KARIN SCHULER

Von der Kenntnis zur Erkenntnis

Dass die größte Gefahr für die Datensicherheit in Unternehmen nicht etwa von Hackern, Datendieben und Spionen ausgeht, sondern von – in der Regel durchaus wohlmeinenden – Mitarbeitern, ist keine neue Erkenntnis. ›Awareness‹-Programme setzen genau dort an.

Es ist Montagmorgen *in einem mittelständischen Unternehmen, genau 8.30 Uhr: Der Pförtner Michael Klein sitzt im Foyer des Unternehmens hinter seiner Theke und beobachtet die hereinkommenden Beschäftigten. Er hat ein ausgesprochen gutes Namensgedächtnis und kennt viele der Kolleginnen und Kollegen mit Namen. Zwischen den vertrauten Gesichtern sieht er einen unbekannten Herrn im schwarzen Anzug. Er tritt an die Theke, stellt sich vor und möchte Herrn Maier, den Chef der EDV sprechen, mit dem er einen Termin vereinbart habe. Normalerweise werden die seltenen Besucher vom jeweiligen ›Gastgeber‹ im Foyer abgeholt, aber in der EDV-Leitung wird ständig telefoniert. Inzwischen ist der angegebene Termin schon um fünf Minuten überzogen. Schließlich erklärt der Pförtner dem Gast, um ihn nicht noch länger warten zu lassen, den recht einfachen Weg zur EDV-Abteilung und schickt ihn alleine auf die Reise. Eine halbe Stunde später verlässt der elegante Herr das Haus bereits wieder, wie Michael Klein leicht erstaunt feststellt – diesmal mit einem großen Paket unter dem Arm. Nun, der Termin hat wohl nur der Abholung von Unterlagen oder Ähnlichem gedient …*

Ein paar Unternehmen weiter hat sich Heike Müller am Morgen trotz einer lästigen Erkältung ins Büro geschleppt, weil der Monatsabschluss unbedingt fertig werden muss, die Kollegin aber ebenfalls krank ist und im Bett liegt. Da stürzt nach nur einer Stunde Arbeit an Tabellen und Auswertungen ohne Vorwarnung der PC ab. Zum Glück hat Heike Müller ihre Arbeitsergebnisse regelmäßig gesichert. Nur: Ein Neustart bringt zunächst nicht gewünschten Erfolg. Ein Anruf bei der Hotline ergibt, dass das Netzwerk wegen eines Stromausfalls kurzzeitig nicht verfügbar ist, in einer Viertelstunde aber wieder bereit sein wird. Tatsächlich ist nach der angekündigten Zeitspanne die Arbeit wieder möglich, so dass Frau Müller erleichtert ihre Arbeit fortsetzen kann. Merkwürdig nur, dass es während des ganzen Tages immer wieder kleine Störungen gibt, insbesondere sind die Reaktionszeiten stark verzögert.

Kurz nach der Mittagspause ist Heike Müller froh, dass sie mit ihrer Arbeit langsam zum Ende kommt. Da klingelt das Telefon und am anderen Ende meldet sich einer der Hotline-Administratoren, um ihr von zu erwartenden Schwierigkeiten im Netzwerk zu berichten. Er bittet sie, sich kurzzeitig abzumelden um ihre Arbeitsergebnisse nicht zu gefährden. Erschreckt meldet sich Heike Müller noch während des Telefonats aus dem Netzwerk ab. Der Administrator erklärt ihr weiter, dass er für Sicherungs- und Reparaturarbeiten direkt auf ihren Account zugreifen müsse, weshalb er sie um ihr Passwort bittet. Frau Müller zweifelt wegen der morgendlichen Störung nicht an der Wichtigkeit der Reparaturarbeiten und teilt ihr Passwort mit, um ihren mühsam erstellten Monatsabschluss keinesfalls zu gefährden …

Sicherheitsprobleme – wer ist schuld?

