secure-it in NRW. Mitarbeiter sensibilisieren für IT-Sicherheit und Datenschutz. Maßnahmen und Handlungsempfehlungen

secure IT®

Ministerium für Innovation, Wissenschaft, Forschung und Technologie des Landes Nordrhein-Westfalen

NRW.

Impressum

Agentur »secure-it.nrw«
bei der IHK Bonn/Rhein-Sieg
Bonner Talweg 17
D-53113 Bonn
Telefon: +49 (0) 228/2284-184
Telefax: +49 (0) 228/2284-5184
E-Mail: info@secure-it.nrw.de
Internet: www.secure-it.nrw.de

Ministerium für
Innovation, Wissenschaft,
Forschung und Technologie
des Landes Nordrhein-Westfalen
www.innovation.nrw.de

Texte:
Medienpool Köln GmbH in Zusammenarbeit mit Natalie Mareth, Secorvo Security Consulting GmbH, Karlsruhe, und Karin Schuler, Datenschutz und IT-Sicherheit, Bonn

Abbildungen:
Titel: Dia/Mediacolors, S.8: Fotofinder/ Kaleidoscope, PhotoCase.com

Realisation und Herstellung:
Medienpool Köln GmbH

Inhalt

Menschen machen Technik sicher

Viele Unternehmen Nordrhein-Westfalens haben erkannt, dass Informations- und Kommunikationstechnologien strategische Instrumente sind, die Innovationen und betriebliches Wachstum unterstützen – wenn gleichzeitig die IT-Sicherheit gewährleistet ist. Die Sicherheit digitaler Abläufe wird immer mehr zum wichtigen Faktor in den Geschäftsbeziehungen und verschafft den Unternehmen gegenüber Mitbewerbern auch aus dem Ausland eine gute Position.

Bei einem wirkungsvollen IT-Sicherheitskonzept spielt nicht nur Technik eine Rolle: Ein Unternehmen kann ein noch so ausgefeiltes System haben, um seine Daten und Systeme zu schützen – spielt der Mensch nicht mit, bleibt die Technik wirkungslos. Damit IT-Sicherheit in allen Bereichen eines Unternehmens greift, müssen Unternehmensleitung und Mitarbeiter Sicherheitsaspekte bei ihrer täglichen Arbeit berücksichtigen. Die hierzu nötige Aufgabe, ein Bewusstsein zu schaffen, nennen Fachleute „Security awareness“ und meinen damit „Sensibilisierung für IT-Sicherheit“. Dabei darf der Fokus nicht einseitig auf die IT-Infrastruktur gerichtet sein, sondern muss alle Sicherheitsaspekte einbeziehen, wie beispielsweise den Umgang mit Dokumenten, Zugangsregelungen und den Datenschutz.

Diese Broschüre richtet sich vornehmlich an kleine und mittlere Unternehmen. Sie möchte die Entscheider dort bei der Ansprache ihrer Mitarbeiter unterstützen. Denn immer noch schrecken viele vor dem vermeintlich hohen Aufwand einer Awareness-Kampagne zurück, häufig aus Angst, nicht alle Aspekte angemessen bearbeiten zu können.

Diese Broschüre möchte vermitteln, dass mit jedem noch so kleinen Schritt in Richtung Sensibilisierung die Sicherheit im Unternehmen spürbar gesteigert werden kann. Der Erfolg hängt dabei viel weniger vom Aufwand der Maßnahme ab als davon, dass wirklich alle – vom Geschäftsführer über den IT-Leiter bis zu den Mitarbeitern – an einem Strang ziehen. In diesem Sinne möchte ich motivieren, erste Schritte zu gehen.

Professor Dr. Andreas Pinkwart

Minister für Innovation, Wissenschaft, Forschung und Technologie
des Landes Nordrhein-Westfalen

IT-sicher ist eine Firma nur, wenn alle mitmachen

Daten und Abläufe: Rundum geschützt

IT-Sicherheit und Datenschutz sind Schutzziele, die eng miteinander verzahnt sind. Sie tragen entscheidend zur Informationssicherheit in Firmen bei, werden aber zumeist von Entscheidern in Unternehmen unterschiedlich bewertet: IT-Sicherheit wird aus ureigenem Firmeninteresse angestrebt, um die eigene Handlungs- und Produktionsfähigkeit zu bewahren – so sollte es jedenfalls sein. Netzwerkausfälle durch technische Probleme oder durch Virenbefall verursachen, je länger sie andauern, enorme Kosten – nicht nur bei der Wiederherstellung der Systeme und Daten, sondern auch durch den Produktivitätsverlust der nicht arbeitsfähigen Beschäftigten. Dazu kommen meist auch Imageschäden, denn IT-Probleme bleiben Kunden durch den heute üblichen elektronischen Geschäftsverkehr selten verborgen.

Diesem Schutzziel steht das Schutzobjekt „Mensch“ gegenüber: Immer wenn Daten über ihn verarbeitet werden, verlangen die gesetzlichen Datenschutzregelungen, dass sein Recht auf informelle Selbstbestimmung nicht verletzt wird. Diese Verpflichtung, personenbezogene Daten zu schützen, wird von Unternehmern anders wahrgenommen als der Schutz ihrer IT – als organisatorisches Handicap, weil diese sensiblen Daten eben nicht zweckentfremdet benutzt werden dürfen.

Trotzdem: Immer mehr Firmen erkennen, dass ihre Leistungsfähigkeit von Kunden und Partnerunternehmen auch danach beurteilt wird, ob ihre IT-Abläufe ebenso sicher wie datenschutzgerecht sind.

Richtlinien sind immer nur der erste Schritt

Bei der Einführung von Sicherheitskonzepten gehen die meisten Unternehmen „klassisch“ vor: Sie identifizieren die Gefährdungen, formulieren Schutzbedürfnisse, legen Maßnahmen fest und dokumentieren alles. Danach werden diese Richtlinien in die Firmenhierarchie transportiert und alle IT-Nutzer des Unternehmens zur Einhaltung verpflichtet.

Das Vorgehen ist im Prinzip richtig und notwendig, allerdings sollte es nicht bei diesem ersten Schritt bleiben: Die Nutzer fühlen sich bei solchen Anweisungen schnell bevormundet und haben bei starren Richtlinien nicht das Gefühl, Akteure in einem Prozess zu sein. Nicht selten macht sich dann ungute Stimmung breit: „Wozu das alles?“

Dies kann zu einer unzureichenden Einhaltung der mühsam festgelegten Schutzmaßnahmen führen und letztlich ihren Erfolg gefährden: Denn in der Regel werden Notebooks weiterhin unbeaufsichtigt in Besprechungsräumen oder im Zugabteil liegen gelassen, Bildschirmschoner inklusive Viren heruntergeladen oder Passwörter auf Post-it-Zetteln an den Rechner geklebt.

Innovative Unternehmen setzen deshalb auf die Sensibilisierung der Mitarbeiter: Es gilt, die IT-Nutzer von der Richtigkeit und Wichtigkeit der Vorschriften, Verfahren und Maßnahmen zu überzeugen. Man muss sie persönlich in die Maßnahmen zum Datenschutz und zur IT-Sicherheit einbinden.

