Die kopernikanische Wende

Informationssicherheit in der Sackgasse

Dr. Wolfgang Schnabl
www.security-awareness.at

Ein immer mehr an Technik verbessert die Informationssicherheit nur unwesentlich. Diese wird heute ausschließlich aus Unternehmenssicht gesehen; das Unternehmen steht im Mittelpunkt. Führen wir einen Perspektivenwechsel durch. Stellen wir den Menschen in den Mittelpunkt. Erklären wir dem Mitarbeiter, wie die virtuelle Welt funktioniert und wie er einen persönlichen Nutzen daraus ziehen kann. Dadurch profitieren sowohl die Unternehmen als auch wir alle.

Allgegenwärtige Informationssicherheit

Informationssicherheit ist in den letzten Jahren zum allgegenwärtigen Thema geworden. Kein Produkt, das nicht explizit seine Sicherheitsfeatures anpreist, kein IT-Konzept, das nicht mit Sicherheitsüberlegungen geplant wird, kein Unternehmen, das nicht Sicherheit als oberste Priorität verkündet.

Leben wir also inzwischen in einer durch und durch abgesicherten Geschäftswelt, der keine Störung etwas anhaben kann, die unverwundbar geworden ist? Die Realität spricht andere Worte. Tagtäglich lesen und hören wir von Sicherheitsvorfällen, die Unternehmen schwer schädigen und sogar bis in den Ruin treiben. Die Hersteller von Security-Produkten nehmen dies zum Anlass immer neue, bessere, teurere Produkte auf den Markt zu werfen. Nicht müde werdend preisen sie in bunten Marketing-Prospekten die einzigartige Überlegenheit und alleinige Glückseligmachung ihrer Erzeugnisse an. Jedes Fabrikat ein Meisterwerk, eine eierlegende Wollmilchsau [1].

Besucht man Security-Veranstaltungen oder Hersteller-Vorträge, so zeigt sich ein Bild, das mit der Wirklichkeit nicht übereinstimmt. Wir fahren mit immer schwereren Geschützen auf um im Krieg mit der tödlichen Internetwelt nicht an Boden zu verlieren. Darüber, „einen Schritt voraus zu sein“ wird gar nicht gesprochen. Wir stecken Unmengen an Geld in Hightech Geräte, die den Bedrohungen nur unbefriedigend entgegentreten. Mit dieser stetigen Spirale des Wettrüstens können wir auf lange Sicht nur verlieren. Unsere Firmen werden sich die ausufernden Sicherheitsmaßnahmen bald nicht mehr leisten können.

Realität versus Security-Weltbild

Warum klaffen Realität und Security-Weltbild derart auseinander? Warum wird die Situation nicht besser obwohl wir immer intelligentere Produkte im Einsatz haben?

Wir sind mit unserer gegenwärtigen Art, wie wir auf Sicherheitsbedrohungen reagieren, in eine Sackgasse gelaufen. Wo liegt das Problem?

Bereits 2007 schätzte Vint Cerf, "Chief Internet Evangelist" bei Google [19], am Weltwirtschaftsgipfel in Davos die Anzahl der mit Schadsoftware befallenen Rechner auf fünfundzwanzig Prozent [18]. Ein Viertel aller Rechner im Internet ist demnach mit Schadsoftware befallen und hängt in Botnetzen. Neuere Untersuchungen zeigen [14], dass die Situation schlimmer geworden ist und wir haben – offensichtlich – keine Strategie zur Besserung.

Betrachten wir die Art, wie heute Security-Konzepte für Unternehmen gemacht werden. Ein Unternehmen, das sich gegen Gefahren der virtuellen Welt absichern will, muss sich zuerst im Klaren darüber werden, wo seine Werte, materielle und immaterielle, liegen und welchen Risiken diese ausgesetzt sind. Danach

können Sicherheitsmaßnahmen getroffen werden, um die Risiken zu minimieren. Das ist die klassische Vorgehensweise, erprobt in unzähligen Implementierungen, gefordert von allen wichtigen Standards in diesem Bereich. Diese Vorgehensweise ist nicht falsch, sie geht nur am Kern des Problems vorbei.