Was ist diesen beiden Szenarien gemein? Nun, Eines ahnt man schon: Sie gehen beide nicht gut aus. Und in der Tat: im ersten Fall wird später rekonstruiert, dass der elegante Gast keineswegs den EDV-Chef besucht hat. Vielmehr hat er sich in einem nicht belegten, abgelegenen Besprechungsraum mithilfe eines mitgebrachten Laptops und über die dort vorhandenen Netzwerkdosen Zugang zum Unternehmensnetzwerk verschafft und – vermutlich mithilfe eines ›Sniffers‹ – den Netzwerkverkehr ›abgehört‹. Umfang und Art seiner ›Beute‹ lassen sich nicht ermitteln. Die einzige gegenständliche Beute war der im Besprechungsraum stehende ›Beamer‹ – das Paket, das dem Pförtner sogar aufgefallen war.

Im zweiten Fall kann sich Frau Müller nach Ablauf einer halben Stunde immer noch nicht wieder (wie vom Administrator versprochen) im Netzwerk anmelden und erhält stattdessen immer wieder Fehlermeldungen, die behaupten, dass sie ein falsches Passwort benutze. Als sie schließlich noch einmal die Hotline anruft, um sich nach dem weiteren Verlauf der Reparaturarbeiten zu erkundigen, stellt sich heraus, dass niemand derartige Arbeiten nach Beseitigung der morgendlichen Netzwerkprobleme vorgenommen hat. Auch ein Administrator habe nicht bei ihr angerufen – und schon gar nicht nach ihrem Passwort gefragt.

Eine schnellstens eingeleitete Prüfung ergibt, dass der vermeintliche Administrator vermutlich eine Schwachstelle innerhalb des Firmennetzwerks ausgenutzt hat um sich ins Netzwerk einzuschleichen und dann höchst bequem mit Frau Müllers umfangreicher Netzwerkbe-

rechtigung über eine halbe Stunde lang streng vertrauliche Daten eingesehen – und vermutlich auch kopiert – hat. Außerdem sind die Zahlen des Monatsabschlusses verfälscht und müssen vollkommen neu berechnet werden ...

Eine weitere Gemeinsamkeit der Szenarien: Beide Firmen haben recht umfangreiche Datenschutz- und IT-Sicherheits-Richtlinien entwickelt, deren Beachtung für alle Beschäftigten verpflichtend ist. In diesen Richtlinien findet man selbstverständlich Besucherregelungen, die die Begleitung von Gästen durch das Haus vorsehen und eine Bestimmung, die die Weitergabe von Passworten – gleich an wen – strikt untersagen.

Die Schuldigen sind also klar und man könnte es sich einfach machen, den Pförtner und die Sachbearbeiterin wegen ihres jeweiligen Fehlverhaltens abmahnen und dann zur Tagesordnung übergehen – bis zum nächsten gleichartigen Fall ...

Wo liegen die wirklichen Ursachen?

Variationen derartiger ›Unglücke‹ gibt es unzählige und aller Erfahrung nach (und gestützt durch diverse Studien zum Sicherheitsbewusstsein in Unternehmen) wird eine vergleichbare Situation vermutlich überall und recht bald wieder eintreten.

Warum ist das so? Sind Beschäftigte nicht willens, die Datenschutz- und Sicherheitsrichtlinien ihres Unternehmens einzuhalten? Warum hat Herr Klein den ›Gast des EDV-Chefs‹ ohne Begleitung ins Haus gelassen? Und warum hat Frau Müller ihr Passwort herausgerückt, obwohl sie selbst ihrer Kollegin immer wieder sagt, dass man auf keinen Fall das Passwort auf einem Zettel unter der Tastatur verwahren darf?

In Herrn Kleins Fall war eine der Ursachen sicherlich seine im Hause allgemein bekannte und geschätzte Hilfsbereitschaft. Er ist als Pförtner und Hausverwalter immer bemüht, flexibel nach Problemlösungen zu suchen. Viele Kolleginnen und Kollegen wenden sich daher an ihn, wenn es um die Beschaffung einer Pinwand, die Suche nach einem Besprechungsraum oder ähnliche organisatorische Vorgänge geht. Dass Herr Klein bei diesen kleinen ›Notfällen‹ freundlich hilft, wird von der Geschäftsleitung ausdrücklich begrüßt.

