitsbeauftragte kommunizieren, warum bestimmte Sicherheitsmaßnahmen notwendig und sinnvoll sind. Er muss jedem Mitarbeiter klarmachen, was von ihm erwartet wird und wie er in sicherheitskritischen Situationen reagieren sollte. Auch wenn er nicht alles selbst machen muss, so muss er doch die Richtung vorgeben. So mancher IT-Sicherheitsbeauftragte ist darauf denkbar schlecht vorbereitet, denn IT-Fachwissen allein reicht nicht – er muss sich als Kommunikator bewähren.

3 Der naive Umgang mit dem Wort

Managen heißt kommunizieren

In den Managementtheorien und Ratgebern für die Unternehmensführung wird der Manager als der große Kommunikator beschworen. Diesen gibt es ja auch, aber meist in der Variante des raumfüllenden Alphatiers, der kommunikative Dominanz und Machtspiele perfekt beherrscht. Ansonsten verstehen Manager wenig von Kommunikation – IT-Manager bilden keine Ausnahme. Über die Grundlagen des Austauschs zwischen Menschen haben sie in Ausbildung und Berufspraxis wenig bis nichts gelernt. Und so gehen sie oft recht naiv an die Aufgabe heran, Botschaften zu formulieren darüber, was sinnvoll, notwendig oder unbedingt zu unterlassen ist. Naiv meint hier: Es herrscht das fröhliche Urvertrauen, dass Worte eindeutig sind oder sich per definitionem unmissverständlich machen lassen. Eindeutig formulierte Botschaften müssen, so die Illusion, bei jedem gutwilligen Empfänger richtig ankommen und verstanden werden.

Die Botschaft entsteht im Kopf des Empfängers

So funktioniert Kommunikation aber nicht. „Ich weiß erst was ich gesagt habe, wenn ich die Antwort höre“, sagte der Philosoph und Mathematiker Norbert Wiener. Was jemand sagen wollte oder „gemeint“ hat, ist am Ende gleichgültig. „Die Botschaft entsteht im Kopf des Empfängers“, umschreibt es der Kommunikationswissenschaftler Paul Watzlawick. Was dort aus den Worten wird, hat der Absender der Botschaft nie völlig in der Hand. Mit diesen Problemen muss sich der IT-Sicherheitsbeauftragte auseinandersetzen, da er sonst sein Kerngeschäft nicht in den Griff bekommt.

4 Wissen um kommunikative Grundlagen

Die Botschaft kommt von oben

Missverständliche Formulierungen, unverständliche Begriffe und mangelnde Erklärungen sind dabei nicht das Hauptproblem. Die in Worten klar in den Mittelpunkt gestellte wohlbegründete „Sache“ ist nicht automatisch eine Basis für Verständigung. Der Sicherheitsbeauftragte kann nicht erzwingen, dass seine Aussagen in erster Linie als Sachinformation verstanden werden. Niemals vergessen: In Unternehmen mit einer hierarchischen Kommandostruktur haben wir es in der Regel mit asymmetrischer Kommunikation zu tun. Auch freundlich und dialogorientiert formulierte Aussagen „von oben“ haben Weisungscharakter. „Die da oben wollen wieder was von uns!“ Eine aus der Befindlichkeit des Empfängers herrührende negative Grundinterpretation beeinträchtigt die Wahrnehmung von Sachaussagen.

Schließlich wollen alle Informationen aus dem IT-Sicherheitsmanagement ja auf den Empfänger Einfluss nehmen, ihn dazu bringen, etwas zu tun oder zu lassen. Wer gesagt bekommt, dass er mit seinem privaten USB-Stick vom dienstlichen Rechner wegbleiben soll, registriert erst einmal eine emotionale Botschaft: Die wollen etwas von mir, meine liebgewordenen Gewohnheiten sollen sich ändern, da kommt eine Zumutung auf mich zu.