Zunehmend reagieren Unternehmen darauf, dass die Anwendung der „klassischen Methoden“ allein keine IT-Sicherheit gewährleistet: Sie organisieren Awareness-Kampagnen. Diese fassen alle Maßnahmen zusammen, die den Beschäftigten ein Verständnis für Gefahren und Anforderungen vermitteln und gleichzeitig deren Interesse, Neugier und einsichtsvolles Verhalten fördern. Im Vordergrund steht nicht das Ziel eines gehorsamen Befolgens von Sicherheitsrichtlinien, sondern die persönliche Auseinandersetzung jedes Mitarbeiters mit dem Thema und seine Überlegung, wie er in seinem Wirkungskreis zum Datenschutz und zur IT-Sicherheit in seiner Firma beitragen kann.

Maßnahmen zur Mitarbeitersensibilisierung ersetzen nicht strukturierte und dokumentierte Schutzkonzepte und Richtlinien; sie wecken aber bei den Mitarbeitern mehr Verständnis für die Schutzziele und die notwendigen Maßnahmen, diese zu erreichen.

! Gesetzliche Grundpflichten beim Datenschutz

- Bestellung eines Datenschutzbeauftragten ab zehn Personen, die mit personenbezogenen Daten umgehen
- Verpflichtung aller Beschäftigten auf das Datengeheimnis
- Datenschutz-Unterweisung der Beschäftigten
- Dokumentation aller Verfahren mit personenbezogenen Daten (Verfahrensverzeichnis)

? FAQ – kurz gefragt

IT-Sicherheit
... bezeichnet das Ziel, im Unternehmen elektronische Daten, IT-Systeme und IT-Infrastruktur jederzeit einsatzbereit, inhaltlich korrekt und vor unberechtigter Einsichtnahme und Verwendung geschützt zu erhalten. Unter diesen Schutz fallen unter anderem auch aus elektronischen Daten erzeugte Papierausdrucke und Akten.

Datenschutz
... bezeichnet das Ziel, das Persönlichkeitsrecht von Menschen gemäß Artikel 2 Grundgesetz zu schützen: Beim Umgang mit personenbezogenen Daten müssen gesetzlich definierte Grundprinzipien eingehalten werden.

Informationssicherheit
... bezeichnet das Ziel, alle wichtigen betrieblichen Daten und Informationen unabhängig von ihrer Erscheinungs- und Ablageform zu identifizieren und betriebliche Abläufe und Maßnahmen so zu organisieren, dass ihre Verfügbarkeit, Korrektheit und Vertraulichkeit jederzeit gewährleistet sind.

Awareness/Sensibilisierung
... bezeichnet das Ziel, betriebliche Akteure so zu schulen und zu informieren, dass sie Anforderungen der Informationssicherheit, der IT-Sicherheit oder des Datenschutzes aus eigener Einsicht bei der Durchführung ihrer Arbeitsaufgaben erkennen und beachten.

! Das 1x1 der IT-Sicherheitsorganisation

Das gehört zu den unverzichtbaren Bestandteilen eines betrieblichen IT-Sicherheitskonzepts:

- Virenschutzkonzept
- Backup-Konzept
- Notfallpläne
- Benutzerrichtlinien (Passwörter, Internet etc.)
- Berechtigungskonzepte
- Definition der Zuständigkeiten
- Qualifizierungskonzept

(IT-)Sicherheit ist auch eine Frage des Gespürs der Mitarbeiter für unsichere Situationen

Erst Sicherheit, dann Höflichkeit

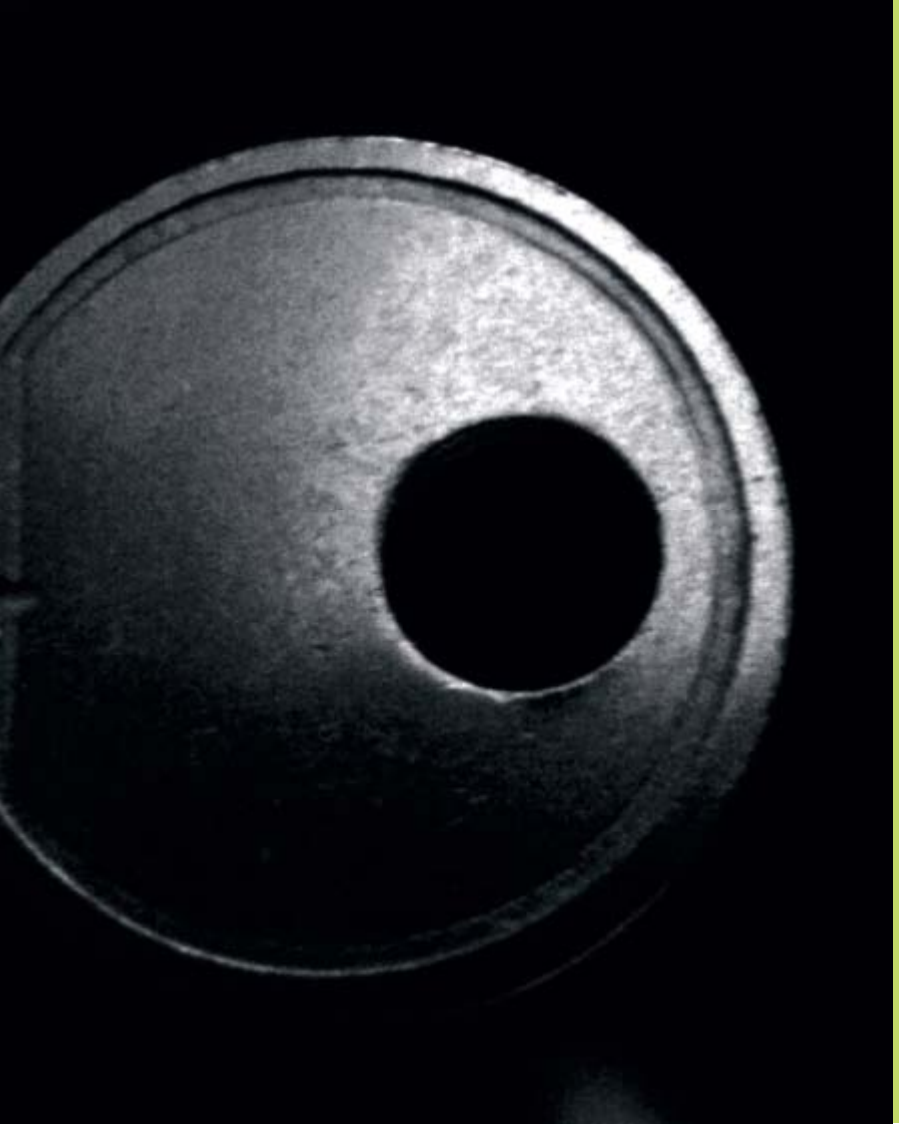
Auch in Firmen, die Richtlinien zur IT-Sicherheit entworfen und den Mitarbeitern mitgeteilt haben, kommt es zu Sicherheitsvorfällen. Denn die Erfahrung zeigt: Selbst wer die Richtlinien kennt, macht Fehler. Doch in den wenigsten Fällen liegt es am mangelnden Verantwortungsbewusstsein. Oft müssen Mitarbeiter blitzschnell entscheiden – und entscheiden falsch: Sie wollen höflich sein und geben dabei sensible Informationen weiter. Sie möchten Geschäftstermine einhalten und gehen dafür Sicherheitsrisiken ein. Starre Regeln genügen nicht. Es muss klar sein, wie man sie umsetzt. Mitarbeiter müssen Richtlinien nicht nur kennen, sondern auch verstehen, warum diese wichtig sind. Sie sollten lernen, welche Situationen Gefahren bergen. Und dass im Zweifelsfall Sicherheit vor Höflichkeit geht.