In dieser Sicht steht das Unternehmen im Mittelpunkt, seine Prozesse, seine Produkte, sein Umsatz und Gewinn. Wir können diese Sicht mit dem ptolemäischen Weltbild der Antike vergleichen. Die Erde als Mittelpunkt unseres Universums. Wie wir heute wissen ist dieses Weltbild nicht falsch. Systeme, die durch eine Koordinatentransformation ineinander übergeführt werden können, sind, laut Einsteins Theorie, äquivalent [2]. Das heliozentrische Weltbild, propagiert und vehement von Kopernikus vertreten, ist also auch Teil dieser mathematischen Wirklichkeit. Dennoch hat die kopernikanische Wende, bei der nun die Sonne als Mittelpunkt angenommen wurde, die Wissenschaft enorm vorangetrieben und letztendlich unser ganzes Denken revolutioniert. Das ptolemäische Weltbild stieß auf schier unüberwindbare Grenzen, da die Berechnung von Ereignissen immer komplexer und schwieriger wurde.

Jedoch nicht nur die Mathematik änderte sich bei der Anpassung der Theorie. Erst dadurch, dass die Sonne in den Mittelpunkt des damaligen Universums gestellt wurde war es dem Menschen möglich, aus seinen alten Denkbahnen auszubrechen, sich selbst gleichsam „von außen“ zu betrachten. Es wurde ganz plötzlich ein anderes Bild sichtbar, ein größeres und viel monumentaleres. Immanuel Kant vergleicht in der Vorrede zur zweiten Auflage der Kritik der reinen Vernunft seine Änderung der Sichtweise in Bezug auf unsere Erkenntnis von Gegenständen mit dem Perspektivenwechsel, den Kopernikus vollzog: „Es ist hiermit ebenso, als mit den ersten Gedanken des Kopernikus bewandt, der, nachdem es mit der Erklärung der Himmelsbewegungen nicht gut fort wollte, wenn er annahm, das ganze Sternenheer drehe sich um den Zuschauer, versuchte, ob es nicht besser gelingen möchte, wenn er den Zuschauer sich drehen, und dagegen die Sterne in Ruhe ließ. In der Metaphysik kann man nun, was die Anschauung der Gegenstände betrifft, es auf ähnliche Weise versuchen.“ [5].

Grenzen des Denkens

Wenn wir uns Grenzen setzen, so können wir über diese Grenzen nicht hinaus denken. Die Grenzen sitzen im Kopf. Erst als Kopernikus diese Grenzen erweitert hatte, wurde auch das Denken über die alten Grenzen hinaus möglich. Neue Sichtweisen, neue Theorien, neue Ergebnisse waren die Folge. Die erkenntnismäßige Überwindung des geozentrischen Weltbildes führte schlussendlich zu einem fundamentalen Umdenkprozess hinsichtlich der Stellung des Menschen im Kosmos.

Unser ptolemäisches Weltbild der Informationssicherheit – das Unternehmen im Mittelpunkt – ist also nicht falsch, es beschreibt nur die Welt aus einer Sicht, die an sehr enge Grenzen stößt. Über diese Grenzen können wir nicht hinaus denken, daher kommen wir immer wieder zu denselben Lösungen. Diese erweisen sich jedoch als ineffektiv.

Mensch im Mittelpunkt

Stellen wir nicht das Unternehmen in den Mittelpunkt unserer Welt. Stellen wir den Menschen in den Mittelpunkt! Betrachten wir ein heliozentrisches Weltbild der Informationssicherheit. Was ändert sich bei dieser Betrachtungsweise? Bevor wir diese Frage beantworten können, müssen wir die aktuellen Bedrohungen in der virtuellen Welt näher untersuchen.

In immer kürzeren Abständen werden ständig neue Bedrohungen bekannt und Hersteller von Sicherheitsprodukten bieten immer neuen Schutz dagegen an. Die Sicherheit, die wir damit erreichen, ist jedoch – vor allem unter wirtschaftlichen Gesichtspunkten – kaum befriedigend. Wir erreichen keine optimale Sicherheit, denn unser System der Absicherung bekämpft lediglich die Symptome. Wir haben uns eine Art Notfallmedizin erschaffen, die schnell auf neue Gefahren, neue virtuelle Krankheiten reagieren kann. Die Ursachen der Erkrankung werden nicht beseitigt, sie werden nicht einmal betrachtet.