Leider ist ihm seine Hilfsbereitschaft in diesem Falle zum Verhängnis geworden. Der Wunsch, dem Gast nicht als bürokratischer Torhüter zu erscheinen und ihn nicht über den vereinbarten Termin hinaus an der Pforte festzuhalten, hat den Ausschlag für sein sicherheitswidriges Verhalten gegeben. Herr Klein hat nicht aus Unkenntnis oder Böswilligkeit die Sicherheitsrichtlinie verletzt, sondern weil er unter dem Druck stand, helfen zu wollen. Ein menschlich eigentlich sehr wünschenswertes Verhalten.

Ähnlich menschlich – und ähnlich problematisch – hat sich Frau Müller verhalten. Trotz ihrer Krankheit hat sie sich aus Pflichtbewusstsein in die Firma begeben, um den Monatsabschluss nicht zu gefährden. In ihrem angeschlagenen Zustand hat sie der Netzwerkausfall besonders hart getroffen und den erhofften Feierabend weiter hinausgezögert. Als der Anruf des vermeintlichen Administrators ihr weitere Datenverluste ›androhte‹, tat sie deshalb alles, was aus ihrer Sicht eine weitere Komplikation vermeiden konnte.

Das abstrakte Verbot der Passwortweitergabe trat in diesem Fall ganz in den Hintergrund, denn der Anruf passte so gut ›ins Bild‹ der vorhergegangenen Ereignisse, dass die Möglichkeit eines Missbrauchs ihr gar nicht in den Sinn kam.

Aus der Analyse dieser und ähnlich gelagerter Fälle lassen sich einige typische Probleme erkennen:

- Richtlinien sind unerlässlich, um Datenschutz- und Sicherheitsstandards eindeutig und transparent festzuschreiben. Umgekehrt sichert ihre bloße Existenz jedoch nicht, dass sie den Mitarbeitern auch bekannt sind – und schon gar nicht ihre Einhaltung.
- Selbst Beschäftigte, die sich in der Regel zuverlässig an Richtlinien halten, erleben Situationen, in denen sie Datenschutzregeln oder Sicherheitsgrundsätze verletzen, ohne sich dessen unmittelbar bewusst zu sein.
- Darüber hinaus gibt es meist eine Reihe von Beschäftigten oder auch Externen, die von der Existenz der Datenschutz- und IKT-Sicherheitsrichtlinien gar nicht, noch nicht oder nur vage gehört haben – oder bestenfalls einzelne Regelungen eher zufällig kennen gelernt haben.
- Datenschutz- und IKT-Sicherheitsrichtlinien eilt meist der Ruf voraus, kompliziert, realitätsfern und lästig zu sein: So muss man sich beispielsweise ständig neue Passworte merken, obwohl die eigenen Daten »doch gar nicht so wichtig sind«. Mögliche schädliche Auswirkungen eigenen Verhaltens werden häufig unterschätzt.
- Nicht wenige Unternehmen erreichen durch eine zentrale Datenschutz- oder

Sicherheitsorganisation, dass das Thema ›in guten Händen‹ – und zwar in denen der ›Zuständigen‹ – zu sein scheint. Dass die Zuständigkeit für die Umsetzung von Datenschutz und IKT-Sicherheit bei jedem und jeder Einzelnen liegt, gerät dabei in Vergessenheit.

- Die Realität ist oft nicht frei von Zielkonflikten (z.B. Hilfsbereitschaft gegen Sicherheit), die im Extremfall sogar durch widerstreitende Anforderungen aus unterschiedlichen Richtlinien erzeugt werden können. Die Abwägung im Einzelfall muss durch den betroffenen Beschäftigten meist sehr spontan durchgeführt werden.

Jedes der skizzierten Probleme beschreibt auf die eine oder andere Weise, dass es in Unternehmen ›menschelt‹. Die Arbeit wird eben (glücklicherweise) nicht von maschinenhaft agierenden Wesen nach den Vorgaben unzähliger Richtlinien erledigt, sondern von Menschen mit Vorlieben, Schwächen, unterschiedlicher Tagesform und verschiedenen Interessenslagen.

