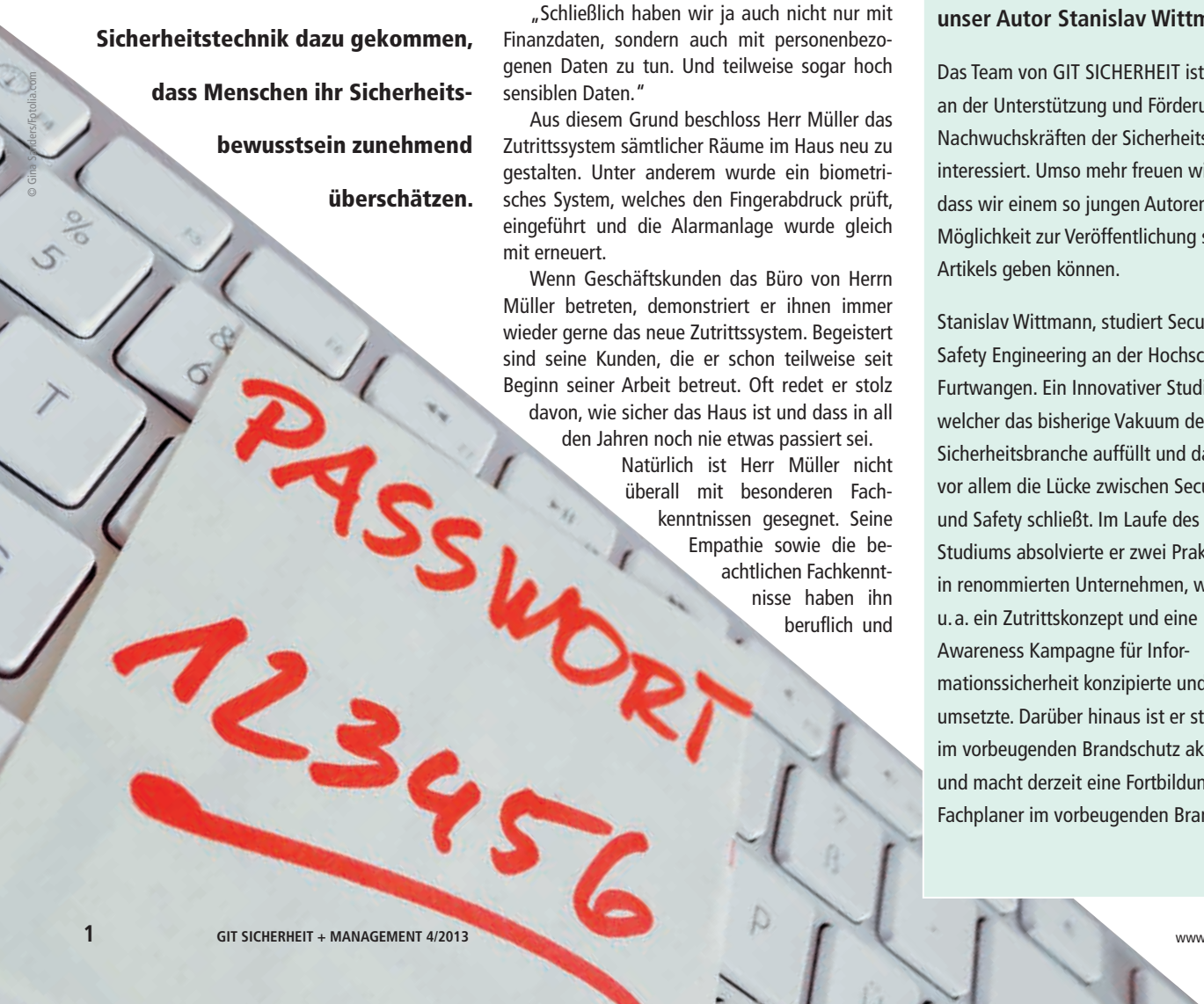
INFORMATIONSSICHERHEIT

„Spionage? Nicht bei uns“

Mitarbeiter sensibilisieren – Informationssicherheit erhöhen

Sicher ist, dass Sicherheitstechnik in unserer Gesellschaft kaum noch wegzudenken ist. Doch die eigentliche Schwachstelle vieler Unternehmen ist nicht mehr die Technik selbst, sondern der Mensch. Diesen Schwachpunkt nehmen einige Unternehmen immer noch nicht bewusst wahr. Vielleicht ist es ja gerade durch den enormen Fortschritt der Sicherheitstechnik dazu gekommen, dass Menschen ihr Sicherheitsbewusstsein zunehmend überschätzen.



© Gina Sanders/fotolia.com

Ein Beispiel aus dem Leben

Montag, acht Uhr. Lukas Müller kommt zur Arbeit. Pünktlichkeit war schon immer eine Tugend von ihm. Seit etwa 35 Jahren arbeitet Herr Müller für eine recht erfolgreiche Versicherungsgesellschaft. Fleiß, Loyalität und sicher auch ein wenig Glück haben ihn schnell zur Führungskraft befördert. Das bedeutet natürlich auch Verantwortung. Denn Herr Müller muss sowohl gegenüber den Kunden als auch seinen Mitarbeitern stets ein Vorbild sein.