Nichtsprachliche Signale

Eine ungeschickte Tonalität kann die ungünstigen Voraussetzungen weiter verschlechtern. In jeder Formulierung stecken neben Sachinhalten auch Informationen über den Absender. Aus der Nachricht geht hervor, wie dieser zum Empfänger steht, was er von ihm hält. Oft zeigt sich dies in der Formulierung, im Tonfall und in nichtsprachlichen Signalen. Eine Nachricht zu senden heißt immer auch, zu dem Angesprochenen eine bestimmte Art von Beziehung auszudrücken.

(„So stehen wir zueinander“). Und nicht nur Sprache, sondern jedes Verhalten zwischen Menschen hat Mitteilungscharakter, ist also im weitesten Sinne Kommunikation. Handeln oder Nichthandeln, Worte oder Schweigen beeinflussen andere, und diese können ihrerseits darauf reagieren. Damit sind sie Teil des Kommunikationsprozesses.

Was wollen wir eigentlich erreichen?

Eine Botschaft kommt, so das Fazit, eben nicht automatisch so an, wie sie gemeint ist. Dazu müssen sich beide Seiten bemühen. Unterschiedliche Standpunkte und Sichtweisen beeinflussen erheblich die Wahrnehmung und Interpretation von Botschaften. Dabei lassen sich Ursache und Wirkung nicht unterscheiden: Die Frage nach dem Anfang ist genauso unlösbar, wie das Henne-Ei-Dilemma. Je nachdem, wo der Teufelskreis durchschnitten wird, finden Schuldzuweisungen statt. Einzige Lösung: Kommunikation sollte als kreisförmig und ohne Anfang verstanden werden. Deshalb soll Metakommunikation nicht fragen, wie es zu Missverständnissen kam und wer daran schuld war; sie soll die Aufmerksamkeit auf gemeinsame Interessen lenken („Um was geht es denn eigentlich/Was wollen wir eigentlich erreichen?“). Es geht um Dialog.

5 IT leidet unter chronischer Vermittlungsinkompetenz

Weil diese Mechanismen nicht bewusst sind, ist Kommunikation die Achillesverse vieler Unternehmen nach innen wie nach außen. Im IT-Sicherheitsmanagement ist gute Kommunikation ein Schlüsselthema, mehr noch als anderswo. Die Themen sind nicht leicht zu vermitteln. Gelingt dies aber nicht, fehlt in den zu gestaltenden Prozessen zur Einführung, Realisierung und Aufrechterhaltung des Systems ein ent-

scheidendes Element: das Einverständnis derjenigen, die damit arbeiten sollen. Zudem muss der IT-Sicherheitsbeauftragte der Unternehmensleitung kontinuierlich über die Leistung des Systems sowie über Möglichkeiten, Notwendigkeiten und Methoden zur Verbesserung berichten. Auch das schafft er nur, wenn er Sinn und Notwendigkeiten eines strukturierten Sicherheitsmanagements und seiner Zumutungen für alle Beteiligten sprachlich plausibilisieren kann.

Hürden zur Nutzung der Information

Hieran scheitert es meist: Die Sprache der IT ist englisch, die der typischen Systemdokumentationen „auditorisch", d. h. auf die Normen, die Auditoren sowie auf die Erlangung des 27001-Zertifikats ausgerichtet. In der Sprache der IT-Security wimmelt es von bürokratischen Monsterbegriffen wie Anmeldeinformationsverwaltung, Dateiverschlüsselungszertifikate, Benutzerkontensteuerungsoptionen, Domänenverwaltungsinstrumente und anderen abschreckenden Wortschöpfungen. Das errichtet Hürden zur Nutzung der angebotenen Information. Viele IT-Experten sind außerstande, über Sicherheitsfragen und ihre Lösungen anders als in den Begrifflichkeiten technischer Modelle zu sprechen. Das ist wohl eine der tieferen Ursachen für die oft schwache Position des IT-Sicherheitsbeauftragten im Unternehmen: Die Sachwalter der IT-Sicherheit können sich alltagssprachlich nicht vermitteln und deshalb nicht nachhaltig überzeugen.