Unsere Security ist massiv technikgetrieben. Sicherheitsmaßnahmen zu setzen bedeutet fast immer, neue Hardware zu installieren. Unsere Security in den Unternehmen wird durch die IT-Abteilungen implementiert. Die IT-Mitarbeiter sind Techniker, die ihre Security Ausbildung durch Training on the Job erfahren. Die Security-Experten, die diese Nebenbei-Ausbildung unserer IT-Mitarbeiter durchführen, sind die Hersteller von Security-Produkten. Die Hersteller werden von den Unternehmen gerufen, wenn es Securityprobleme zu lösen gilt. Hersteller informieren die Unternehmen über neue Gefahren und beraten hinsichtlich Lösungen. Die Ausbildung unserer IT-Mitarbeiter verläuft daher äußerst einseitig in einem engen Lösungskorsett und in einem vorgefertigten Denkschema.

Wenn wir also nur einen Hammer als Werkzeug haben, warum wundern wir uns, wenn jedes Problem wie ein Nagel aussieht [17]? Techniker – in IT-Abteilungen und bei Herstellern – denken in technischen Lösungen. Wir dürfen uns also über die dargebotenen Antworten für unsere Probleme nicht wundern. Sie scheitern an den Grenzen des Denkens, der Vorstellung.

Gehen wir einen Schritt weiter, betrachten wir unter dem Phänotyp, dem Erscheinungsbild – den Symptomen – die Grundlage des Problems. Spam, Phishing, DDoS, Scareware, Erpressung, Identitätsdiebstahl und all die anderen Security-Themen sind nur Symptome einer Krankheit. Die scheinbare Ursache sind allgegenwärtige Botnetze. Mit diesen wird heute das Geschäft im Internet gemacht, diese sind für faktisch alle Betrügereien verantwortlich oder spielen dabei zumindest eine entscheidende Rolle [4].

Wer steckt hinter Botnetzen? Untersuchungen zeigen, dass es zahlreiche Botnetze gibt, die von unterschiedlichen Gruppen gesteuert werden [12]. Diese Gruppen, mafia-ähnliche Organisationen, verdienen sehr viel Geld damit. Schätzungen gehen soweit, dass mit dieser Art von Cyberkriminalität bereits mehr Umsatz gemacht wird als mit dem internationalen Drogenhandel [13].

Doch die zahlreichen Botnetze sind auch nur Symptome, sie sind nicht die eigentliche Ursache, nicht die Root Cause der Cyberkriminalität.

Root Cause der Securityprobleme

Wir selbst sind die Ursache, die Root Cause der stetig wachsenden Cyberkriminalität. Wir ermöglichen es erst, dass es Botnetze überhaupt gibt. Unsere mit Schadsoftware befallenen Rechner sind die Grundlage für organisierte Kriminalität. Ein Viertel unserer Rechner hängt in Botnetzen. Wir selbst sind für Spam, Phishing und all den anderen Betrug letztendlich verantwortlich. Die größten kriminellen Organisationen weltweit funktionieren nur, weil wir ihnen die Basis liefern, wir selbst sind die Grundsteine, das Fundament des organisierten Verbrechens. Wir sind die Ursache für die ausufernde Cyberkriminalität. Alles andere sind lediglich Symptome.

Wie sieht unsere bewährte Antwort auf dieses Problem aus? Firewall und Virenschutz auch für Heimanwender. Wir setzen wieder auf die Technikkeule.

Stellen wir uns einen Menschen vor, der an Laktoseintoleranz leidet, an Milchzuckerunverträglichkeit. Dabei kommt es zu Blähungen, Übelkeit, Erbrechen bis hin zu chronischer Müdigkeit und depressiven Verstimmungen. All das sind Symptome. Gegen jedes dieser Symptome kann der Arzt Medikamente verschreiben, die die Auswirkungen lindern. Auch hier wirkt die Technikkeule. Wir alle wissen, dass dies jedoch nicht die Lösung ist. Haben wir eine Laktoseintoleranz, so müssen wir auf milchzuckerhaltige Lebensmittel verzichten, wir müssen unsere Ernährung umstellen. Der wichtige Punkt dabei ist, dass wir selbst dies machen müssen. Wir sind gefordert, wir müssen uns der Gefahr bewusst sein und eigenverantwortlich handeln. Medikamente unterstützen uns dabei bestenfalls, sie können aber die eigene Verantwortung nicht ersetzen.

