

Das schwächste Glied der Sicherheitskette zählt

Hinter 80 Prozent der IT-Sicherheitsvorfälle steht der Mensch. Die Erhöhung der Sensibilität im Umgang mit Informationen ist deshalb ein effektives Mittel, die Sicherheit im Unternehmen merklich zu erhöhen. *Wolfgang Sidler, Daniel Eugster*



Wolfgang Sidler

ist eidg. Wirtschaftsinformatiker mit FA, Nachdiplom FH in Informatiksicherheit (Executive Master of Information Security) und Microsoft Certified Systems Engineer (MCSE). Seit 2001 IT-Security Officer bei der Privatbank Julius Bär in New York und Zürich und Mitautor des «Sicherheitshandbuchs für die Praxis». www.sihb.ch

Daniel Eugster

ist IT-Security Officer bei der MIGROSBANK. Betriebsökonom FH, Nachdiplom FH in Informatiksicherheit (Executive Master of Information Security).



Bei der Informationssicherheit ist es wie im Strassenverkehr: Korrektes Verhalten jedes Einzelnen ist entscheidend für die Sicherheit aller, obwohl technische, organisatorische und bauliche Vorkehrungen vorhanden sind. Die optimalen Sicherheitsmassnahmen wirken automatisch, also ohne Zutun einer Person, können nicht umgangen werden und sind weder störend noch einschränkend. Im Umfeld eines Arbeitsplatz-PC mit all seinen Anwendungen können Sicherheitsmassnahmen häufig keine hundertprozentige Sicherheit gewährleisten, oder sie hängen von ihrer Anwendung durch den Benutzer ab. Sie können folglich nicht erzwungen werden. In beiden Fällen kommt dem Menschen eine sehr wichtige Rolle zu: Er muss die Massnahmen richtig beziehungsweise überhaupt anwenden.

Wie im Strassenverkehr ist der Mensch für die Informationssicherheit zentral: Mit seinem Verhalten trägt er Verantwortung, die er nicht delegieren kann. Die Sicherheit im Strassenverkehr hängt somit wesentlich vom persönlichen, verantwortungsvollen und aufmerksamen Verhalten jedes Einzelnen ab, was als Sicherheitskultur verstanden wird.

Nicht die Technik, sondern der Mensch soll überlistet werden

Die Wichtigkeit der Sicherheitskultur in einem Unternehmen wird durch Statistiken und durch aktuelle Vorfälle untermauert: Laut Untersuchungen «versagt» in rund 80% aller IT-Sicherheitsvorfälle der Mensch und in nur rund 20% die Technik. Und es gibt kaum eine technische Massnahme, bei der nicht in irgendeiner Form der Mensch involviert ist. Aktuelle Vorfälle, wie zum Beispiel das Erschleichen von Passwörtern oder E-Banking-Zugangscodes (Phishing), und die heutigen Vorgehensweisen von Viren zeigen, dass vermehrt der Mensch und nicht die Technik überlistet werden soll.

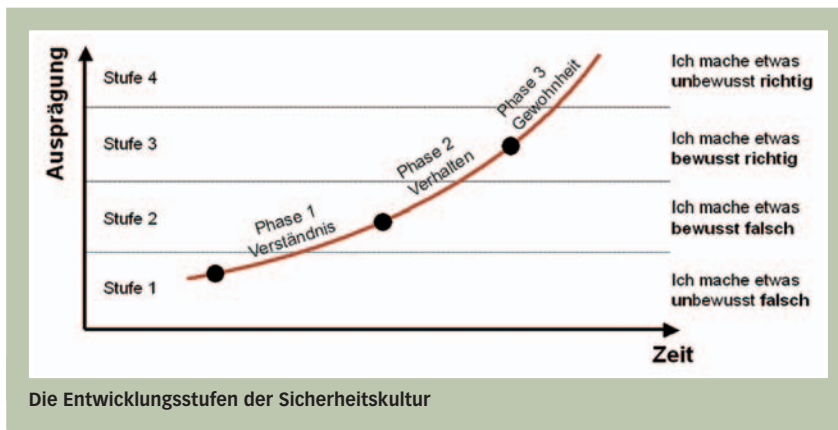
Informationssicherheit ist zudem keinesfalls mehr eine rein interne Angelegen-

heit: Einerseits sind die Kunden indirekt betroffen, wenn aufgrund von Betriebsproblemen, etwa wegen eines Virenausbruchs, die Dienstleistungen nicht mehr wie gewohnt erbracht werden können. Direkt sind sie andererseits betroffen, wenn sie beispielsweise von der Firma angebotene elektronische Verkaufskanäle wie Bestellungen via E-Mail oder Zahlungen über E-Banking nutzen. Je sensibler die verarbeiteten Kundendaten sind, umso wachsamer verfolgen die Kunden die gelebte Sicherheitskultur eines Unternehmens. Die Mitarbeiter an der Kundenschnittstelle sind dementsprechend von grosser Wichtigkeit für das Image der Unternehmung.

Im Vordergrund steht für den Mitarbeiter der für ihn optimale und bequemste Weg zur Leistungserbringung. Sicherheitsmassnahmen hemmen die bekannten Abläufe und stören die Effizienz der Arbeit, so die gängige Meinung. Die Stärkung des Sicherheitsbewusstseins verbessert die Akzeptanz der Informationssicherheit und führt damit zum Wachstum der Sicherheitskultur im Unternehmen, sodass die Informationssicherheit zu einer Selbstverständlichkeit und zum Bestandteil der Firmenkultur wird. Es geht letztlich darum, das Verhalten der Mitarbeiter bleibend zu verändern. Bei Banken ist dies im Bereich der physischen Sicherheit bereits seit Jahren der Fall.

