Mitarbeiter für den sorgsamen Umgang mit Daten sensibilisieren

Rund 170.000 Unternehmen in Deutschland wurden 2014 Opfer von Cyberkriminalität. Der hochgerechnete Schaden liegt bei 51 Mrd. Euro pro Jahr – Tendenz steigend. Die Zahlen des BITKOM-Studienberichts „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter“ sprechen eine deutliche Sprache. Daten und vertrauliche Informationen sind wertvoll – für Unternehmen stehen die Wettbewerbsfähigkeit und oft auch ihre Existenz auf dem Spiel, wenn vertrauliche Daten in falsche Hände geraten. Wie können sie ihre Daten schützen und auch ihre Mitarbeiterinnen und Mitarbeiter für diese wichtige Aufgabe motivieren?

Informationsschutz und IT-Sicherheit erfordern die Aufmerksamkeit der Unternehmensführung. Eine wachsende Zahl von technischen Komponenten, Tools und Lösungen können physikalische Barrieren errichten und Zugangswege versperren oder reglementieren. Doch über 80 % aller bekannten Sicherheitsvorfälle werden von Mitarbeitern – oft unbewusst – verursacht, weil sie technische Systeme umgehen und/oder Sicherheitsregeln nicht beachten. Durch Unwissenheit, Bequemlichkeit und Gewohnheit werden die meisten Schäden verursacht. Deshalb müssen sowohl die Technik wie auch „der Faktor Mensch“ beim Aufbau eines Informationssicherheitsmanagement-Systems berücksichtigt werden. Nur wenn die Bereiche Mensch und Technik ausreichend berücksichtigt werden, sichere und funktionierende Prozesse existieren und die Anwender den Nutzen der Maßnahmen verstehen und ihr Verhalten anpassen, ist ein Maximum an Informationssicherheit gewährleistet. Der Schwerpunkt dieses Merkblattes liegt auf der Sensibilisierung der Mitarbeiter.

Was kann denn schon passieren?

Die Einschätzung von Mitarbeiterinnen und Mitarbeitern zu den Folgen von verloren gegangenen oder gestohlenen Daten ist manchmal eher naiv und verharmlosend. Aus ihrer Perspektive sind die Folgen nicht immer absehbar, manche Handlung erfolgt unbewusst und ohne die Konsequenzen zu bedenken. Deshalb muss die Unternehmensführung im Rahmen der internen Kommunikation Mitarbeiter sensibilisieren.

Praktische Beispiele können helfen, konkrete Auswirkungen zu prognostizieren und mögliche Folgen sichtbar zu machen:

- Was würde passieren, wenn ein unternehmenseigenes Laptop oder Smartphone mit Detailinformationen zu Produkten (Zeichnungen, Materialzusammensetzungen, Patenten usw.) aus einem Firmenwagen gestohlen wird?
- Angenommen, ein Vertriebsmitarbeiter verlässt das Unternehmen und wechselt zu einem Marktbegleiter. Er nimmt Kundendaten auf einem USB-Stick mit. Was kann er damit anfangen und kann er dem Unternehmen Schaden zufügen?
- Auf dem Weg zu einer wichtigen Messe unterhalten sich zwei Kollegen in der Bahn über die Schwierigkeiten bei der Einführung eines neuen Produktes. Es wird intensiv diskutiert, für welche Kunden es besonders interessant ist und wo die Vorteile liegen. Auch über die Preisgestaltung diskutieren die Beiden intensiv. Was wäre, wenn der Entwicklungsleiter eines Marktbegleiters zufällig im Abteil sitzen würde?

