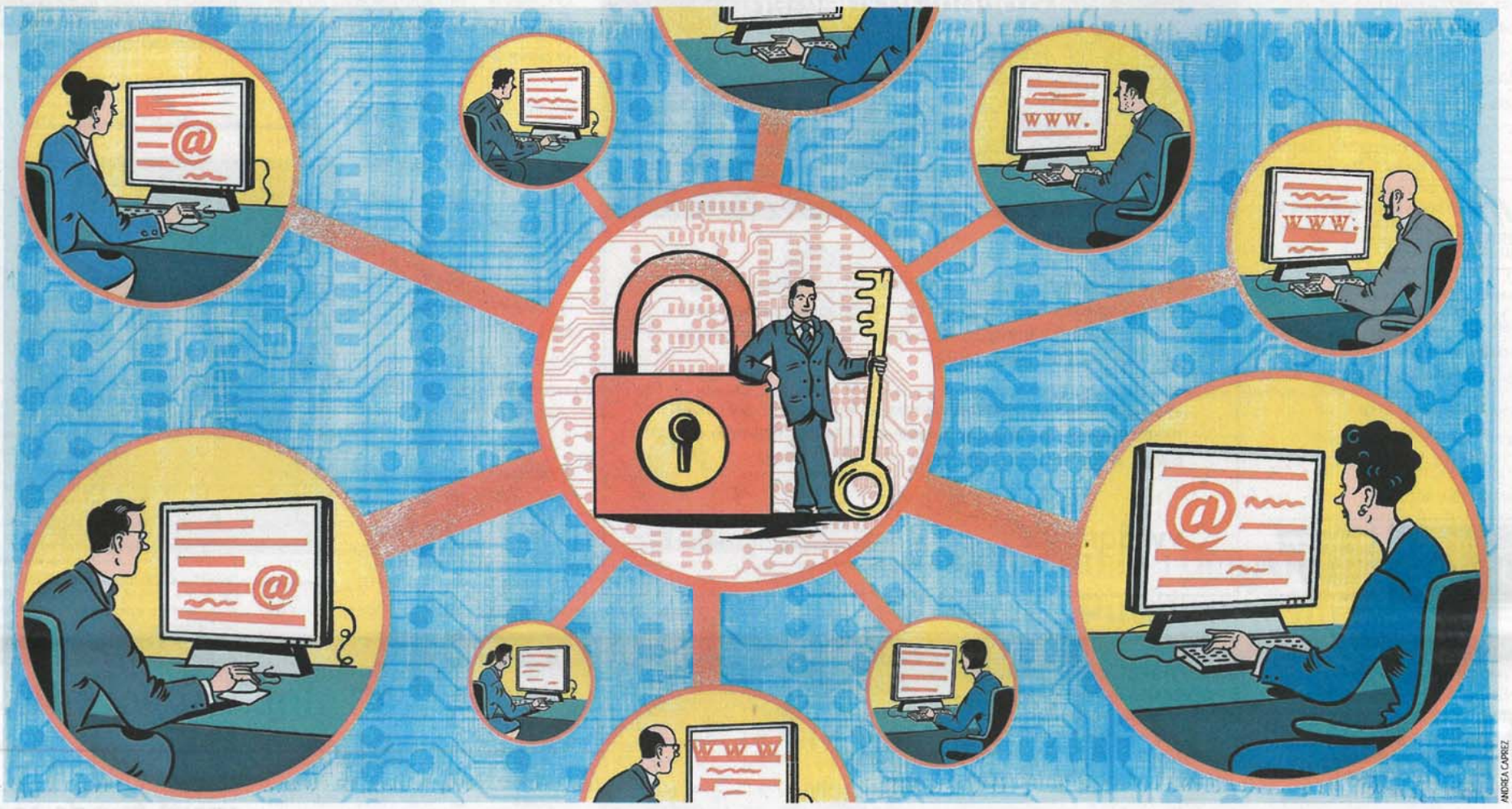
Management

Lücken ohne Ende

Daten Mitarbeiter gefährden mit privater Cloud- und Gerätenutzung die IT-Sicherheit ihrer Firma.



ANDREA CAPREZ

STEFAN MAIR

Wichtige Datenschätze einer Firma sind nicht nur durch externe Attacken gefährdet. Oft ist es das unvorsichtige Verhalten von Mitarbeitern, das Firmen für Datendiebstahl, Datenverlust oder andere Probleme anfällig macht. Viele Massnahmen gegen diese Bedrohung sind bekannt. So gehört es zum Standard, dass Passwörter regelmässig gewechselt werden, dass Mitarbeiter zum Thema Datensicherheit geschult werden und dass sensible Daten verschlüsselt werden.