Sensibilisierung ist eine permanente Aufgabe

Um das Sicherheitsbewusstsein der Mitarbeiter und den hohen Stellenwert der Informationssicherheit innerhalb des Unternehmens zu fördern, sollte ein umfassendes, organisationsweites Sensibilisierungsprogramm durchgeführt werden. Ziel eines solchen ist, die Informationssicherheit zu einem integrierten Bestandteil der täglichen Arbeit zu machen. Es gibt verschieden Ansätze, wie man eine Sicherheitskultur aufbauen und prägen kann. Für einen nachhaltigen



Erfolg sind in jedem Fall eine zielpublikumsorientierte Kommunikation wichtig und das Bewusstsein, dass es sich dabei um einen kontinuierlichen und mehrjährigen Prozess handelt. Denn Sensibilisierung ist eine permanente Aufgabe.

Die Entwicklung einer Sicherheitskultur kann grob in die drei Phasen «Verständnis schaffen», «Verhalten ändern» und «zur Gewohnheit werden» aufgeteilt werden. In der ersten Phase soll das Verständnis für die Thematik geschaffen werden. Die Mitarbeiter werden mit ausreichenden Hintergrundinformationen versorgt, damit sie verstehen, welche für sie relevanten Sicherheitsmassnahmen und -regelungen im Unternehmen bestehen sowie einzuhalten sind – und vor allem wozu sie dienen. Die Kenntnis darüber allein genügt jedoch nicht. Die Mitarbeiter müssen dazu gebracht werden, im Modell die Phase zwei umzusetzen, das heisst das Gelernte in der Praxis auch wirklich anzuwenden.

Dies ist der eigentliche Kernpunkt einer Sicherheitskultur und damit eines Sensibilisierungsprogramms. Denn für erzwingbare Sicherheitsmassnahmen, wie beispielsweise die Badge-Nutzung für den Gebäudezu-

tritt, benötigt es grundsätzlich keine Sensibilisierung. Dass man beim Eintritt darauf achten sollte, dass nicht noch eine weitere unberechtigte Person durch die offene Türe eintritt, hingegen schon. Ebenfalls kann man Mitarbeiter nicht zwingen, ein virenverseuchtes E-Mail nicht zu öffnen. Genau in solchen Bereichen setzt ein Sensibilisierungsprogramm an.

Die dritte Phase bezweckt das automatische oder unbewusste Anwenden von Sicherheitsmassnahmen. Eine erfolgreiche Sensibilisierung führt letztendlich zu einer nachhaltigen Verhaltensänderung der Mitarbeiter. Sie müssen immer wieder mit dem Thema Informationssicherheit konfrontiert werden, damit diese zum selbstverständlichen Bestandteil der täglichen Arbeit wird. Um eine bleibende Verhaltensänderung zu bewirken, sollten die Informationen regelmässig aufgefrischt und aktualisiert werden.

Erkennen der Notwendigkeit durch Kennen der Risiken

Da Sicherheitskultur nicht erzwungen werden kann und Informationssicherheit immer noch als Störfaktor und Verhinderer gesehen

wird und weniger als unternehmensstrategischer Erfolgsfaktor, ist es mit einer reinen Informationskampagne nicht getan. In der heutigen Informations- und Regulationsflut (Letzteres insbesondere bei den Banken) kann die Wichtigkeit des Themas Informationssicherheit schnell untergehen. Als ein kritischer Erfolgsfaktor haben sich in der Praxis das Erkennen der Notwendigkeit der Sicherheitsmassnahmen sowie das Kennen der effektiv vorhandenen Risiken bei jedem einzelnen Mitarbeiter herauskristallisiert. Erst wenn dies erreicht ist, werden die Sensibilisierungsinformationen bewusst aufgenommen und in korrektes Sicherheitsverhalten umgesetzt. Über das Erzeugen einer gewissen Verunsicherung kann der Mitarbeiter zur Einsicht und anschliessend zum Ziel, dem Soll-Verhalten, geführt werden. Diese Verunsicherung kann ausgelöst werden, indem beispielsweise von tatsächlichen Sicherheitsvorfällen berichtet wird oder durch Live-Demonstration von Risiken wie dem Knacken eines Passwortes, dem Fälschen eines E-Mails oder der Einfachheit einer Vireninfektion.

Aha-Effekte bringen mehr als lange Predigten

So genannte Aha-Effekte bei Zuhörern sind langen Erklärungen über Sinn und Zweck vorzuziehen, da sie wesentlich besser und nachhaltiger aufgenommen werden. So zeigt beispielsweise das Knacken eines Passwortes oder das Fälschen eines E-Mails direkt während einer Sensibilisierungspräsentation eindrücklich die Risiken auf. Der Hinweis auf eine mögliche, ja sogar sinnvolle Nutzung der Verhaltenshinweise auch im Umgang mit dem privaten PC erhöht die Aufmerksamkeit des Publikums merklich.

Auch die Verknüpfung der Informationen mit privatem Nutzen hat sich als erfolgversprechend erwiesen: Im Rahmen einer unternehmensweiten IT-Security-Awareness-Aktion wurde eine CD «Vertrauen ist gut, Kontrolle ist besser! Wie Sie Ihren Home-PC schützen können» mit einem Virus-Scanner und anderen Tools inklusive Booklet mit Internet-Tipps allen Mitarbeitern abgegeben, damit sie zu Hause ihren PC sicher und kontrolliert betreiben können. Besonders heute, mit der Verwendung von USB-Memory-Sticks, ist das Risiko, einen Virus oder andere schädliche Programme einzuschleusen, sehr hoch. Das Feedback der Mitarbeiter war durchgehend positiv, zumal sie einen aktuellen Viren-Scanner mit Update-Abo und Tipps für das korrekte Verhalten im Internet kostenlos bekommen haben.