Warum ziehen wir keine Parallelen zur virtuellen Welt? Die virtuelle Welt ist in dieser Hinsicht analog zur realen Welt. Warum versuchen wir im Cyberspace alleine mit Technik alle Probleme zu lösen und ignorieren die eigene Verantwortung kategorisch?

In der virtuellen Welt tut ein Virenbefall des eigenen Rechners nicht weh, er schmerzt nicht. Waren Viren früher noch eine Plage – sie zerstörten Dateien und wichtige Daten – so sind sie heute gleichsam unsichtbar geworden. Selbst ein massiver Befall eines Rechners mit Schadsoftware fällt nicht auf. Früher wurde Schadsoftware für „Ruhm und Ehre“ geschrieben, heute geht es dabei ums reine Geldverdienen. Wird heute eine Schadsoftware am Rechner entdeckt und entfernt, so bedeutet das für den Botnetzbetreiber einen finanziellen Verlust. Jeder einzelne befallene Rechner unterstützt das Botnetz und bringt daher Einnahmen. Heutige Schadsoftware arbeitet im Verborgenen, das Geschäftsmodell hat sich geändert. Benutzer bekommen dadurch allerdings den Eindruck, dass alles in Ordnung ist.

Angriffsziel Benutzer

Die Computer-Benutzer sind inzwischen die Angriffspunkte der Crimeware Industrie geworden. Bis vor wenigen Jahren war die technische Absicherung von Rechnern in vielen Unternehmen noch mangelhaft und somit ein Einbruch über die Internetverbindung mit vergleichsweise geringem Aufwand möglich. Inzwischen hat die Sicherheitstechnik ein Niveau erreicht, bei der der Mensch wieder das schwächste Glied der Sicherheitskette geworden ist. Ein Angriff auf die Mitarbeiter ist damit wieder lukrativer und einfacher geworden, als die Technik auszuhebeln. Aus diesem Grund werden wir mit weiterer Technik unsere Sicherheit nicht mehr wesentlich erhöhen können. Das Grundproblem ist der Benutzer.

Im Jahr 2006 erschien auf der SANS Liste „Top 20 Internet Security Problems, Threats and Risks” erstmals eine nicht-technische Schwachstelle – Phishing/Spear Phishing – als eines der größten Probleme. Die beste Lösung für diese Art von Bedrohung sieht SANS in regelmäßigen Benutzerschulungen. „The most promising method of stopping spear phishing is continuous periodic exercises for all your users in which they experience safe phishing.” [10]. Die Bedrohungen werden immer weniger technisch, sie zielen immer stärker auf unbedarfte Benutzer ab.

Die Anzahl der Unternehmen, die sich bewusst sind, dass ihre Mitarbeiter der Schlüssel zur Informationssicherheit sind, steigt stetig an [6]. Sie verwenden Awareness-Maßnahmen um ihren Mitarbeitern klar zu machen, was sie dürfen und was nicht. Solche Awareness Kampagnen können in der Nomenklatur der Information Security als “Security Controls” betrachtet werden, wie sie auch in internationalen Standards zum Management für Informationssicherheit gefordert werden [3]. Das aus dem Faktor Mensch resultierende Risiko soll dadurch eliminiert, oder zumindest minimiert werden. Eine grundlegende Herausforderung bei allgemeinen Awareness Kampagnen besteht darin, dass man es bei den Mitarbeitern mit Individuen unterschiedlicher Charaktere, Erfahrung, Ausbildungsstände, mit unterschiedlichem Sicherheitsbewusstsein und -bedarf, mit unterschiedlichen Aufgaben und Rollen im Unternehmen und mit unterschiedlichem kulturellem Hintergrund zu tun hat.

Schulung durch IT-Abteilung

Awareness wird oft mit dem Begriff Schulung gleichgesetzt. Diese Awareness-Schulungen erklären üblicherweise die Richtlinien für Passwort, E-Mail, Webzugriff. Das ist natürlich nötig und sinnvoll und die Vorgehensweise verständlich. Nur, so erreichen wir keine entscheidende Steigerung der Informationssicherheit.