Stellen Sie sich vor ...

… in der Mittagspause klingelt das Telefon. Der betreffende Mitarbeiter ist nicht am Platz. Eine Kollegin nimmt den Anruf entgegen. Er sei Organisator eines Weiterbildungs-Seminars, stellt sich der Anrufer vor. Der Angerufene zähle zu den Teilnehmern; aber seine Anmeldung sei leider unvollständig. Er habe vergessen, das Geburtsdatum und seine Position im Unternehmen einzutragen. Außerdem fehle die private Rufnummer für kurzfristige Rückfragen. Die Kollegin überlegt und erinnert sich, dass ihr Büronachbar ihr erst kürzlich von dem Seminar erzählt hat. Und der Mann am anderen Ende der Leitung klingt sehr nett und vertrauenswürdig. Wer weiß, ob sie ihrem Kollegen mit der Auskunft nicht sogar einen Gefallen erweist? Der Anrufer erhält die gewünschten Informationen. Als der Kollege aus der Mittagspause zurückkommt, wird klar: Er hatte die Felder im Anmeldeformular ganz bewusst nicht ausgefüllt. Denn er hielt die Auskünfte für zu privat.

… ein Besucher stellt sich beim Pförtner vor. Er habe um 15 Uhr einen Termin mit Herrn Grube vom Einkauf. Der Pförtner versucht, Herrn Grube anzurufen, damit dieser seinen Besucher am Empfang abholen kann. Doch es geht niemand ans Telefon. Es ist bereits nach 15 Uhr. Herr Grube ist wahrscheinlich schon im Besprechungsraum, überlegt der Pförtner: Vielleicht wartet er sogar schon ungeduldig auf den Besuch. Also fragt er den Besucher, ob sich dieser im Gebäude auskenne. Und bittet ihn schließlich, sich doch allein auf den Weg zum Besprechungszimmer zu machen. Eine halbe Stunde später sieht der Pförtner den Besucher das Gebäude verlassen. Und zu seiner Verwunderung betritt nur wenig später Herr Grube die Firma. Es stellt sich heraus: Er hatte Termine außer Haus. Und den Besucher kennt er nicht. In seinem Büro macht Herr Grube später eine böse Entdeckung: Der Wandschrank steht offen. Und sein Beamer ist daraus verschwunden.

… in der IT-Abteilung wurden einige PCs aufgerüstet und neue Festplatten eingebaut. Nun sollen die alten Festplatten fachgerecht entsorgt werden, denn sie enthalten sensible Daten. Doch der Kurier der Entsorgungsfirma verspätet sich. Anderthalb Stunden vergehen. Der zuständige Mitarbeiter in



der IT-Abteilung ist unruhig – er muss zu einer wichtigen Besprechung. Er ist pflichtbewusst und will seine Gesprächspartner nicht warten lassen. Schließlich legt er die Festplatten in eine Kiste vor sein Büro und eilt zu seiner Sitzung. Am Empfang gibt er Bescheid, wo der Kurier sie abholen soll. Am nächsten Morgen schaut der IT-Mitarbeiter in sein Postfach – und wundert sich: Dort liegt eine Quittung über die Abholung von zehn Festplatten. Dabei hatte er doch insgesamt 25 Platten in die Kiste gelegt! Eine Rückfrage ergibt, dass tatsächlich nur zehn Stück in der Kiste lagen, als der Kurier eintraf. Die restlichen 15 bleiben verschwunden.

… der Forschungsbereich eines Unternehmens ist nur Personen zugänglich, die eine spezielle Codekarte für die Eingangstür besitzen. Ein berechtigter Mitarbeiter öffnet gerade die Tür, als ihm eine Dame entgegenkommt – den Arm voller Akten. Er hat sie noch nie gesehen. Aber sie sieht freundlich und seriös aus. Und die Akten scheinen schwer zu sein. Er denkt: In einem so großen Unternehmensbereich kann man nicht alle Gesichter kennen. Wahrscheinlich ist sie gerade erst eingestellt worden. Und überhaupt: Wenn sie Akten bei sich hat, wird sie ja wohl zur Firma gehören. Er erinnert sich an seine gute Kinderstube, grüßt die Dame zuvorkommend – und hält ihr die Eingangstür zum Forschungsbereich auf. Sie bedankt sich, eilt an ihm vorbei und verschwindet um die Ecke. Als sich der Mitarbeiter später beiläufig nach der vermeintlich neuen Kollegin erkundigt, erfährt er, dass niemand im ganzen Forschungsbereich sie kennt. Er hat einer Fremden Einlass gewährt.

? FAQ – kurz gefragt

Mit welcher Sicherheitsmaßnahme könnte im Unternehmen ein erster Awareness-Schritt verbunden werden?

Eine einfache, aber wirkungsvolle Schutzmaßnahme besteht in der Verwendung eines passwortgeschützten Bildschirmschoners. Dieser sollte sich nach spätestens drei Minuten einschalten, wenn man den Arbeitsplatz verlassen hat, und nur durch Eingabe eines Passwortes wieder ausschalten lassen.

Das Vorgehen der Geschäftsleitung:

1. Per E-Mail die Nutzer um Mithilfe bitten und den Sinn dieser Schutzmaßnahme erläutern.
2. Erklären, wie sich die Einstellung vornehmen lässt (für Windows: Systemsteuerung/Anzeige/Bildschirmschoner).
3. Bitte um Überprüfung und eventuelle Anpassung an die betrieblichen Standards, die kurz erläutert werden müssen.
4. Möglichkeit zur Nachfrage oder Kontaktaufnahme anbieten.

Wie könnte eine Awareness-Maßnahme zur Unterstützung der Regelung aussehen, dass nur Befugte Türen mit Zugangscode benutzen dürfen?

Sensibilisierung bedeutet: Es gibt nicht nur ein striktes Regelwerk („Kein Durchgang für Unbefugte“), sondern auch Hilfen zur angemessenen Umsetzung dieser Regeln im betrieblichen Alltag. Besuchern könnte auf Plakaten auf oder in der Nähe solcher Türen erläutert werden, dass die Mitarbeiter angehalten sind, keine Externen ohne Identifizierung hineinzulassen. Mitarbeiter sollten über Inhalt und Grund dieser Regeln informiert sein und die Höflichkeitsregeln (Tür aufhalten) in diesem Fall explizit aufgehoben werden.

Kleine und mittlere Unternehmen können die Sensibilisierung ihrer Mitarbeiter schon mit minimalen Mitteln erreichen

Sensible Mitarbeiter: Chefsache!

52 Prozent der IT-Schäden, so das Ergebnis einer KES/KPMG-Studie, werden durch Mitarbeiter verursacht. Sie für den Umgang mit den digitalen Medien zu sensibilisieren sollte im Unternehmen fest verankert sein – und ein entsprechendes Budget erhalten. Das geht in der Regel nur, wenn die Unternehmensleitung dies entscheidet und unterstützt. Mitarbeitersensibilisierung ist Chefsache! Das bedeutet auch, dass „von oben“ die entsprechenden Signale gesendet werden müssen: Jeder Mitarbeiter sollte das Gefühl haben, dass die IT-Sicherheit in der Unternehmensleitung einen hohen Stellenwert besitzt und dass er bei seinen Bemühungen um IT-Sicherheit am Arbeitsplatz unterstützt wird. Wirksame Sensibilisierungseffekte sind keine Frage der Kosten oder eines hohen Aufwandes, sondern das Ergebnis einer angemessenen Strategie. Der erste Awareness-Schritt in einer Firma könnte beispielsweise mit einer einfach zu installierenden Schutzmaßnahme verknüpft werden – ein nur durch Passwort zu deaktivierender Bildschirmschoner (siehe Seite 5). Dabei werden die Nutzer über die Gefahren eines unbefugten Zugriffes auf den Rechner aufgeklärt und über den Schutz, den ihnen der neue Bildschirmschoner bietet. Wenn weitere kleine Awareness-Schritte folgen, bleibt IT-Sicherheit in der Firma Gesprächsthema.