Richtlinien und schriftlich fixierte Regelwerke müssen jedoch sehr abstrakt ›die Beschäftigten‹, ›die Nutzer‹ oder ›die Administratoren‹ ansprechen und können den beschriebenen menschlichen Faktor nur wenig einbeziehen.

Awareness – der Name ist Programm

Es ist daher sehr zu begrüßen, dass zunehmend nach Wegen gesucht wird, wie man den Beschäftigten den Sinn der aufgestellten Regeln verdeutlichen und ihnen ihre Wichtigkeit ans Herz legen kann.

Inzwischen hat sich auch ein Name für konzentrierte Bemühungen um die Sensibilisierung der Beschäftigten in IKT-Sicherheitsfragen durchgesetzt: ›Awareness‹-Programm. Hinter diesem Wortungetüm verbirgt sich der Versuch, über einen längeren Zeitraum durch aufeinander abgestimmte Aktionen das Bewusstsein (= Awareness) der Beschäftigten so zu schärfen, dass eine möglichst hohe Sensibilität für Sicherheits- und/oder Datenschutzfragen entsteht.

Letztlich soll ein hohes Schutzbewusstsein möglichst aller Beschäftigten für ein insgesamt hohes Schutzniveau des Unternehmens sorgen, getreu dem Motto: Die Kette ist nur so stark wie ihr schwächstes Glied. Dahinter steckt die Idee, dass Menschen, die den Sinn der Ihnen abverlangten Handlungsweisen verstehen und ihre eigene Verantwortung erkennen, zuverlässiger richtig handeln, als wenn sie ›nur‹ blind den Regeln folgen sollen. Das Ziel der Bemühungen innerhalb eines Awareness-Programms sollte also Erkenntnis (und nicht die bloße Kenntnis der Regeln) über Gefährdungen und den Zusammenhang mit eigenen Verhaltensweisen sein.

Soweit die Theorie ... Aber: Was verbirgt sich konkret hinter einem solchen Programm?

Mit vielen Aktionen an die Öffentlichkeit

In der Regel wird man den Start einer Awareness-Kampagne (wie das Vorhaben auch manchmal genannt wird) zu einem möglichst betriebsöffentlichen Ereignis werden lassen. Dies kann durch eine Veranstaltung, eine Bekanntmachung, eine Plakataktion oder Ähnliches geschehen. In dieser Phase sollte bereits erkennbar werden, dass ein breites Bündnis betrieblicher Akteure das Vorhaben unterstützt – wenn möglich gleichermaßen die Unternehmensleitung, der Betriebsrat, der betriebliche Datenschutzbeauftragte, der IKT-Sicherheitsbeauftragte und die EDV-Abteilung. Aber auch die für Unternehmenskommunikation oder Marketing zuständigen Abteilungen können zur Unterstützung hinzugezogen werden (Stichwort: Corporate Identity ⊡→).

Es folgen dann – über die Laufzeit des Programms verteilt – unterschiedlichste Aktionen. Je nachdem welche Datenschutz- oder IKT-Sicherheitsanforderungen im Unternehmen besonderer Aufmerksamkeit bedürfen, liegt die veranschlagte Zeitspanne zwischen sechs Monaten und zwei Jahren. Die Aktionen reichen beispielsweise von informierenden Intranet-Seiten ⊡→, Intranet-Lernprogrammen, Merkzetteln über Arbeitshilfen, Bildschirmschonern, regelmäßigen Veröffentlichungen in der Unternehmenszeitschrift bis hin zu Preisausschreiben, Live-Hacking-Vorführungen ⊡→ und der Einrichtung einer Sprechstunde des ›PC-Doktors‹ für die Privat-Computer der Beschäftigten. Der Phantasie sind bei der Entwicklung und Auswahl bewusstseinsbildender Maßnahmen sind kaum Grenzen gesetzt.