Eine große Hürde bei der Durchführung von Schulungen ist auch der Vortragende selbst. Meist wird für Policy-Schulungen, die gleichzeitig als Awareness-Schulungen verkauft werden, die interne IT-Abteilung herangezogen. IT-Administratoren haben tagtäglich mit den Gefahren der virtuellen Welt zu tun und verstehen daher die Probleme besser als jeder Anwender. Der Schluss liegt nahe, den eigenen IT-Administrator als Security Experten auf die Benutzer loszulassen. Die Idee hinter dieser Maßnahme mag legitim sein, sie bewirkt jedoch häufig das Gegenteil des gewünschten Effekts. IT ist für den Standard-Benutzer eine andere Welt, IT verwendet eine andere Sprache. Auch Ärzte, Juristen, Chemiker und viele andere Berufe verwenden ihre eigene Sprache, haben ihren eigenen Jargon. Außenstehenden fällt es daher

meist schwer dem roten Faden einer Diskussion zwischen zwei Experten überhaupt folgen zu können. Der IT-Administrator mag noch so beschlagen und motiviert sein, er erreicht den Zuhörer nicht.

„Gedacht heißt nicht immer gesagt, gesagt heißt nicht immer richtig gehört, gehört heißt nicht immer richtig verstanden, verstanden heißt nicht immer einverstanden, einverstanden heißt nicht immer angewendet, angewendet heißt noch lange nicht beibehalten." Diese Aussage, die Konrad Lorenz gerne zitierte, trifft auch auf die Versuche der IT zu, dem gewöhnlichen Benutzer Bedrohungsbilder und Sicherheitslösungen zu vermitteln.

In der Kommunikation kommt es nicht darauf an, was der Vortragende spricht, sondern darauf, was der Zuhörer versteht. Walther Umstätter definiert als eine Prämisse für erfolgreiche Kommunikation, dass der Sender einer Nachricht den gleichen Zeichensatz zur Informationsübertragung benutzt wie der Empfänger [15]. Dies trifft jedoch bei Mitarbeiterschulungen durch die IT-Abteilung nicht zu. Statt Verstehen der Gefahren und Probleme, statt Akzeptanz für implementierte Lösungen, statt Aufmerksamkeit und Vorsicht im Umgang mit Computern entstehen Frust und Desinteresse.

Inhaltliche Vollständigkeit bedeutet keineswegs eine Erhöhung der Sensibilisierung für die vorgetragenen Themen. Es bedeutet auch nicht, dass eine Verhaltensänderung angestoßen wurde. Eine Verhaltensänderung, eine Änderung der Unternehmenskultur, ist jedoch eine zwingende Voraussetzung für Nachhaltigkeit. Die IT-Abteilung eines Unternehmens ist also der denkbar schlechteste Lehrmeister um Awareness-Schulungen durchzuführen.

Das National Institute of Standards and Technology definiert zudem recht deutlich, wie sich Schulung von allgemeiner Awareness unterscheidet. "Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly." [20]. Eine Awareness-Schulung wird auch aus diesem Grund ins Leere gehen, es fehlt den Teilnehmern die Grundlage um für den dargebotenen Stoff prinzipiell aufnahmefähig zu sein.

Aber nicht nur Schulungen sind das Problem. Selbst Unternehmen, die gut konzipierte und professionell begleitete Kampagnen durchführen, erzielen damit nicht den gewünschten Effekt. Das Sicherheitsniveau erhöht sich zwar, bleibt dennoch meist hinter den – hoch gesteckten – Erwartungen zurück [11].

Der Grund dafür ist, dass auch bei solchen Kampagnen wieder das Unternehmen im Mittelpunkt steht. Security-Spiele, Security-Preisausschreiben, Security-Screensaver sind alles Maßnahmen, die nur scheinbar den Menschen als Mittelpunkt sehen. Bei all diesen Effekten geht es für den Mitarbeiter hauptsächlich um das „Zuckerl", jedoch kaum jemals um den fachlichen Inhalt. Aus diesem Grund greifen Awareness Maßnahmen nicht oder liefern nur minimale Erfolge.

Die tiefenpsychologische Studie „Entsicherung am Arbeitsplatz" [7] nähert sich einigen Gründen des beschriebenen Bildes. Sie untersucht auf wissenschaftlicher Grundlage die psychologischen Faktoren der IT-Security und versucht die Ursache unverständlicher Phänomene (Entsicherung) zu klären.