Langweilige, unverständliche Berichterstattung

Die Kommunikationsschwäche schlägt sich nieder in der meist langweiligen und unverständlichen Berichterstattung über IT-Sicherheit in den Mitarbeitermedien der Unternehmen: Diese lässt sich nicht dem Desinteresse oder der Unfähigkeit der CP-Redakteure anlasten. Angesichts der Komplexität und Tragweite des Themas geht es um die Bringschuld der IT-Experten, die selten in der Lage sind, ihre Themen und deren Bedeutung den professionellen

Kommunikatoren klarzumachen. Meistens sehen sie nicht einmal die Dringlichkeit dieser Aufgabe, haben sie doch auch ohne dies Arbeit genug.

Das wirkt sich nicht nur nach innen negativ aus: Es ist im Interesse des Unternehmens, mit Kunden und Partnern über Fragen der IT-Sicherheit zu sprechen, um Vertrauen zu schaffen und die Leistung weiter zu verbessern. Die Kundenanforderungen an die Sicherheit ihrer Daten gilt es in das Bewusstsein des gesamten Unternehmens zu übertragen. Dafür sollten geeignete Kommunikationsstrukturen und Informationswege eingerichtet werden, um Unsicherheiten auszuräumen, Missverständnisse zu klären und Lücken bei der Weitergabe von Informationen zu schließen.

6 Kein IT Security Management ohne Kommunikationsplanung

Kommunikation von Anfang an

Einführung, Veränderung, aber auch der Alltagsbetrieb eines IT-Sicherheitsmanagements müssen vom ersten Augenblick an von einer Kommunikationsstrategie und -planung flankiert sein. Dabei stützt sich der IT-Sicherheitsbeauftragte selbstverständlich auf Rat und praktische Unterstützung der Unternehmenskommunikation und eventuell externer Experten. Verlassen sollte er sich auf deren etablierte Instrumente und Methoden allein nicht.

Kommunikation immer mit bedenken

Im Regelkreis (Deming-Kreis) müssen die kommunikativen Anforderungen stets mitbedacht werden. Wenn der Ist-Zustand analysiert wird und die Rahmenbedingungen für das IT-Sicherheitsmanagement festgelegt werden, ist auch nach den Kommunikationsprozessen zu fragen:

- Welche sind die wichtigen und die weniger wichtigen Zielgruppen für Information und Dialog?
- Wie ist deren Bild der IT-Sicherheit? Was sind deren Fragen und Probleme?
- Welche Medien existieren? Welche Vermittlungswege müssen eventuell neu geschaffen werden?

Ohne Strategie geht nichts

Bei der Erarbeitung von Konzepten und Abläufen werden die Erkenntnisse im Idealfall in eine abgewogene Vielfalt begleitender kommunikativer Maßnahmen umgesetzt – von der Schulung über Plakate, Videos, Artikel in Mitarbeitermedien bis hin zu dialogischen Aktivitäten in internen Web-2.0-Foren. Deren Ergebnisse (Erfolge wie Misserfolge) gehören dann im Zuge der Überprüfung zu den qualitativen und quantitativen Informationen, die zu betrachten sind. Auch Annahmen über Zielgruppen, Kommunikationsziele und Medien sind auf ihren Realitätsbezug zu überprüfen, um die gewonnenen Informationen für Strukturverbesserungsmaßnahmen und Prozessoptimierung zu nutzen.

Eine Kommunikationsstrategie zu haben bedeutet: Information und Dialog bleiben nicht dem aktuellen Bedarf (sicherheitsrelevante Ereignisse, Datenpannen) oder dem Zufall überlassen – auch in einem kleineren Unternehmen.

7 Einmal ist keinmal

Kontinuität ist entscheidend

Entscheidend ist tatsächlich die Kontinuität – langfristig geplante, gut dosierte Thematisierung wichtiger Fragen der IT-Sicherheit bewirkt mehr als aufwendige Kampagnen. „Das Thema hatten wir doch schon vor drei Monaten!“ ist ein falscher Reflex. Ohne ein Mindestmaß an Redundanz dringt Information nicht durch und gerät wieder in Verges-