Kleine und mittlere Unternehmen können aufgrund ihrer flachen Hierarchien und direkten Kommunikationswege bereits mit geringem finanziellem Aufwand erreichen, dass die Beschäftigten IT-Sicherheit als wichtigen Teil ihres Arbeitsalltags sehen.

Sicherheit braucht System

IT-sicher wird eine Firma Schritt für Schritt – mithilfe eines systematischen Sicherheitskonzeptes: Zunächst wird die bestehende Infrastruktur im Betrieb dokumentiert, dann der Schutzbedarf der einzelnen Komponenten festgestellt und schließlich wird eine Liste möglicher Schutzmaßnahmen angefertigt. Aus diesem Konzept können dann konkrete Handlungsanweisungen, Richtlinien und Verbote für den einzelnen Benutzer abgeleitet werden. Diese sollten den Mitarbeitern bekannt gemacht werden und verbindlich sein.

Das Bestehen von Richtlinien allein sorgt allerdings noch nicht für Sicherheit. Regeln müssen umgesetzt werden. Meist führt weder Zwang zum Ziel noch das Vertrauen darauf, dass die Mitarbeiter diese von allein befolgen. Erfolgversprechender ist, um Verständnis für die Regeln zu werben, das geplante Vorgehen zu erläutern und ihre Anregungen einzubeziehen: Wenn klar aufgezeigt werden kann, aus welchen Gründen Richtlinien eingeführt wurden und eingehalten werden sollen, hat die Unternehmensleitung die Mitarbeiter auf ihrer Seite. Sie erkennen, dass die Richtlinien auch ihrem eigenen Schutz dienen und nicht aufgestellt wurden, um ihnen das Leben schwer zu machen.

Guter Start: die Passwort-Richtlinie

Eine einfach umzusetzende und von ihrem Umfang her überschaubare Sicherheitsmaßnahme könnte die Einführung einer Passwort-Richtlinie sein. Um nicht bereits bei der ersten kleineren Attacke geknackt zu werden, muss ein Passwort möglichst lang und komplex sein: Je schlechter man es sich

merken kann, weil es aus einer scheinbar sinnlosen Aneinanderreihung von Zeichen besteht, desto sicherer ist es. Es gibt mehrere Möglichkeiten, wie ein Unternehmen die Einführung einer Passwort-Richtlinie gestalten kann. Die beiden folgenden beispielsweise sind – für sich alleine betrachtet – nicht geeignet, das gewünschte Ziel einer IT-sicheren Firma zu erreichen: Erstens: Durch Konfiguration der Systeme werden nur noch starke Passwörter akzeptiert. Ohne weitere Information der Nutzer sorgt diese Maßnahme für Frust und Unverständnis. Zweitens: Dem Nutzer wird es selbst überlassen, ein starkes Passwort zu gestalten. Auch dieser Weg ist wenig erfolgversprechend, wählen die Mitarbeiter im Zweifel doch wieder die gewohnten, einfach zu merkenden Passwörter.

Nur die dritte Methode verspricht eine nachhaltige Wirkung: Um Mitarbeiter zu sensibilisieren, müssen diese erfahren, wie schnell „schwache“ Passwörter entschlüsselt werden können. Das kann etwa durch interne oder externe IT-Fachleute geschehen, die eine Vorführung an einem Rechner einrichten, der in der Betriebskantine oder einem anderen zentralen Ort zu Demonstrationszwecken installiert wird. Dort können Mitarbeiter im „Vorbeigehen“ erleben, wie schnell die üblichen PC-Passwörter geknackt werden können. Benutzer, deren Passwörter innerhalb einer Minute entschlüsselt werden, erleben dabei meist einen lehrreichen Schock.

Natürlich müssen den Anwendern danach Lösungen angeboten werden, wie sie sich komplexe, sichere Passwörter merken können. Denn das Aufschreiben von Passwörtern ist ja tabu. Hilfen reichen von systematischen Ansätzen („Bildung von Passwörtern über Merksätze“) bis zu softwareunterstützten Lösungen („Passwortsafe“), die die Verwaltung vieler verschiedener Passwörter erleichtern.

? FAQ – kurz gefragt

Wie hoch in etwa ist der Budgetanteil für Sicherheitsmaßnahmen in einer IT-sicherheitsbewussten Firma?

Je nach Unternehmensgröße und IT-Infrastruktur sollten die Ausgaben für IT-Sicherheit mindestens zehn, im optimalen Fall 20 Prozent des gesamten IT-Budgets betragen.

Für den Fall, dass Awareness-Maßnahmen nicht mit Bordmitteln organisiert werden können: Worauf ist bei der Auswahl eines externen Dienstleisters zu achten?

- Welche Erfahrungen/Referenzen hat der Dienstleister in diesem Bereich?
- Auf welche Awareness-Projekte kann er verweisen?
- Schlägt er ein breites Maßnahmenspektrum vor oder bietet er seine Beratung nur in Zusammenhang mit dem Kauf eines seiner Produkte an?
- Gibt es themenbezogene Veröffentlichungen oder Vorträge des Dienstleisters?

Die Nutzung des Internets kann gefährlich sein für die betriebliche IT-Sicherheit

Türöffner in die Firmen-IT

Eigentlich dürfte nichts passieren: Virenscanner gehören zur Standardausrüstung jedes Computers am Arbeitsplatz. Die Nutzung des Internets ist in den meisten Unternehmen strengen Regeln unterworfen und manchmal sogar untersagt:

Bestimmte Dateitypen dürfen nicht heruntergeladen oder unbekannte E-Mail-Anhänge nicht geöffnet werden. Auch private Nutzung ist häufig verboten. Doch gerade hier werden die Grenzen technischer und organisatorischer Maßnahmen zum Schutz der Firmen-IT sehr deutlich, denn die durch unvorsichtige Internetnutzung hervorgerufenen Schadensfälle in den Unternehmen häufen sich.

Ein wirksamer Schutz vor Viren und Trojanern, die in die betriebliche IT eindringen, ist ohne die Mitarbeit des Internetnutzers nicht möglich: Täglich kommen neue Viren in Umlauf, die den Virenscannern bislang noch nicht bekannt waren. Der Mitarbeiter muss darauf achten, dass seine Software immer auf dem aktuellen Stand ist. Selbst wenn die Aktualisierung automatisch erfolgt, muss der Nutzer sich verantwortungsbewusst im Netz bewegen.

