



Link: <https://www.cio.de/a/it-sicherheit-scheitert-meist-an-mitarbeitern,2971808>

Sicherheitskultur im Unternehmen

IT-Sicherheit scheitert meist an Mitarbeitern

Datum: 24.09.2014

Autor(en): Marcus Beyer

Der Mensch stellt nach wie vor den größten Risikofaktor für die Informationssicherheit im Unternehmen dar. Nur wer seine Unternehmens- und Kommunikationskultur ändert, kann IT-Security von seinem "Bremsklotz-Image" befreien.

Als ich kürzlich am Flughafen Zürich auf meinen Abflug wartete, zog es meine Blicke automatisch auf das Notebook meines Nachbarn, der gerade geschäftliche E-Mails bearbeitete. Es war einfach, mitzulesen. Was ich sah, wollte ich eigentlich gar nicht wissen. Genau genommen durfte ich es auch nicht wissen. Denn die Informationen waren nicht für mich bestimmt. Gerät Wissen dieser Art in falsche Hände, kann für das Unternehmen großer Schaden entstehen.

Was mich dabei beschäftigt ist die Tatsache, dass der Benutzer dieses Notebooks derart in seine Arbeit vertieft war, dass er wohl keinen Gedanken an die Gefahr des Informationsverlustes verlor. Diese Haltung ist weit verbreitet und beschreibt das eigentliche Problem der IT-Sicherheit: die Anwender zu wenig sensibilisiert.

IT-Sicherheitsberater reden seit über zehn Jahren über die Sensibilisierung der Nutzer für Sicherheitsthemen. Offensichtlich will es nicht in die Köpfe der Mitarbeiter hineingehen. Selbst vorbildliche CISOs, die ihre Mitarbeiter in Schulungen über Security und ihre Anwendung im Alltag informieren, müssen feststellen, dass bestimmte Vorgaben zwar kurz nach der Schulung von vielen eingehalten werden, die Akzeptanz im Laufe der Zeit jedoch wieder stark nachlässt. Bei näherer Betrachtung wird klar, dass das Thema nicht richtig verankert ist und dass in der Kommunikation Fehler gemacht werden.

Das Thema Security wird als "Bremsklotz" wahrgenommen

IT-Security ist in Unternehmen in den meisten Fällen bei der IT-Abteilung aufgehängt und wird oft aus rein technischer Sicht betrachtet. Mit der Installation von Sicherheitsmaßnahmen wie Firewalls, USB-Port-Blocking, Passwortverwendung und vielen mehr werden zwar wichtige Bereiche abgedeckt, allerdings schützen diese nicht vor kriminellem oder unbeabsichtigtem Fehlverhalten der Nutzer und somit auch nicht vor Datenverlust beziehungsweise Informationsdiebstahl.

Im Gegenteil: Solange das Thema rein technisch betrachtet wird, wird Security im Unternehmen als "Bremsklotz" wahrgenommen, den man ungern unterstützt. Das ließe sich ändern, sofern es die Verantwortlichen schaffen, Security als "Enabler" zu positionieren, also als Thema, das die Ziele und Prozesse des Unternehmens und seiner Mitarbeiter unterstützt.

Die IT kann sie sich als "Enabler" positionieren

Die IT-Abteilung muss dazu die geschäftskritischen Prozesse und die davon betroffenen IT-Anwendungen analysieren. Erkennt die IT, dass Mitarbeiter zum Beispiel Dropbox nutzen, weil sie diese für ihre tägliche Arbeit dringend benötigen, obwohl dies in den Richtlinien nicht vorgesehen ist, sollte sie in Zusammenarbeit mit dem Management eine sichere Alternative bereitstellen. Andernfalls werden die Anwender immer weiter aus den Verhaltensregeln ausbrechen.

Das erfordert generell eine andere Herangehensweise an das Thema: Dabei hat der CISO in seiner Funktion als Enabler die Prozesse, Risiken und den Mitarbeiter, der mit Risiken umgehen muss, in seinem Blickfeld. Auch beim oben genannten Flughafenbeispiel könnte er die Enabler-Rolle einnehmen, indem er automatisch bei jedem neuen Notebook-Rollout eine Blickschutzfolie auf mobile Endgeräte anbringt bzw. dem Nutzer mitgibt. Denkt er noch einen Schritt weiter, liefert er auch einen verschlüsselbaren USB-Stick mit aus, damit die Daten auch bei Verlust geschützt sind.

Wer die Arbeitsprozesse des Nutzers versteht, findet einfache, praktikable Lösungen, die dann auch von den Mitarbeitern unterstützt werden: Ein CISO einer Bank ärgerte sich, dass einige Angestellte ihre Rechner während der Mittagspause nicht sperrten und entwickelte eine simple aber sehr gut funktionierende Lösung.