Ein wichtiges Ergebnis für Sicherheitsverantwortliche im Unternehmen und Personen, die Awareness-Kampagnen planen ist sicherlich die Kernaussage der Studie: „Ein 100-prozentig dichtes Unternehmen ist [für den Mitarbeiter] seelisch nicht auszuhalten. […] Unternehmen, die immer weniger rein und auch immer weniger raus lassen, minimieren ihre Entwicklungschancen und die Ihrer Mitarbeiter. Arbeit, die sich – nicht zuletzt durch technologische Innovationen – immer sachlicher gestaltet und immer weniger Eigenes bzw. Menschliches zulässt, erscheint leblos und fade. […] Es kommt zu Ausbrüchen, die dem Prinzip des Menschlichen Eröffnens folgen, eine Notlösung, bei der die Mitarbeiter die bereits fortgeschrittene entmenschlichte Sachlichkeit nicht länger aushalten können. Exakt an dieser Schnittstelle lassen sich in Unternehmen die meisten der so genannten Fehlleistungen identifizieren, bei dem die Mitarbeiter sich und ihr Umfeld entsichern."

Je stärker die Mitarbeiter zu einer sachlich-verschlossenen Haltung genötigt werden, umso stärker wird beispielsweise das Passwort zum Symbol der Aufgabe eigener Identität. „Ausbrüche" äußern sich dann

etwa in der bewussten Verwendung unsicherer Passworte, welche Wünsche, Hoffnungen oder einfach nur positiv Erlebtes widerspiegeln. Zu starke und sachliche IT-Security wird mit dem Verlust der eigenen Identität verbunden. Es gelingt dadurch den Unternehmen heute kaum noch, den menschlichen Faktor zu integrieren.

Das Unternehmen steht im Mittelpunkt, die Sensibilisierung trifft die Menschen nicht, sie betrifft sie nicht. Wir frönen dem ptolemäischem Weltbild. Wie können wir diese besorgniserregende Realität ändern?

Heliozentrisches Weltbild

Stellen wir den Menschen in den Mittelpunkt. Gehen wir auf die Bedürfnisse der Menschen ein. Zeigen wir ihnen die Welt da draußen, die virtuelle Welt. Zeigen wir ihnen die Vorteile, aber auch die Nachteile. Sprechen wir mit ihnen über den Nutzen, den sie persönlich daraus ziehen können, und über die Gefahren.

Die Maslow'sche Bedürfnispyramide [9] gilt nicht nur für die physische Welt, sie hat für den Menschen auch in der virtuellen Welt Bedeutung. Gerade die Defizitbedürfnisse „Sicherheit" und „Soziale Bedürfnisse" der unteren Pyramiden-Schichten sind von essentiellem Einfluss auf das Wohlbefinden im Cyberspace.

Online Banking, Amazon, eBay, Facebook, Twitter, Picasa, Google – das bewegt die Menschen, das ist ihr tägliches Leben. Information darüber, wie sie dieses Online-Leben sicher gestalten können, befriedigt grundlegende Bedürfnisse. Hier steht der Mensch ganz und gar im Mittelpunkt. Die Folge ist, dass Veranstaltungen zu diesen Themen ungeteilte Aufmerksamkeit bei den Zuhörern bewirken. Daraus entwickelt sich Verständnis für die Gefahren und Bedrohungen, aber auch für die Lösungen und Schutzmaßnahmen. Dementsprechend ändern die Menschen ihr Online-Verhalten.

Wird im privaten Umfeld das Online-Verhalten bewusster und sicherer, so wirkt sich das zwangsläufig auch auf das Firmenumfeld aus, in dem die betreffende Person arbeitet. Unsichere und unwissende Mitarbeiter werden zu mündigen Partnern im Kampf gegen Cyberkriminalität; ganz ohne Zwang, ganz ohne Anweisungen.

Persönliche Betroffenheit ist der Schlüssel zum Erfolg. Verstehen alleine reicht nicht, Awareness Kampagnen werden weiterhin ins Leere laufen, wenn es nicht gelingt die Zuhörer zu motivieren. Dies erreicht man weder durch Zwangsteilnahme an Veranstaltungen noch durch unterstützende Preisausschreiben. Dies gelingt nur durch das Aufzeigen eines persönlichen Nutzens für den Teilnehmer, für den Menschen.