Dazu benötigt er Kompetenz. Er muss Risiken erkennen und vermeiden können. Und er muss wissen, welche Gefährdungen ein Verstoß gegen betriebliche Regelungen mit sich bringt und welchen Nutzen die Einhaltung der Regeln hat. Diese Kompetenz ist eine Sicherheitsgarantie für die Firma, denn die Erhaltung der IT-Sicherheit kann die IT-Abteilung allein nicht gewährleisten. Sie ist im Übrigen auch nicht als Einzige zuständig für dieses Thema. Weder bei den betrieblichen IT-Experten noch beim Datenschutzbeauftragten kann

! Die größten durch sorglose Mitarbeiter hervorgerufenen Gefahren für die Firmen-IT

- Passwörter auf Post-its am Arbeitsplatz
- „Verlassene“ Computer ohne Schutzmaßnahme, wie beispielsweise sichere Bildschirmschoner (s. Seite 5)
- Öffnen von E-Mail-Anhängen unbekannter Sender
- Auswahl schwacher Passwörter
- Verlust von Notebooks
- Ausplaudern von Passwörtern oder Firmendaten
- Installation von „Bypass“-Lösungen (z.B. Modems)
- Geheimhaltung von Sicherheitsvorfällen
- Verwendung veralteter (fehlerhafter) Software
- Unterschätzung der Bedrohung durch „Innentäter“

die Verantwortung für ein sicheres Firmennetzwerk abgegeben werden. Ohne Zutun des einzelnen Benutzers kann nicht wirksam verhindert werden, dass Viren und Trojaner ins Firmennetzwerk eindringen und so die unbefugte Kopie der Firmendaten erleichtert oder erst möglich gemacht wird.

Wie der Nutzer diese Kompetenz erwirbt, darüber sind sich die Awareness-Experten einig: Ihm muss seine Rolle in der Sicherheitsorganisation verdeutlicht werden, und er muss einsehen, durch sein sicherheitsbewusstes Verhalten seinen Teil zum Schutz der Firmen-IT beizutragen. Einen Irrtum, der den Datendieben das Leben leicht macht, sollte der Nutzer schnellstens ablegen: den, dass die Daten auf seinem Rechner „sowieso für andere uninteressant“ seien.

Gewöhnlich stimmt das zwar – in der Regel interessieren sich die Web-Gauner weniger für dessen Daten als für die des Firmensystems. Aber sein Computer fungiert als „Türöffner“.

! **Modell für eine Passwort-Richtlinie**
(orientiert an den IT-Grundschutz-Katalogen des Bundesamtes für Sicherheit in der Informationstechnik)

- Ein Passwort besteht aus mindestens 8 Zeichen.
- Es müssen jeweils mindestens ein Groß- und ein Kleinbuchstabe sowie ein Sonderzeichen oder eine Ziffer verwendet werden.
- Das Passwort darf kein Wort sein, das in einem Wörterbuch enthalten ist.
- Es dürfen keine einfach zu ratenden Kombinationen verwendet werden (Kfz-Kennzeichen, Geburtsdatum oder bekannte Zahlenfolgen wie 0815).
- Das Passwort muss geheim gehalten und darf keiner anderen Person mitgeteilt werden.
- Das Passwort darf nicht aufgeschrieben werden, es sei denn, es ist für ein Notfallkonzept erforderlich. In diesem Fall sollte das Passwort in einem verschlossenen Umschlag in einem Safe aufbewahrt werden.
- Das Passwort muss regelmäßig gewechselt werden.
- Frühestens nach sechs Passwortänderungen darf sich ein Passwort wiederholen (laut IT-Grundschutz-Katalogen gar nicht).

Ein geringer Etat ist kein Hinderungsgrund für eine Awareness-Kampagne

Maßgeschneidert

Steter Tropfen ... die kleinere Variante

Der IT-Leiter der Firma Klein & Fein GmbH beobachtet seit einiger Zeit, dass die Mitarbeiter bei der Nutzung des Internets nicht immer die bestehenden Sicherheitsregeln beachten. Er hält es für dringend geboten, das Sicherheitsbewusstsein der Beschäftigten zu schärfen. In Absprache mit dem Geschäftsführer legt er zunächst einige Themen fest, die vermittelt werden sollen. Um einen Wiedererkennungseffekt zu erzielen, einigt man sich auf die Verwendung des Mottos „Klein & Fein sicher“ und ein einheitliches Erscheinungsbild für alle Veröffentlichungen. Der Geschäftsführer richtet ein erläuterndes Schreiben an die Belegschaft und startet damit die Sensibilisierungskampagne. Als Medium wird der wöchentlich erscheinende E-Mail-Newsletter verwendet.

Wichtig ist, dass jede Ausgabe den Spannungsbogen beibehält, deshalb werden die geplanten Informationen in unterschiedliche Formen verpackt: Berichte, Fallbeispiele, Interviews und Nachrichtenmeldungen. Flyer und Broschüren vertiefen das jeweilige Thema.

Zum jährlichen Betriebsfest wird an zentraler Stelle ein Infostand aufgebaut, ein kleines Gewinnspiel zu Sicherheitsfragen sorgt zusätzlich für Aufmerksamkeit. Nach jedem Quartal erstattet der IT-Leiter dem Geschäftsführer einen kurzen Bericht über den Ablauf und die Erfolge der Maßnahmen. Da die Sensibilisierungskampagne bisher recht günstig war, bewilligt der Geschäftsführer ein kleines Budget für die Gestaltung von Werbeträgern.

Daraufhin werden Zettelblöcke und Schlüsselbänder mit dem Motto „Klein & Fein sicher“ bedruckt und an die Belegschaft verteilt.

Live-Demos im Foyer ... die größere Variante

Die Administratoren der Gut & Gewachsen AG beklagen unnötige Schäden im Firmennetzwerk durch unachtsamen Umgang mit dem Internet. Gemeinsam mit dem Vorstand wird daher die Durchführung einer kleinen Awareness-Kampagne geplant. Frühzeitig werden die Abteilungen für Marketing und innerbetriebliche Kommunikation beteiligt. Zunächst werden Themen und Präsentationsform abgesprochen, die Marketingabteilung gestaltet Formatvorlagen und ein Logo, um der Kampagne ein eigenes Gesicht zu verleihen.

Jeder Mitarbeiter erhält ein Schreiben des Vorstands mit einem kleinen Ordner, der die im Verlauf der Kampagne veröffentlichten Schriften aufnehmen und jedem als Nachschlagewerk dienen soll. Im Intranet werden weiterführende Informationen und Links zur Verfügung gestellt.

Der Datenschutzbeauftragte konzipiert regelmäßige Schulungseinheiten, ein internetgestütztes Trainingsprogramm wird eigens angeschafft. Pro Quartal wird im Foyer für jeweils einen Tag ein Info-Point eingerichtet, an dem IT-Mitarbeiter Fragen beantworten oder Live-Demos vorführen. Das Unternehmen lädt auch externe Sicherheitsspezialisten zu Vorträgen, Diskussionen oder Demonstrationen ein. In einem Gewinnspiel mit Fragen zum Thema werden Sachpreise verlost.

? FAQ – kurz gefragt

Welche Medien eignen sich im Unternehmen für den Transport von Awareness-Themen?

Intranet, Mitarbeiterzeitung, E-Mail-Newsletter, Rundbrief mit Neuigkeiten, Flyer und Informationsbroschüren, Poster für Ankündigungen, Schwarzes Brett

Welche Themen kommen als Inhalt einer Awareness-Kampagne in Frage?