Sicherheitsbewusstsein ist bei Herrn Müller auch schon immer vorhanden gewesen. Vor kurzer Zeit hörte er, dass ein Mitbewerber in der Stadt Opfer von Spionageangriffen wurde. Sensible Kundendaten sind in falsche Hände gelangt. „Spionage? Nicht bei uns“, dachte er sich selbstsicher.

„Schließlich haben wir ja auch nicht nur mit Finanzdaten, sondern auch mit personenbezogenen Daten zu tun. Und teilweise sogar hoch sensiblen Daten.“

Aus diesem Grund beschloss Herr Müller das Zutrittssystem sämtlicher Räume im Haus neu zu gestalten. Unter anderem wurde ein biometrisches System, welches den Fingerabdruck prüft, eingeführt und die Alarmanlage wurde gleich mit erneuert.

Wenn Geschäftskunden das Büro von Herrn Müller betreten, demonstriert er ihnen immer wieder gerne das neue Zutrittssystem. Begeistert sind seine Kunden, die er schon teilweise seit Beginn seiner Arbeit betreut. Oft redet er stolz davon, wie sicher das Haus ist und dass in all den Jahren noch nie etwas passiert sei.

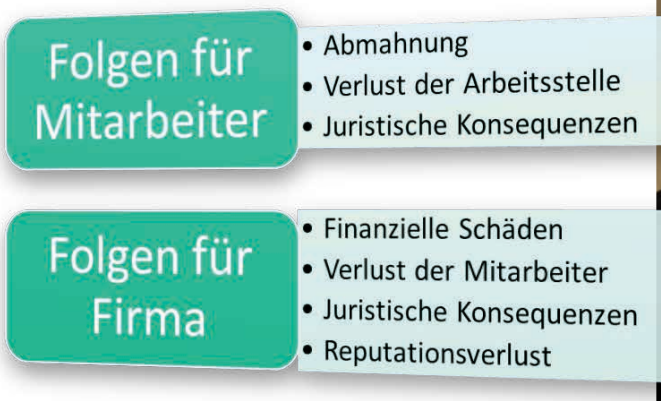
Natürlich ist Herr Müller nicht überall mit besonderen Fachkenntnissen gesegnet. Seine Empathie sowie die beachtlichen Fachkenntnisse haben ihn beruflich und privat stets weitergebracht. Gerne gibt er den Auszubildenden und Mitarbeitern sein Wissen pflichtbewusst weiter. Doch wenn es um IT-Systeme geht, läuft es ihm kalt den Rücken herunter. Diese ständigen Sicherheitsupdates und Systemumstellungen sind einfach nicht seine Welt.

Seit kurzem stellt die Geschäftsführung erhöhte Sicherheitsanforderungen an die Computernutzung. Kennwörter müssen dabei u.a. vierteljährlich gewechselt werden. Und diese müssen neben Groß- und Kleinbuchstaben auch noch Ziffern oder Sonderzeichen enthalten. An-

Nachwuchsförderung – unser Autor Stanislav Wittmann

Das Team von GIT SICHERHEIT ist sehr an der Unterstützung und Förderung von Nachwuchskräften der Sicherheitsbranche interessiert. Umso mehr freuen wir uns, dass wir einem so jungen Autoren die Möglichkeit zur Veröffentlichung seines Artikels geben können.

Stanislav Wittmann, studiert Security & Safety Engineering an der Hochschule Furtwangen. Ein Innovativer Studiengang, welcher das bisherige Vakuum der Sicherheitsbranche auffüllt und dabei vor allem die Lücke zwischen Security und Safety schließt. Im Laufe des Studiums absolvierte er zwei Praktika in renommierten Unternehmen, wo er u. a. ein Zutrittskonzept und eine Awareness Kampagne für Informationssicherheit konzipierte und umsetzte. Darüber hinaus ist er stark im vorbeugenden Brandschutz aktiv und macht derzeit eine Fortbildung zum Fachplaner im vorbeugenden Brandschutz.



▲ **Mögliche Konsequenzen** bei Wissensabfluss

▲ **Stanislav Wittmann**

gemessene Nutzung von Kennwörtern gehört ja schließlich auch zu einer aktiv gelebten Sicherheitskultur. Und außerdem soll jeder Mitarbeiter seinen Bildschirm sperren, sobald er den Arbeitsplatz verlässt. Viele solcher Regelungen bereiten Herrn Müller mächtig Probleme. „Ständiger Passwortwechsel und diese Sonderzeichenregelungen. In mein Büro kommt doch eh keiner außer mir herein", denkt er sich immer und schreibt jedes neue Passwort schön ordentlich auf einen kleinen gelben Zettel, der an seinem Monitor klebt. Gegen fünf Uhr nachmittags verlässt er heute sein Büro. Ein Auszubildender begegnet ihm auf dem Flur und fragt ihn: „Herr Müller, schließen Sie denn nicht ab? Nein, heute nicht. Morgen früh habe ich einen wichtigen Kundentermin und möchte, dass das Büro picco bello aussieht. Wenn ich das Büro verriegle, kommt das Reinigungspersonal nicht herein."