Im heutigen Umfeld der Sozialen Netzwerke und Blogs verschwimmen die Grenzen zwischen Arbeit und Privatleben. Mitarbeiter verkünden Firmeninternes in Freundschaftsnetzen, sie posten auf privaten Blogs – das Wort „dooced" aus dem gleichnamigen Blog von Heather Armstrong wird inzwischen als Bezeichnung für eine Person verwendet, die auf Grund ihres Blogs gekündigt wurde [16]. Auch unbeabsichtigte Preisgabe von vertraulichen Daten wird zum globalen Problem für jedes Unternehmen, wie der designierte MI6 Chef selbst erfahren musste, als seine Frau private Fotos auf Facebook online stellte [8].

Unternehmen, die diese Vorfälle ernst nehmen und daraus lernen, werden ihre Mitarbeiter in den Mittelpunkt von Awareness-Kampagnen stellen, sie werden den Mitarbeitern erklären, wie sie sich sicher im Cyberspace bewegen können. Firmen die verstehen, dass sich der Perimeter des Unternehmens immer weiter auflöst, dass „innen" und „außen" immer weniger zu unterscheiden sind, werden die eigenen Mitarbeiter bei ihren Sicherheitsüberlegungen an zentrale Stelle stellen.

Aber nicht nur das Bedürfnis nach der eigenen virtuellen Sicherheit ist zu befriedigen. Gehen wir noch einen Schritt weiter. Beziehen wir das soziale Umfeld des Mitarbeiters mit ein. Eine „sichere" Familie, Partner und Kinder, Freunde und Verwandte mit eingeschlossen, ist ein Anliegen für den Mitarbeiter. Erklären wir auch seinem Lebenspartner wie er sicher im Internet einkauft. Erklären wir dem besorgten Vater, was er zu tun hat, damit sich sein Sprössling sicher im Internet bewegen kann.

Titel von Vorträgen könnten etwa sein: „Einkaufen im Internet – aber sicher!“, „Facebook, Twitter & Co. – aber sicher!“, „Heim-PC verwenden – aber sicher!“, „Jugendliche im Internet – aber sicher!“.

Bisher achten wir nicht auf die Mitarbeiter, sie sind unpersönliche Teilnehmer bei Security Schulungen, die von den Unternehmen – in bester Absicht – durchgeführt werden. Nehmen wir uns der Mitarbeiter als eine eigenständig denkende Person an, stellen wir den Mitarbeiter in den Mittelpunkt. Durch Veranstaltungen, die den persönlichen Nutzen in den Vordergrund stellen, wird dem Mitarbeiter klar, warum im Unternehmen bestimmte Regeln bezüglich Informationssicherheit gelten. Sicherheitsregeln werden daher plötzlich ohne Zwang eingehalten – denn, nur was der Mensch versteht, befolgt er auch. Kurzfristig profitieren dadurch vor allem die Unternehmen, die diese Veranstaltungen ihren Mitarbeitern anbieten.

Langfristig profitieren wir alle davon. Firmenumfeld und privates Umfeld sind immer weniger zu trennen. Durch eine wachsende Anzahl an sicherheitsbewussten Menschen sinkt die Anzahl an infizierten Rechnern, wodurch die Zahl der Botnetze zurückgeht. Es sinkt die Zahl der Angriffe und dadurch flaut die Zahl der Betrugsfälle ab.

Umdenkprozess

Informationssicherheit ist in eine Sackgasse geraten. Ein immer größeres Arsenal an technischen Sicherheitsprodukten bringt nicht die erwartete Steigerung an Sicherheit. Um aus dieser Sackgasse herauszukommen, benötigen wir einen grundlegenden Umdenkprozess. Unsere unternehmenszentrierte Sicht lässt uns stets den gleichen Lösungswegen folgen. Stellen wir den Menschen in den Mittelpunkt unserer Sicherheitsüberlegungen, so ist es uns durch den veränderten Blickwinkel möglich, in alternativen Bahnen zu denken.

Unsere Wertschöpfung in Unternehmen basiert auf unseren Mitarbeitern. Verstehen die Mitarbeiter die virtuelle Welt nicht, weder Nutzen noch Gefahren, so werden sie jegliche Vorschriften unbeabsichtigt ignorieren.

Security-Produkte Hersteller denken in technischen Lösungen, IT-Mitarbeiter denken in technischen Lösungen. Beide Gruppen sprechen eine Sprache, die von Mitarbeitern nicht verstanden wird. Sie sind denkbar schlechte Ansprechpartner um Awareness Veranstaltungen durchzuführen.