- Passwortsicherheit
- Mobile Sicherheit: Laptops, Organizer, Handys und Co.
- Der Lebenszyklus von Dokumenten und Datenträgern: Erstellung, Weitergabe, Vernichtung
- Sichere Nutzung von Internet und E-Mail: Virenabwehr, Verschlüsselung, Schutz vor schädlichen Webseiten, Phishing
- Social Engineering: Gespräche mit Fremden, Handy-Telefonate in der Öffentlichkeit, Weitergabe von Informationen
- Unternehmenssicherheit: Umgang mit Besuchern, Verschluss von Büros
- Datenschutz

Schon bei den Planungssitzungen wurden Kriterien für die Beurteilung des Erfolgs der Kampagne festgelegt. Messbare Verbesserungen wie etwa Senkungen bei der Zahl verlorener Laptops oder automatisiert knackbarer Passwörter im Netzwerk werden dem Vorstand regelmäßig vorgetragen und anschließend auch betriebsöffentlich gemacht.

! So geht's

Was ist für wen sinnvoll? Hier eine (nicht vollständige) Sammlung von Einzelmaßnahmen im Rahmen einer Awareness-Kampagne.

Preiswert und schnell umsetzbar

- Aufhängen eines „Meckerkastens“ zu Datenschutz- und IT-Sicherheitsthemen
- Einrichtung eines (moderierten) betriebsinternen Diskussionsforums im Intranet
- Regelmäßige Kolumne in der Mitarbeiterzeitung
- Einrichten einer „Sicherheits-Sprechstunde“
- Nutzung von Tools der Initiative »secure-it.nrw«: www.secure-it.nrw.de

Zeitaufwändig, aber geringe Sachkosten

- Merkblätter zu einzelnen, sicherheitsrelevanten Richtlinien und Verhaltensweisen, beispielsweise zum datenschutzgerechten Telefonieren, zum Thema „Was tun, wenn die Urlaubsvertretung kommt?“ oder zum Umgang mit mobilen Geräten
- Schulungseinheit „Wie funktioniert Verschlüsselung?“
- Schulungen zur Medienkompetenz der Mitarbeiter („Wie vermeide ich Risiken im Internet?“)
- Erstellen von Fallbeispielen mit Bildschirmansichten, zum Beispiel „Wie könnte es ablaufen, wenn mein Rechner einen Virus hat?“

Finanzielle Mittel nötig

- Gelbe Post-its mit Aufdruck „Hier kein Passwort“
- Erstellen einer „Unternehmens-Sicherheits-CD“ als Sammlung aller Richtlinien, Arbeitsanweisungen und Links zu Sicherheitsthemen
- Sicherheits-Schnitzeljagd auf Betriebsausflug oder andere Sicherheitsspiele (Quiz) mit sicherheitsbezogenem Preis
- Bedrucken von Give-aways (Werbemitteln) mit Sicherheitsaufforderungen: Mousepads, Schlüsselbänder oder Tassen
- Einsatz von „Web Based Training“ (WBT) oder Videos zur Wissensvermittlung
- Durchführen einer Plakataktion, beispielsweise Fotos von Sicherheitslücken (Bildschirm mit Passwort-Post-it, verlassener Schreibtisch mit vertraulichen Unterlagen)
- Entwicklung eines Passwort-Merktools

IT-Sicherheit und Awareness sind in einigen Firmen schon lange ein Thema

Und in der Praxis ...

M. DuMont Schauberg: Miteinander reden

Schon Ende der 90er Jahre ließ das Kölner Verlagshaus M. DuMont Schauberg (MDS) die Sicherheit seines zentralen SAP/R3-Systems durch einen unabhängigen Gutachter prüfen. Jürgen Grüne erinnert sich gerne an das erfreuliche Ergebnis: „Der Prüfbericht hat uns ein sehr gutes Sicherheitsniveau bescheinigt. Das war für mich der Anreiz, auch in der Produktion den Aufbau einer Sicherheitsorganisation zu fördern."

Die kontinuierliche, erfolgreiche Überzeugungsarbeit bei der Geschäftsführung hat ihm schließlich den Auftrag zur Erstellung einer Sicherheitspolicy eingebracht – und den Posten des IT-Sicherheitsbeauftragten. Diese anfangs parallel zur Leitung der Anwendungsentwicklung ausgeübte Tätigkeit wurde recht schnell zu einem Vollzeitjob – nicht zuletzt, um Interessenkonflikte zu vermeiden: Die Gewichtung von Sicherheitsanforderungen und Funktionalitätsbedürfnissen muss eben manchmal erst gefunden werden.

Bei seiner Arbeit wurde er von Beginn an vom Betriebsrat unterstützt, der auf die Sicherheit der Systeme ebenfalls großen Wert legt. Schließlich geht es unter anderem auch um die Sicherheit von Mitarbeiterdaten. „Außerdem profitieren wir alle davon, wenn eine Sicherheitspolicy betriebliche Mindeststandards etabliert", betont Jürgen Grüne, „denn dann muss man sich nicht anlässlich jeder Systemeinführung mit den gleichen elementaren IT-Sicherheitsfragen befassen."

„Die Sicherheitsorganisation beruht bei uns auf drei Säulen", erläutert er weiter, „der kleinen zentralen Einheit um den IT-Sicherheitsbeauftragten, der dezentralen Organisation mit Koordinatoren in den Abteilungen und der Partnerschaft mit anderen betrieblichen Akteuren. Dazu zählt auch der Betriebsrat." Zum Einsatz der Informationstechnologie schloss das Unternehmen mit dem Betriebsrat eine Rahmenvereinbarung ab. Darin sind bestimmte Vorgehensweisen bei der Einführung und Änderung von IT-Systemen vorgegeben. Unter anderem ist die Pflicht zu Rücksprache und Stellungnahme durch den IT-Sicherheitsbeauftragten und den betrieblichen Datenschutzbeauftragten festgeschrieben, wenn Investitionen anstehen.

Als nächster Schritt steht die Durchführung einer Awareness-Kampagne auf der Agenda. „Wir waren ein wenig zu gut", scherzt der IT-Sicherheitsbeauftragte, „weil wir aufgrund unserer Maßnahmen in letzter Zeit keine dramatischen Vorfälle hatten, sinkt das Gefährdungsbewusstsein unserer Mitarbeiter." Das spiegelt sich in der Akzeptanz der Nutzer wider: Die Policy wird akzeptiert und beachtet, solange keine Konflikte auftreten. Sobald die Funktionalität unter der Sicherheit leidet, sinkt die Akzeptanzschwelle. Da der Ausfall von Produktionssystemen die Firma jedoch ernsthaft gefährden könnte, sollen die Mitarbeiter durch gezielte Sensibilisierungsmaßnahmen weiter geschult werden.

Schon im Planungsstadium soll der Betriebsrat beteiligt werden. Das beginnt mit der Erstinformation, und anschließend

Dass bei der IT-Security sehr schnell auch Mitarbeiterinteressen berührt sind, weiß Jürgen Grüne von M. DuMont Schauberg. Das Kölner Verlagshaus, das unter anderem die Tageszeitungen Express und Kölner Stadt-Anzeiger herausgibt, hat daher schon frühzeitig den Betriebsrat eingebunden.

„In der Energieversorgung geht Sicherheit über alles", sagt Ulrich Herz von Mark-E. Das Energieunternehmen aus der märkischen Region mit 230.000 Privat- und Geschäftskunden sowie 1.800 Industriekunden hat frühzeitig die Sicherheitserfordernisse im internen IT-Betrieb erkannt.

soll gemeinsam ausgelotet werden, wie man ohne übermäßige Leistungs- und Verhaltenskontrolle die Erfolge der Maßnahmen überprüfen kann. Beispielsweise kann es unter Umständen sinnvoll sein, sich die Teilnahme an einem Internet-basierten Trainingsprogramm nachweisen zu lassen.