Er koppelte den Betrieb der Rechner an die Signaturkarte. Die Mitarbeiter benötigen diese, um in andere Räume zu kommen, für die Nutzung des Kopierers und für die Bezahlung in der Kantine. Damit hat der CISO sichergestellt, dass die Mitarbeiter ihre Karte beim Verlassen des Arbeitsplatzes mitnehmen und somit automatisch ihre Rechner sperren. Die Mitarbeiter wiederum akzeptierten die Maßnahme von Beginn an, weil sie den Sinn verstanden deren Umsetzung automatisch erfolgt.

Über welche Art von Sicherheit reden IT-Verantwortliche?

Weil Security ein Prozess ist, der nie aufhört, muss das Thema kontinuierlich und nachhaltig kommuniziert werden. Es darf nicht abstrakt und "digital" behandelt werden, vielmehr muss der Umgang mit Sicherheit Bestandteil der Unternehmenskultur werden. Und damit kommt es auch aus der technischen Ecke heraus, denn das Thema umfasst den gesamten Bereich des Informationsschutzes und sollte daher unter der Bezeichnung Informationssicherheit gehandhabt werden, bei dem auch der Mensch eine zentrale Rolle spielt.

Mit wem reden CISOs - mit wem nicht?

Eine Ursache für die mangelnde Akzeptanz bei den Mitarbeitern liegt in der unzureichenden Kommunikation seitens der Sicherheitsverantwortlichen. Nicht jeder IT-Fachmann ist von Haus aus ein "Sozialautist", aber es fällt schwer, echte und authentische Kommunikationstalente zu finden, die auch noch auf Augenhöhe mit dem Management und den Mitarbeitern reden können. Doch die werden benötigt, damit Security aus dem "stillen Kämmerlein" herauskommt und bei den Mitarbeitern wie auch beim Management ankommt.

Häufig behelfen sich IT-Verantwortliche damit, externe Berater ins Unternehmen zu holen, die das Management auf Sicherheitslücken und Risiken aufmerksam machen. Das mag im Einzelfall sinnvoll sein, generell jedoch ist dies der falsche Weg.

Die IT muss selbst auf das Management zugehen und ihre Themen pushen. Sie muss in der Lage sein, sie vor dem Management wie auch vor den Mitarbeitern zu erklären. Auch hier ist die Enabler-Funktion von großer Hilfe.

Ein typisches Thema ist die Nutzung von Social Media. Das Management gibt häufig aus Sicherheitsgründen vor, diese Kanäle zu sperren, was die IT in ihren Richtlinien verankert. Zunehmend kommt aus dem Business und der Personalabteilung jedoch die Anforderung, Social Media in den Vertriebs-, Marketing- und Rekrutierungsprozess einzubinden.

Die IT wird mit ihrer bestehenden Richtlinie als "Verhinderer" wahrgenommen, es sei denn, sie kommuniziert das Thema und wird beim Management wie bei den Fachabteilungen aktiv, um eine Lösung zu erarbeiten.

Wirkungsvolle Awareness-Kampagnen

Benjamin Franklin sagte: "Tell me and I forget, teach me and I may remember, involve me and I learn". Diese Erkenntnis lässt sich auf die Vermittlung von Sicherheitsthemen im Unternehmen übertragen. Wer nur darüber redet, wird scheitern, wer das Thema veranschaulicht, erntet das eine oder andere Kopfnicken.

Wer aber nachhaltige Wirkung erzielen will, bezieht die Menschen in das Thema mit ein. Aus diesem Grund gehen immer mehr Unternehmen dazu über, Awareness-Kampagnen zu initiieren, die genau darauf ausgerichtet sind. Sie tragen dazu bei, dass Informationssicherheit von den Mitarbeitern wahrgenommen wird, die Schwachstellen für jeden sichtbar werden und positionieren sie im richtigen Kontext.

Ein anschauliches Beispiel dafür liefert der "Security Parcour", den T-Systems als Training für seine Mitarbeiter organisiert. Er umfasst mehrere Stationen - wie in einem Circle-Training - zum Mitmachen mit Themen wie "Informations-Klassifizierung", "Clear Desk", "Besucher und Ausweise", "Password-Hacking", "Social Engineering" und "Social Media". An jeder Station wurden die Teilnehmer durch einen Moderator in das Thema eingeführt. In Teams wurde jeweils eine Aufgabe gelöst und anschließend besprochen. Die intensive Beschäftigung erhöhte die Aufmerksamkeit für das Thema Internetsicherheit im Unternehmen.

Ein anderes Beispiel kommt von einem Schweizer Uhrenhersteller: Dieser forderte seine Mitarbeiter in einem Fotowettbewerb während einer Awareness-Maßnahme dazu auf, kleine zusammenbaubare Plastikmonster auf potenzielle Sicherheitslücken am Arbeitsplatz zu stellen, diese zu fotografieren und die Bilder auf einer speziell dafür eingerichteten Kampagnenseite im Intranet zu veröffentlichen.