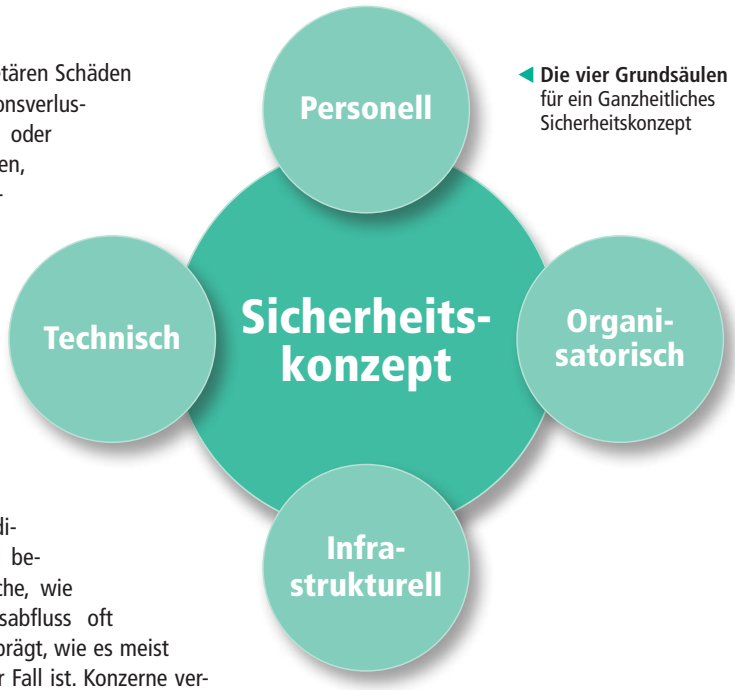
Hoffen wir, dass außer dem Reinigungspersonal niemand sonst das Büro betritt…

Die Bedeutung von Informationssicherheit in Unternehmen

Ist dieses ausgedachte Beispiel von Herrn Müller wirklich nur erfunden? Oder gibt es immer noch zu viele Sicherheitslücken, die vor allem durch den Menschen entstehen? Eine Studie von Corporate Trust zur Industriespionage 2012 zeigt, dass mehr als die Hälfte aller befragten Unternehmen mangelnde Sensibilität von Mitarbeitern beim Umgang mit vertraulichem Know-how als konkretes Sicherheitsrisiko für ihr Unternehmen sehen. Das heißt im Klartext, dass jedes zweite Unternehmen die aktuelle Gefahrenlage bereits kennt! Die Konsequenzen von Know-how-Abfluss können, gerade für KMU's, existenzbedrohende Auswirkungen haben. Diese können nicht nur zu kurzfristigen monetären Schäden führen. Auch Reputationsverluste gegenüber Kunden oder juristische Konsequenzen, u.a. durch die Missachtung des Bundesdatenschutzgesetztes (BDSG) können Unternehmen nicht unerhebliche Schäden bereiten.

Ganzheitlicher Ansatz

Gerade bei mittelständischen Unternehmen sind besondere Sicherheitsbereiche, wie der Schutz von Wissensabfluss oft nicht entschlossen ausgeprägt, wie es meist bei großen Konzernen der Fall ist. Konzerne verfügen teilweise sogar über eine eigene Corporate Security und decken sämtliche Sicherheitsrelevante Themen in dieser ab. Jedoch haben alle Unternehmen einen individuellen Schutzbedarf und müssen dafür Sorge tragen, dass dieser durch angemessene Maßnahmen umgesetzt wird. Technische Maßnahmen allein reichen bei weitem nicht aus und müssen durch weitere geeignete Anordnungen ergänzt werden. Grundsätzlich sollte bei allen Unternehmen ein ganzheitliches und angemessenes Sicherheitskonzept angestrebt werden.



◀ **Die vier Grundsäulen** für ein Ganzheitliches Sicherheitskonzept

„Und der ganzheitliche Ansatz ist der Schlüssel zum Erfolg!"

Mitarbeiterschulungen im Rahmen von Awareness-Kampagnen können dabei die Anforderungen der personellen Schutzmaßnahmen abdecken. Angemessene und nachhaltige Schulungen erfordern ein wohl durchdachtes und abgestimmtes Konzept. Dies ist nicht gerade einfach umzusetzen, zahlt sich aber erfahrungsgemäß bereits mittelfristig aus. Und zwar nicht nur im spürbar erhöhten Sicherheitsniveau, sondern auch in der Produktivität und letztlich in der Wettbewerbsfähigkeit des Unternehmens.

▶ **KONTAKT**

Stanislav Wittmann
wittmast@gmx.de