Jürgen Grüne sieht dieser Abstimmung sehr gelassen entgegen: „Die frühzeitige Beteiligung des Betriebsrates würde ich jedem anderen Unternehmen auch ans Herz legen, denn mit dem Thema IT-Sicherheit bewegt man sich immer im Spannungsfeld zwischen Unternehmensinteresse und Mitarbeiterschutz: dem Wunsch nach umfassender Kontrolle einerseits und dem Schutz der Persönlichkeitsrechte der Mitarbeiter andererseits. Da ist man so schnell im mitbestimmungspflichtigen Bereich, dass man ohne die Beteiligung des Betriebsrates gar nicht vernünftig arbeiten kann."

Mark-E: Klein angefangen

„Als Ende der 90er Jahre die Abhängigkeit von IT-Prozessen immer deutlicher wurde", sagt der Fachbereichsleiter User-Service Ulrich Herz, „haben wir bei Mark-E Nägel mit Köpfen gemacht und einen IT-Sicherheitsausschuss etabliert. Unsere Fachabteilung war und ist zwar für den ordnungsgemäßen Betrieb der Fachapplikationen verantwortlich, aber es gab keine festen Vorgaben für die IT, an denen wir uns hätten orientieren können." Der Ausschuss wurde damals vom Vorstand beauftragt, ein IT-Sicherheitshandbuch zu erstellen und zu pflegen, in dem betriebliche IT-Sicherheits- und Datenschutzvorschriften zentral und verbindlich dokumentiert werden sollten. Der Vorstand lässt sich seitdem regelmäßig über die Aktivitäten des Ausschusses berichten, unterstreicht Ulrich Herz: „Wenn das von oben nicht mitgetragen wird, kann man alle Bemühungen vergessen."

Um größtmögliche Synergien zu erzielen, wurden nicht nur IT-Fachleute, Revision und Betriebsrat mit ins Boot geholt: „Personenbezogene Daten, wie etwa Kunden- und Beschäftigtendaten, gibt es fast nur noch in elektronischer Form. Da hängt der Datenschutz ganz stark von der Güte der ergriffenen Sicherheitsmaßnahmen ab. Deshalb bin auch ich ständiges Mitglied des IT-Sicherheitsausschusses", betont Hans-Joachim Kisser, der Datenschutzbeauftragte der Mark-E.
Inzwischen verfügt das Unternehmen über umfangreiche IT-Sicherheits- und Datenschutzregelungen, die so unterschiedliche Verfahren und Verhaltensweisen betreffen wie die

revisionssichere Berechtigungsvergabe, den datenschutzgerechten Umgang mit Logdateien, den Umgang mit Passwörtern, mobilen Datenträgern und Laptops, die Vertragsgestaltung mit Dienstleistern oder die Vernichtung von Daten.

Irgendwann erkannte man jedoch, dass diese Maßnahmen allein nicht ausreichten. Den IT-Nutzern waren die Beweggründe für die Richtlinien nicht immer ersichtlich – weshalb der Umsetzungsgrad mancher Vorgaben zu wünschen übrig ließ. Ulrich Herz: „Manche Nutzer gaben einfach ihre Passwörter an die Urlaubsvertretung weiter, obwohl unsere Passwortrichtlinie das ausdrücklich untersagt." Herz berichtet auch von „gelben Zetteln" mit notierten Passwörtern, die sich an den unmöglichsten Stellen fanden. Sogar ein defektes Token, eine Hardware zur Erzeugung von Einmal-Passwörtern in der Größe eines Schlüsselanhängers, wurde dem User-Service einmal mit eingravierter PIN zurückgegeben! „Uns wurde klar, dass wir nicht nur ein rundes Sicherheitsregelwerk schaffen, sondern auch Energie in die Sensibilisierung unserer Kolleginnen und Kollegen stecken müssen", beschreibt Herz die damals gewonnene Erkenntnis.
„Da wir unmittelbar handeln wollten, kam eine aufwändige Awareness-Kampagne – auch aus Kapazitätsgründen – nicht in Frage. Also haben wir uns zur Sensibilisierung immer wieder bestimmte Themen vorgenommen und diese jeweils gleichzeitig auf verschiedenen Ebenen kommuniziert."

Der IT-Sicherheitsausschuss bekam eine Kolumne mit eigenem Logo in der Mitarbeiterzeitschrift und thematisierte in der Folge typische Awareness-Themen wie „Passwortsicherheit", „Umgang mit Laptops" oder „Virenvorsorge". Zeitgleich wurden zum jeweiligen Thema weiterführende Hintergrundinformationen in einem eigenen Bereich des Intranets bereitgestellt. Diese enthielten häufig als „Mehrwert" auch ausdruckbare Merkzettel sowie Tipps und Tricks, die sich auch für den heimischen Privat-PC nutzen ließen. Zusätzlich fanden zum jeweiligen Thema kurze Schulungspräsentationen für Führungskräfte statt, die auch Multiplikatorenfunktion übernahmen. Die regelmäßigen Schulungsangebote durch den Datenschutzbeauftragten wurden um Workshops und fachspezifische Fragestellungen ergänzt.

„Es muss gar nicht immer der große Wurf sein", ist sich Hans-Joachim Kisser sicher. „Besser klein anfangen und durch wiederholte Aktionen im Gespräch bleiben, als mit viel Tamtam nur selten in Erscheinung treten. Der Wiederholungseffekt ist der eigentliche Schlüssel zum Erfolg."
„Die Reaktionen waren durchweg positiv", bestätigt auch Ulrich Herz, „und das Klima hat sich deutlich geändert: Man spricht auch schon mal auf dem Flur über Sicherheitsfragen und überlegt gemeinsam mit Kollegen, wie im Einzelfall sicheres Verhalten aussieht. Das ist aus meiner Sicht der große Fortschritt. Heute gibt es fast keine Auffälligkeiten oder Vorkommnisse in unserem internen Netzwerk mehr." Eine wichtige Erkenntnis hat Ulrich Herz im Laufe der Zeit gewonnen: „Im Nachhinein betrachtet, muss ich sagen: Eindeutige Richtlinien sind zwar unverzichtbar, aber wenn keiner ihren Sinn versteht, sind sie schlichtweg nicht durchzuhalten."

„Awareness-Kampagnen wirken nachhaltiger, wenn sie optisch auffällig und damit allgegenwärtig sind“, meint Dr. Christoph Schog, Chief Security Officer bei T-Systems. Die Telekom-Tochter ist einer der führenden Dienstleister für Informations- und Kommunikationstechnik in Europa und betreut im Konzern das Segment Geschäftskunden. Sensibilisierungsmaßnahmen haben im Unternehmen eine lange Tradition.

T-Systems: James Bit, übernehmen Sie ...