Das Ergebnis zeigt die Figuren auf einem Telefonapparat (die Angreifer kommen übers Telefon), auf einer internen Umlaufmappe mit dem Vermerk "vertraulich", mit Kreditkarte in der Hand auf einem Computer sitzend, auf einem Kartenleser zur Zutrittskontrolle am Eingang und vielen weiteren Stationen. Die Aktion hat nicht nur die Aufmerksamkeit der Mitarbeiter erhöht, sondern auch Gedankenbrücken zur Informationssicherheit beim Gebrauch von Umlaufmappen, der Benutzung des Telefons oder bei der Zugangskontrolle gebaut.

Fokus auf die Mitarbeiter richten

Weil der Mensch den größten Risikofaktor darstellt, sollten sich Sicherheitsverantwortliche intensiver mit ihm beschäftigen. Es klingt paradox, aber die größte Aufmerksamkeit erhält ein Mitarbeiter vor Beginn und nach Beendigung seines Arbeitsverhältnisses. So haben die Personalabteilungen klare Prozesse für die Phasen Rekrutierung, Einstellung und Ausstellung. Aber was geschieht in der Zeit dazwischen?

Die meisten Unternehmen schauen auf die kritischen Schnittstellen und auf Veränderungsprozesse bei den Mitarbeitern selbst, nicht aber auf den Standard im Alltag. Es ist nicht der chinesische Praktikant, der die Daten stiehlt. Vielmehr muss sich der Blick manchmal auf jene richten, die überhaupt nicht im Visier der Sicherheitsmenschen sind. So kann ein 50-jähriger mit zwei Kindern, der seit fünf Jahren im Unternehmen ist, ein weitaus höheres Risiko darstellen, wenn dieser beispielsweise durch Scheidung finanziell unter Druck gerät. Auch wenn er die Jahre über ein loyaler Mitarbeiter war, so kann sich das sehr schnell ändern.

Und er kennt die "Kronjuwelen" des Unternehmens besser als ein Praktikant, die für sechs Wochen im Betrieb mitarbeitet. Vor dem Hintergrund, dass einer GULP-Studie zufolge lediglich 60 Prozent der Mitarbeiter loyal gegenüber ihrem Unternehmen stehen und 25 Prozent nichts mehr mit ihm zu tun haben wollen, ist eine stärkere Fokussierung auf den einzelnen Mitarbeiter anzuraten.

Was kann der CISO ändern?

Der erweiterte Blickwinkel hat wenig mit den klassischen Aufgaben einer Security-Abteilung zu tun. Letztere ist mit den bestehenden Anforderungen bei zu wenig Personal, zunehmend komplexer werdenden Aufgaben und dem Kostendruck ohnehin überlastet und steht jeder zusätzlichen Aufgabe kritisch gegenüber.

Manche Unternehmen denken darüber nach, eine eigene Security-Stabsstelle zu schaffen, die den ganzheitlichen Blick auf die Informationssicherheit richtet. Entscheidend für den Erfolg ist weniger die organisatorische Aufhängung des Themas als vielmehr die Verankerung in der Unternehmenskultur. Der Schritt von der IT-Security zur Informationssicherheit ist auch psychologisch zu vollziehen.

Insofern kommt dem Management, den Führungskräften und den Sicherheitsverantwortlichen eine Vorbildfunktion zu. Solange sie das Thema nicht aktiv vorleben, wird es von der Belegschaft kaum übernommen werden. Auch Awareness-Kampagnen können sehr förderlich für die Unternehmenskultur sein, weil sie das Gefühl "wir gehören zusammen" fördern. Sie funktionieren aber nur, wenn sie richtig kommuniziert werden und sie benötigen Zeit.

In der Kommunikation liegt der Schlüssel zum Erfolg

Für die Arbeit des CISOs ist es wichtig, wie er mit dem Management kommuniziert und wie er im Unternehmen vernetzt ist. Er sollte in der Lage sein, das Management mit den entscheidenden Argumenten wie Business-Effizienz oder Schutz vor Restriktionen zu überzeugen. Eine wesentliche Voraussetzung dafür ist, dass er sich mit der Geschäftsleitung regelmäßig austauscht und in der Lage ist, auf Augenhöhe zu kommunizieren und seine Strategie zu erklären.

Auch gegenüber den Mitarbeitern wird er mit Awareness-Maßnahmen nur dann einen nachhaltigen Erfolg erzielen, wenn er kommunikative Menschen in die Abteilung einbindet oder die Maßnahmen mit professionellen Kommunikatoren umsetzt. Ein CISO braucht außerdem auch Mut, etwas Neues zu tun und kreative Wege zu gehen.