- Ein Multifunktionsdrucker/Kopierer oder ein alter Rechner wird ausgemustert. Die Geräte werden als Elektronik-Schrott zum Wertstoffhof gebracht. Sollten/müssen die Daten auf den Geräten gelöscht werden?
- Muss jemand, der nur kurz in eine andere Abteilung geht, seinen Bildschirm sperren und ein vertrauliches Dokument vom Schreibtisch nehmen. Was dort liegt können doch alle sehen, oder?
- Über Facebook stimmen sich die Kollegen aus der Produktion ab, wer in der nächsten Woche welche Aufträge übernimmt. So geht es am schnellsten und alle wissen Bescheid.
- Eine neue Kollegin aus der Marketing-Abteilung verschickt mit Outlook ein Weihnachtsmailing an die Kunden. Versehentlich verschickt sie die E-Mail nicht über das BCC-Feld (englisch: Blind Carbon Copy; sinngemäß in Deutsch: Blindkopie), sondern über den offenen Verteiler des „AN-Feldes“. D.h. alle E-Mail-Adressen sind für die Empfänger der Nachricht vollständig lesbar.

Diese Beispiele zeigen, dass viele potentielle Gefahren im Unternehmensalltag lauern. Verantwortlich für Verstöße gegen den Datenschutz und die Informationssicherheit ist die Geschäftsleitung. Sie müssen dafür sorgen, dass der Informationssicherheit im Unternehmen die richtige Priorität eingeräumt wird, die entsprechenden Ressourcen (Informationen, Zeit und Budget) zur Verfügung stehen und die Mitarbeiter entsprechend angewiesen sowie überwacht werden. Sie können die entsprechenden Aufgaben auch an interne oder externe Datenschutzbeauftragte delegieren und sich entsprechend unterstützen lassen. So wurde z.B. in der oben zuletzt genannten Angelegenheit der Bußgeldbescheid des zuständigen Landesamtes für Datenschutzaufsicht nicht gegen den konkreten Mitarbeiter, sondern gegen die Unternehmensleitung erlassen.

Damit Mitarbeiter Daten des Unternehmens aktiv schützen, müssen sie die Gefahren kennen und ein Bewusstsein für den richtigen Umgang entwickeln. Sie müssen entdecken, dass Regeln und Prozesse ihnen dabei helfen und sie unterstützen. Im Idealfall entwickeln sie einen geschulten Blick für die Risiken im eigenen Handlungsbereich und werden proaktiv tätig, um Schaden vom Unternehmen abzuwenden. Sie achten auf die Einhaltung der Regeln im Unternehmen und weisen auch neue Kollegen oder Praktikanten und Auszubildende ein.

Den richtigen Ton treffen – Belehrungen reichen nicht

Beispiele schaffen Verständnis und verdeutlichen Folgen. Zeitgemäße Kommunikationsmittel wecken Interesse und helfen Informationen im Unterbewusstsein zu verankern. Filme, Comics, Flyer und Plakate zeigen das Thema einfach und plakativ auf und können eine Verhaltensänderung herbeiführen. Schulungsunterlagen, Aufkleber und Checklisten erinnern an wichtige Botschaften und Aufgaben. Informationsmaterialien im Corporate Design stärken gleichzeitig die Unternehmenskultur.

Nach der Erarbeitung einer Sicherheitsrichtlinie für das Unternehmen, die grundsätzliche Fragen und Regeln zum Umgang mit Daten im Unternehmen behandelt, muss eine Informationskampagne zur Bekanntmachung folgen. Schulungsmaßnahmen und Trainings (auch online) können auch komplexere Anforderungen erfüllen. Mit Tests und einer Dokumentation der durchgeführten Maßnahmen können die Verantwortlichen nachweisen, alles aus ihrer Sicht mögliche zur Vermeidung von Sicherheitsrisiken getan zu haben. Das ist im Schadensfall ein wichtiger Punkt.

Von besonderer Bedeutung ist die laufende Wiederholung der Maßnahmen sowie Anpassung auf aktuelle Sicherheitsvorfälle.

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

Denken Sie in kleinen Schritten! Starten Sie besser zeitnah als jahrelang die optimale Awareness-Kampagne vorzubereiten. Prägend für den Erfolg wird das Verhalten des Managements sein. Ohne die Unterstützung der Geschäftsleitung und Führungskräfte wird die Umsetzung nicht gelingen.