James Bit möchte nicht mehr wegsehen, wenn ihm Sicherheitslücken auffallen. Mit dem Slogan „Mir ist es nicht egal“ versucht der fiktive T-Systems-Mitarbeiter, Mitstreiter unter seinen Kollegen für die „Mission Security“ zu gewinnen. Die Figur hat eine tragende Rolle in der gleichnamigen Security-Awareness-Kampagne, die im Jahr 2006 unternehmensweit gestartet wurde. Sicherheit spielt bei T-Systems eine große Rolle – sowohl mit Blick auf die Kunden als auch im Unternehmen selbst. „Viele unserer Mitarbeiter haben bereits ein Sicherheitsbewusstsein“, betont Dr. Christoph Schog, Chief Security Officer bei T-Systems, „aber häufig werden sie durch äußere Umstände daran gehindert, entsprechend zu handeln. Deshalb haben wir mit James Bit eine Figur geschaffen, die in vergleichbare Situationen wie unsere Mitarbeiter gerät und versucht, sicherheitsbewusst zu handeln.“

Aus diesem Grund wurde auch der Security Award ausgeschrieben, bei dem alle Mitarbeiter sechs Wochen lang konkrete Anregungen zur Verbesserung von Sicherheitsprozessen und zum Stopfen von Sicherheitslücken geben konnten. Diese wurden anschließend ausgewertet: Den besten Vorschlägen wurde neben Sachpreisen der T-Systems Security Award verliehen. Gleichzeitig erfolgte eine kontinuierliche Wissensvermittlung über das Intranet, in dem der Mission Security ein eigener Bereich eingeräumt wurde. Dort erklärt James Bit an konkreten Beispielen das richtige Verhalten in Security-Fragen. Außerdem wurde ein Mission-Security-Newsletter etabliert, mit dessen Hilfe Sicherheitsaspekte vermittelt werden.

„Man kann auch mit kleinem Budget eine Awareness-Kampagne durchführen, wenn man sich auf die Punkte beschränkt, die im Unternehmen gerade besonderes wichtig sind“, weiß Dr. Schog. „Uns ist wichtig, dass auch unsere Partner im mittelständischen Bereich Mitarbeitersensibilisierung betreiben. Das richtige Verhalten der Mitarbeiter ist ein wesentlicher Faktor der Unternehmenssicherheit.“ Denn unternehmensinterne Informationen sollen selbstverständlich nicht nur bis zu den Unternehmensgrenzen geschützt sein, sondern auch darüber hinaus bei jeder weiteren Verarbeitung. Außerdem sollen Kunden, die von T-Systems mit qualifizierten Sicherheitsmechanismen ausgestattet werden, diese dann auch möglichst sinnvoll einsetzen.

„Die wirtschaftlichen Rahmenbedingungen zwingen heutzutage viele Unternehmen zu Sparmaßnahmen. Dennoch hat unsere Geschäftsleitung wegen der Wichtigkeit des Themas ein angemessenes Budget bereitgestellt. Bei allen Maßnahmen mussten wir darauf achten, möglichst kostengünstig zu arbeiten. Viele der bei uns eingesetzten Kommunikationswege, zum Beispiel das Intranet oder der E-Mail-Newsletter, sind preiswert und stehen meist auch in mittelständischen Unternehmen zur Verfügung. Wichtig ist vor allem, dass man der Mitarbeitersensibilisierung im Rahmen seiner Möglichkeiten ausreichende Aufmerksamkeit widmet“, empfiehlt Dr. Schog.

Mission Security

So kann in einem Unternehmen eine Awareness-Kampagne vorbereitet und durchgeführt werden

Schritt für Schritt

Es ist besser, mit kleinen Schritten anzufangen, als über Jahre hinweg die optimale Awareness-Kampagne zu planen. Prägend für den Erfolg bleibt letztlich das Verhalten des Managements: Die Geschäftsführung muss Maßnahmen aktiv unterstützen und die Mitarbeiter zur Kooperation auffordern. Auch die Führungskräfte sollten einbezogen werden: Sie müssen ein Umfeld schaffen, das die Umsetzung ermöglicht, ein Budget und die benötigte Arbeitszeit einplanen. Darüber hinaus müssen Führungskräfte selbst mit gutem Beispiel vorangehen und ihren Mitarbeitern sicheres Verhalten vorleben.

1. Schritt: Themenbereiche identifizieren

In welchen Bereichen besteht Handlungsbedarf? Einige allgemeine Themen – Passwortsicherheit, Umgang mit vertraulichen Dokumenten, sichere Administration und Virenschutz – betreffen die meisten Unternehmen. Je nach Art des Betriebs kommen weitere hinzu: Arbeitssicherheit in produzierenden Betrieben, Verarbeitung personenbezogener Daten, mobile Sicherheit im Außendienst und bei Heimarbeitsplätzen. Legen Sie geeignete Themen fest, zu denen Sie sensibilisieren möchten.

2. Schritt: Kommunikationskanäle festlegen

Sie müssen das Rad nicht neu erfinden. Sicherlich gibt es in Ihrem Unternehmen bereits etablierte Kommunikationskanäle wie eine Mitarbeiterzeitung, Intranet-Bereiche oder regelmäßige E-Mail-Newsletter. Nutzen Sie diese! Das erhöht die Akzeptanz und erleichtert Ihnen die Arbeit.

3. Schritt: Maßnahmen visualisieren

Sicherheitsregeln erfreuen sich nicht besonderer Beliebtheit; sie wirken häufig eher trocken und behindernd. Visuelle Präsentationen dagegen sorgen für einen höheren Lerneffekt. Wollen Sie regelmäßige Aktionen durchführen oder mehrere Maßnahmen realisieren, sollten Sie dies kenntlich machen durch ein begleitendes Logo und/oder Motto. Ein Poster oder ein Comic prägen sich besser ein als Rundschreiben. Live-Hacking-Vorführungen, Darstellungen realer Schadensszenarien und Informationsstände im Eingangsbereich verstärken den Lerneffekt.

4. Schritt: Betriebliche Gremien integrieren

Um den Erfolg der Maßnahmen sicherzustellen, sollten Hindernisse von Anfang an ausgeräumt werden. Deshalb sollten Sie bereits in der Planungsphase Personen und Gruppen beteiligen, deren Meinung im Unternehmen wichtig ist. Neben der Geschäftsführung und der Mitarbeitervertretung ist dies auch der betriebliche Datenschutzbeauftragte. Binden Sie die Kommunikations- oder Presseabteilung mit ein. Nutzen Sie die Fähigkeiten dieser Fachleute für die Informationsvermittlung, und vermeiden Sie, dass sich Personen übergangen fühlen.

5. Schritt: Unternehmenskultur berücksichtigen

Haben Sie eher lockere, informelle Umgangsformen, sind strenge, regelorientierte Maßnahmen nicht passend. Spielerische, unkonventionelle Wissensvermittlung verspricht dagegen einen größeren Erfolg.

Auf Plakaten ließ die Fiducia AG ihre Mitarbeiter zum Thema „IT-Sicherheit" zu Wort kommen. Die interne Awareness-Kampagne sorgte für große Aufmerksamkeit.

! Maßnahmenplanung

Die folgenden Aspekte sollten bei der Planung einer Sensibilisierungsmaßnahme berücksichtigt werden:

Organisation

- Managementunterstützung sichern
- Budget klären
- Zeitrahmen bestimmen
- Klare Zielsetzung (nur betriebsintern oder auch mit Wirkung in Richtung Kunden?)
- Messbare Erfolgsfaktoren festlegen

Auswahl der Zielgruppe

- Komplettes Unternehmen oder einzelne Abteilungen?
- Qualifikationsniveau berücksichtigen
- Persönliche Erfahrungen einbeziehen
- Interessen und Motivation abklären

Art der Kommunikation

- Persönliche Ansprache
- Konkrete Ansprache
- Interaktive Elemente
- Etablierte Kommunikationskanäle nutzen

www.secure-it.nrw.de – www.innovation.nrw.de