Awareness Veranstaltungen sind auch vergeblich, wenn dabei den Teilnehmern kein persönlicher Mehrwert geboten wird. Bieten wir den Mitarbeitern und auch deren Angehörigen und Freunden persönliche Weiterbildung zu aktuellen Sicherheits-Themen des Cyberspace an. Facebook, Twitter und Co. bestimmen das Leben der Menschen. Zeigen wir ihnen ihren ganz persönlichen Nutzen. Wir alle werden davon profitieren.

[1] vgl: Eierlegende Wollmilchsau, in: http://de.wikipedia.org/wiki/Eierlegende_Wollmilchsau, 9. Juni 2010
[2] vgl: HOYLE, Fred, in: Nicolaus Copernicus, London 1973
[3] vgl: ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems –Requirements, Control A.8.2.2, 2005
[4] vgl: KAMLUK, Vitaly, Botnetze - Geschäfte mit Zombies, in: http://www.viruslist.com/de/analysis?pubid=200883611, 13. Mai 2005
[5] KANT, Immanuel, Kritik der reinen Vernunft (2nd Edition), in: BOUILLON, Gerd, http://www.gutenberg.org/catalog/world/readfile?fk_files=8384&pageno=6, August 2004
[6] vgl: KLEESTORFER, Dr. Klaus, Capgemini Studie IT-Trends 2009, Abb. 23: Security – Geplante Projekte, in: http://www.at.capgemini.com/m/at/tl/IT_Trends_2009.pdf, 2009
[7] Known-Sense, „Entsicherung am Arbeitsplatz“, Studie, 2006
[8] vgl: LEWIS, Jason, MI6 chief blows his cover as wife's Facebook account reveals family holidays, in: http://www.mailonsunday.co.uk/news/article-1197562/MI6-chief-blows-cover-wifes-Facebook-account-reveals-family-holidays-showbiz-friends-links-David-Irving.html, 5. Juli 2009

[9] vgl: MASLOW, Abraham, Maslowsche Bedürfnispyramide, in: http://de.wikipedia.org/wiki/Maslowsche_Bedürfnispyramide, 1943
[10] SANS Institute, Users (Phishing/Spear Phishing). How to Prevent Phishing Attacks, in: http://www.sans.org/top20/2006/#h2, 15. November 2006
[11] vgl: Securitymanager, in: http://www.securitymanager.de/magazin/artikel_1499_security_awareness_symposium_2007.html, Juni 2007
[12] vgl: STEWART, Joe, Top Spam Botnets Exposed , in: http://www.secureworks.com/research/threats/topbotnets, 8. April 2008
[13] vgl: SULLIVAN, Dan, McAfee CEO: Cybercrime Bigger Than Drug Trade , in: http://www.realtime-websecurity.com/market_news_and_trends/2007/09/mcafee_ceo_cybercrime_bigger_t.html, 19. September 2007
[14] vgl: Trend Micro, The Internet Infestation, How Bad Is It Really?, in: http://blog.trendmicro.com/the-internet-infestation-how-bad-is-it-really/, 16. September 2009
[15] UMSTÄTTER, Walther, Die Skalierung von Information, Wissen und Literatur, in: http://www.ib.hu-berlin.de/~wumsta/pub67.html, 1992
[16] vgl: WATERS, Darren, Pick of the blogs: Dooce , in: http://news.bbc.co.uk/2/hi/entertainment/4659469.stm#dooce, 20. Juli 2005
[17] vgl: WATZLAWICK, Paul, in: http://www.paulwatzlawick.de/ 9. Juni 2010
[18] vgl: WEBER, Tim, Criminals 'may overwhelm the web', in: http://news.bbc.co.uk/2/hi/business/6298641.stm, 25. Jänner 2007
[19] vgl: WILKENS, Andreas, Vint Cerf wird "Chief Internet Evangelist" bei Google, in: http://www.heise.de/newsticker/meldung/Vint-Cerf-wird-Chief-Internet-Evangelist-bei-Google-129019.html, 08. September 2005
[20] WILSON, Mark und HASH, Joan, NIST SP - 800-50 - Building an Information Technology Security Awareness and Training Program, 2.2 Awareness, in: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=151287, Oktober 2003