Bei der Auswahl und Gestaltung der einzelnen Aktionen sollten allerdings einige grundlegende Erfahrungswerte beachtet werden:

- Häufige, kleinere Aktionen sind effektiver als seltene, große Aktivitäten. Die Themen Datenschutz und IKT-Sicherheit müssen vor allem ›im Gespräch bleiben‹.
- Eher theoretisch orientierte Aktionen (z.B. die Vermittlung von Hintergrundinformationen) sollten sich mit solchen mit höherem Spaßfaktor abwechseln (z.B. ein Quiz zu Sicherheitsfragen). Das Verhältnis von Theorie und praktischen Tipps sollte ausgewogen sein.
- Das Interesse der Beschäftigten sollte auch durch einen über den dienstlichen Alltag hinausgehenden ›Mehrwert‹ geweckt werden (z.B. indem auch Tipps für den Schutz des privaten Rechners gegeben werden). Das resultierende Verantwortungsbewusstsein kommt in jedem Fall dem Unternehmen zugute.
- Die Attraktivität größerer Informationsveranstaltungen kann gut durch ›spektakuläre Einlagen‹ erhöht werden (z.B. durch Vorführen von ›Passwort-Sniffing‹ ⊡→ oder ›Live-Hacking‹)
- Die Aktionen sollten möglichst auch betriebsgruppenbezogene Anteile enthalten (z.B. spezielle Datenschutz-Tipps für die Personalabteilung oder das Call-Center).
- Die Abfolge der Aktionen sollte eine inhaltliche Steigerung beinhalten, das heißt, die Themen sollten sich vom Allgemeinen zum Besonderen entwickeln und der Schwierigkeitsgrad der behandelten Themen sollte über die Laufzeit allmählich erhöht werden.
- Mit einem Symbol, einem Logo oder Kampagnenkennzeichen werden Wiedererkennungseffekte gefördert. Dies darf dann auch auf Bildschirmscho-

nern, Mausmatten oder Baseball-Kappen auftauchen.
- Und schließlich: Die Aktionen dürfen Spaß machen!

Eine Chance auch für den Betriebsrat!

So wichtig derartige Sensibilisierungskampagnen für das Unternehmen sind, so sehr stellen sie auch eine Chance für den Betriebsrat dar. Am besten sollte er selbst die Initiative ergreifen und ein derartiges Programm vorschlagen.

Warum das? Nun, allzu häufig leiden Betriebsräte unter ihrem Image im Betrieb: dass sie nämlich gerade im Bereich moderner Techniknutzung als Verhinderer, Bedenkenträger und manchmal sogar als ›Spaßbremser‹ wahrgenommen werden. Auch wenn diese Etikettierung oftmals ungerechtfertigt ist und aus politisch unlauteren Gründen vorgenommen wird, so erschwert sie doch die Arbeit und frustriert die Betriebsratsmitglieder. Insbesondere wenn die Vorwürfe nicht mehr nur aus dem Unternehmerlager kommen, sondern von den Beschäftigten übernommen werden (»Nur euretwegen können wir nicht mailen!«), hat der Betriebsrat einen schweren Stand wenn er IKT-Systeme nur mit angemessenen Schutzmaßnahmen akzeptieren will.

Selbst wenn man weiß, dass sich derartige Konfliktsituationen niemals vollständig vermeiden lassen, so wäre es doch angenehm, einmal ein von allen als konstruktiv empfundenes Projekt zu befördern, das möglichst wenig Konfliktpotenzial birgt. Und eine solche Chance bieten die skizzierten Awareness-Programme allemal:

- Das Interesse am positiven Endergebnis (= gesteigertes Sicherheitsbewusstsein) haben Unternehmen und Betriebsrat gleichermaßen, so dass man gut einmal »an einem Strang ziehen« kann. Und: Arbeiten am gemeinsamen Ziel stellt immer auch eine vertrauensbildende Maßnahme dar.
- Das Konfliktpotenzial ist, verglichen mit Verhandlungen über den Einsatz von IKT-Systemen, äußerst gering. Man erörtert gemeinsam vernünftige Vorgehensweisen und Maßnahmen und findet sich nicht so leicht in den alten Pro- und Contra-Ecken wieder.
- Die Erfolgsaussichten sind von vornherein recht gut. Und je besser man plant, desto schneller und deutlicher werden positive Effekte eintreten.
- Der Betriebsrat verfolgt gleichermaßen Mitarbeiterinteressen und vitale Unternehmensinteressen. Er wird sowohl vom Unternehmen wie auch von den Beschäftigten als konstruktiver und kreativer ›Macher‹ wahrgenommen. Bei gut aufeinander abgestimmten Aktionen hat jeder den einen oder anderen Gewinn und ist dem Projekt (und den Akteuren) gegenüber positiv eingestellt.
- Dem Betriebsrat verschafft ein derartiges Projekt einen guten Ausgleich zu den üblichen konfliktträchtigen Arbeiten – eine Art ›Verschnaufpause‹ und gleichzeitig Auftrieb für die Motivation des Gremiums.
- Ein solches Projekt macht Freude – und zwar sowohl dem Projektteam wie auch den Beschäftigten! Schon bei der Planung möglicher Aktionen wie auch bei deren Durchführung ist Kreativität gefragt. Und obwohl der Inhalt ernst und wichtig ist, so darf, ja, soll die Form der Vermittlung durchaus auch einmal heiter sein.

Selbst wenn der Betriebsrat nicht derjenige war, der das Awareness-Programm initiiert hat (vielleicht weil die Unternehmensleitung schneller war), sollte er sich aus den gleichen Gründen aktiv an der Planung und Umsetzung beteiligen. Formal gesehen hat er in den Bereichen Datenschutz und IKT-Sicherheit zahlreiche Mitbestimmungsrechte, über die man sich jedoch in der Regel bei der Durchführung eines Awareness-Programms nicht streiten muss: Zu sehr ist die Durchführung eines solchen Projekts auf die positive, konstruktive Grundstimmung ausgerichtet und aufgebaut.

Auch wenn Awareness-Projekte die ordentlich dokumentierte Datenschutz- oder IKT-Sicherheits›politik‹ eines Unternehmens nicht ersetzen können: Es ist angemessen und sehr effektiv, die Vermittlung der Unternehmensrichtlinien nicht als ›abgehobene Berieselung‹ (z.B. durch die alleinige Verteilung dicker ›Wälzer‹) daherkommen zu lassen. Durch eine Vermittlung, die gleichermaßen das Interesse weckt und tieferes Verständnis hervorruft, wird das zentrale Ziel, die Notwendigkeit und Tragweite des eigenen verantwortungsvollen Handelns zu verstehen, wesentlich besser erreicht.

Und es besteht die berechtigte Hoffnung, dass die eingangs geschilderten Szenarien in derart sensibilisierten Unternehmen wesentlich seltener schlecht ausgehen, weil die Beschäftigten auch in schwierigen Situationen Gefährdungen intuitiv erkennen und werten können.

Karin Schuler ist freiberufliche Beraterin für Datenschutz und IKT-Sicherheit, stellvertretende Vorsitzende der Deutschen Vereinigung für Datenschutz e.V. und vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannte Sachverständige für IKT-Produkte (rechtlich/technisch); sie berät Betriebs- und Personalräte, betriebliche Datenschutzbeauftragte und IKT-Sicherheitsbeauftragte; Kontakt: fon 0228-2420733, **service@schuler-ds.de**, **www.schuler-ds.de**

Beamer = Projektor für Bildschirminhalte

Corporate Identity = umfasst sowohl das Selbstverständnis wie auch das einheitliche Erscheinungsbild eines Unternehmens, in der Regel geschaffen um ein Unternehmen auf ein bestimmtes Ziel hin auszurichten

Hacking = entgegen der ursprünglichen Bedeutung (= genialer Programmierer) wird der Begriff Hacker heute benutzt um jemanden zu bezeichnen, der Computer zu illegalen Zwecken einsetzt, zum Beispiel in fremde Rechner und Netzwerke eindringt, um dort Schaden anzurichten, der Kopierschutzmechanismen umgeht oder fremde Daten beschädigt.

Hotline = telefonische Beratung/ Unterstützung z.B. für die Softwarenutzung

Intranet = auf ein Unternehmen oder eine Organisation beschränktes Computernetzwerk, das auf der Basis der Internet-Technik arbeitet

Sniffing (Schnüffelei) = Bezeichnung für das gezielte Ausspionieren persönlicher Daten (z.B. Passworte)