Schritt 1: Vorbereitung und Identifikation von Themenbereichen

- Initialworkshop
- Sicherstellung der Unterstützung durch die Geschäftsleitung
- Auswahl der Zielgruppe (komplettes Unternehmen, einzelne Abteilungen, Berücksichtigung des jeweiligen Qualifikationsniveaus)
- Bestimmung des Zeit- und Budgetrahmens
- Festlegung des Handlungsbedarfs
  - Allgemeine Themen, z.B. Passwortsicherheit, Umgang mit vertraulichen Dokumenten, Virenschutz, Umgang mit Spam E-Mails etc.
  - Spezifische Themen, z.B. Verarbeitung personenbezogener Daten, Mobile Sicherheit im Außendienst und bei Heimarbeitsplätzen etc.
- Bestimmung messbarer Erfolgsfaktoren

Schritt 2: Festlegung der Kommunikationskanäle und Integration betrieblicher Gremien

- Art der Kommunikation (unter Berücksichtigung der Unternehmenskultur)
  - Persönliche Ansprache
  - Konkrete Ansprache
  - Interaktive Elemente
  - Auswahl von Materialen
  - Nutzung etablierter Kommunikationskanäle, z.B. Intranet, E-Mail-Newsletter, Mitarbeiterzeitung etc.
- Integration betrieblicher Gremien
  - Geschäftsleitung, Führungskräfte
  - Mitarbeitervertretung
  - Meinungsführer im Unternehmen
  - Betrieblichen Datenschutzbeauftragte
  - Sicherheitsbeauftragte
  - Kommunikations- und Presseabteilung

Schritt 3: Umsetzung und Visualisierung der Maßnahmen

- Präsenzschulungen
  - Mitarbeiterschulung
  - Führungskräfte-Schulung
  - Schulungen für Fachabteilungen (z.B. IT, Personal, Buchhaltung etc.)
  - Spezialschulungen
  - Live-Hacking als Spezialmaßnahme

- Online-Schulungen, z.B. Einsatz von eLearning Lösungen
- Begleitung
  - Newsletter
  - Fachvorträge
  - Factsheets
  - Hauszeitung
  - Broschüre/Flyer
  - Wechselnde Poster an frequentierten Bereichen (z.B. im Eingangsbereich, in der Küche etc.)
- Ansprache und Motivation
  - Quiz
  - Videos
  - Comics zur Einprägung
  - Beispiele aus der Praxis zu Schadensszenarien
  - Verteilung von Give-Aways

Schritt 4: Erfolgsmessung

- Auswertungen, z.B. Intranetzugriffe
- Tests
- Live-Evaluation (Feedbackgespräche)
- Auswertung von (Online-)Schulungen
- Quiz-Analyse
- Social Engineering Angriff
- Techn. Test-Angriff (Fake-E-Mail)

Schritt 5: Wiederholung laufender Maßnahmen und Anpassung auf aktuelle Sicherheitsvorfälle

Wo finden Unternehmen Unterstützung für Security Awareness?

Prinzipiell können Kommunikationsagenturen Unternehmen bei der Umsetzung von Informationskampagnen im Bereich IT-Sicherheit unterstützen. Auf Security Awareness spezialisierte Anbieter können jedoch auf Vorlagen zurückgreifen und verfügen über Fachkenntnisse, die schneller und kostengünstiger zu Ergebnissen führen.

Wichtige Informationen zum Thema IT-Sicherheit und Datenschutz finden Sie unter

- www.bsi.bund.de
- www.lda.bayern.de
- www.allianz-fuer-cybersicherheit.de
- www.bitkom.org
- www.aitiRaum.de

Autoren:

Andrea Henkel, aitiRaum e.V.
Martin Braun, MB-Factory

Dieses Merkblatt wurde im Rahmen der Kooperation IT-Sicherheit für Familienunternehmen der IHK Schwaben mit dem Branchennetzwerk aitiRaum e.V. erstellt.

Ansprechpartner:

Dr. Kristin Joel
Stettenstraße 1 + 3 | 86150
Augsburg
Tel 0821 3162-406 | Fax 0821
3162-342
kristin.joel@schwaben.ihk.de