Dieses Standardprogramm ist aber in vielen Fällen nicht mehr wirksam. Denn Mitarbeiter nutzen zunehmend Cloud-Dienste im Büro, die sie nicht mit der eigenen IT-Abteilung abgesprochen haben. Auch private Geräte breiten sich im Büro aus. Die klassischen Sicherheitsmassnahmen der Firmen werden durch dieses Verhalten untergraben. Viele Firmen setzen bei der Absicherung ihrer Daten nämlich auf ein sogenanntes SIEM-System (Security Information Event Management). Dort werden Protokolle über Änderungen in den Computersystemen erstellt und mithilfe intelligenter Software analysiert und ausgewertet. Erkennt das Programm ein auffälliges Verhalten, gibt es ein Warnsignal und die IT-Sicherheitsabteilung kann reagieren.

Das Problem: Mitarbeiter nutzen Cloud-Dienste, die von solchen Systemen nur schwer überwacht werden können. Die Studie «Cloud Adoption & Risk in Europe» zeigt, dass in Unternehmen im Durchschnitt mehr als 1000 Cloud Services im Einsatz sind, einige offiziell, einige inoffiziell, die meisten werden ohne das Wissen der IT-Abteilung verwendet. Firmen, die diese Sicherheitslücke schliessen wollen, müssen Cloud-spezifische Analyse- und Warnfunktionen in ihre Sicherheitsprogramme integrieren.

Weil Mitarbeiter oft das grösste Sicherheitsrisiko für Firmen sind, versuchen diese, ihre Sicherheitssysteme zu personalisieren. Dabei spielen Behaviour-Analytics-Systeme die wichtigste Rolle. Diese Systeme sammeln Daten über Benutzer und deren Zugangs- und Zugriffsrechte im System. Hier gibt es nicht nur Warnungen vor Aktionen, die als gefährlich eingestuft werden, sondern sie werden auch auf mögliche Auswirkungen analysiert.

Mitarbeiter tracken

So ist es eine vernachlässigbare Gefahr, wenn ein Mitarbeiter, der ohnehin keine Zugriffsrechte hat, aus Versehen auf eine Datei zugreifen will, auf die er nicht zugreifen soll. Kommt dieser Zugriff hingegen von einer Person, die mit diesen Daten möglicherweise Schaden anrichten kann, wird ein Alarm aktiviert. Andere Anwendungsmöglichkeiten sind Aktivitätsmonitorings im Anschluss an eine ungewöhnliche Aktion eines Mitarbeiters im System, die die Firma bei rechtlichen Streitigkeiten absichern. Entfernt beispielsweise ein Mitarbeiter eine Verschlüsselung in einem Dokument, das als besonders wichtig eingestuft wurde, beginnt das Programm seine weiteren Aktivitäten zu protokollieren. In Extremfällen kann das Programm sogar ausgehende E-Mails blockieren, damit wichtige Unterlagen das Unternehmen nicht verlassen. Anbieter in diesem Gebiet sind beispielsweise die Firmen Rapid 7, RedOwl und Securonix.

In manchen Firmen sind Hunderte Cloud-Dienste im Einsatz.

Auch weil Firmen das Verhalten von Mitarbeitern in Arbeits-PC immer häufiger tracken und analysieren, weichen diese auf private Geräte im Büro aus: Eine Umfrage des Marktforschungsunternehmens Wakefield hat ergeben, dass der Anteil von Arbeitnehmern, die ihre privaten Tablets für mehr als etwa nur das Abrufen von Arbeits-E-Mails nutzen, in der Schweiz bei rund 20 Prozent lag. Viele Unternehmen in der Schweiz bestätigen, dass sie ihren Mitarbeitern ermöglichen, private Geräte am Arbeitsplatz zu verwenden. Bei den SBB spricht man von einigen hundert Angestellten, die von dieser Möglichkeit Gebrauch machen. Bei Swisscom sind es immerhin 2000 der 20 000 Mitarbeiter.

Für die Zukunft rechnen diese Unternehmen mit Zuwachsraten bei Arbeitsmodellen, in denen privat und beruflich weniger scharf zu trennen ist. Wie werden aber Sicherheitsprobleme durch das Mitbringen privater Geräte verhindert? Schliesslich werden bei BYOD-Modellen (Bring your own device) Daten der Firma auf nur teilweise kontrollierbaren fremden Geräten verarbeitet, dazu ist oft die Haftung bei Schäden am Gerät während der Arbeitszeit ungeklärt.

Firmen, die ein BYOD-System etablieren wollen, sollten nach einem Dreistufen-Plan vorgehen, um Probleme zu vermeiden. Zuallererst muss überprüft werden, ob die Mitarbeiter nicht schon über private Geräte auf Mitarbeiterdaten zugreifen. Einer Studie des IT-Dienstleisters Aruba Networks zufolge tun dies durchschnittlich 15 Prozent der Arbeitnehmer ohne das Wissen des Arbeitgebers. Die Firma muss feststellen, wie viele und welche Privatgeräte auf das IT-System des Unternehmens zugreifen.

Vernachlässigte ITler

In einem zweiten Schritt müssen Richtlinien zur Nutzung privater Geräte am Arbeitsplatz erarbeitet werden: Welche Geräte haben Zugang zu Firmendaten? Welche Apps sind erlaubt? Welche Compliance-Regeln gelten? Besonders heikel ist der Zugriff der Firma auf private Daten auf den beruflich genutzten Geräten. Die IT-Abteilung muss für jedes Gerät Regeln für den Zugriff besitzen.

Im dritten Schritt sind Schulungen für alle Mitarbeiter unumgänglich. Bedienfehler der Mitarbeiter sind der Hauptgrund für Probleme bei BYOD-Systemen. «Rund 90 Prozent der Support-Anfragen sind auf Bedienungsfehler zurückzuführen», erklärt Christof Keller, der bei der St. Galler Kantonalbank BYOD-Lösungen überprüfte. Eines ist sicher: Der Aufwand für die IT bei der Zulassung eines BYOD-Systems wird bedeutend höher. Firmen müssen kalkulieren, ob sich dies durch eingesparte Kosten bei der Anschaffung von Hardware ausgleicht. Alternativ kann die Betreuung der privat und beruflich genutzten Geräte auch an Firmen ausgelagert werden, was ein hohes Vertrauen in diesen Dienstleister bedingt.

Eine Mitarbeitergruppe, die in der Sicherheitsstrategie des Unternehmens oft vernachlässigt wird, sind die IT-Angestellten. Dabei ist die intensive Kommunikation mit der IT ein Erfolgsfaktor. Das zeigt eine Studie des Wirtschaftsinformatikers Tim Weitzel. Er hat mit zwei Forscherkollegen gezeigt, wie wichtig eine gute Verbindung zwischen IT und Management für die Unternehmenssicherheit und den Firmenerfolg ist. Die Forscher nahmen dafür 149 US-Banken unter die Lupe und analysierten, wie eng in den Geldinstituten Informatiker und Entscheider zusammenarbeiteten. Das Ergebnis: Je besser sich beide Abteilungen verstehen, desto erfolgreicher und sicherer waren die Banken.

Doch dass ein IT-Experte in der Geschäftsleitung sitzt und bei wichtigen Geschäftsentscheidungen mitreden darf, ist selten. Noch immer wird die IT oft als Handwerkerabteilung wahrgenommen, die Probleme lösen soll. «Das Management betrachtet die IT oft lediglich als Kostenfaktor», sagt Thomas Müller, Geschäftsführer der IT-Beratung Solcom, die IT-Experten an Firmen vermittelt.

Für den IT-Sicherheitsexperten Thomas Hänisch liegt ein weiteres Problem der Verständigung aber darin, dass das Management oft nur die IT-Ausgaben im Blick hat. «Gerade in kleinen und mittelständischen Unternehmen will man möglichst nur einmal investieren.» Um sich wirksam etwa vor Hackern, aber auch Risiken, die durch unüberlegtes Mitarbeiterverhalten entstehen, abzusichern, müsse man aber immer wieder nachrüsten. Viele IT-Sicherheitskonzepte hätten aktuelle Entwicklungen wie die Cloud zu wenig berücksichtigt. Die Konzepte sind statisch und bürokratisch. Oft geht es nur mehr darum, ein altes Sicherheitskonzept durchzusetzen. Die Lücken, die inzwischen entstanden sind, werden aber geflissentlich übersehen.

Die häufigsten Fehler von Firmen

- **Private Cloud-Dienste** Die Popularität von Cloud-Diensten führt dazu, dass Mitarbeiter viele verschiedene Anbieter nutzen. Klassische Überwachsungssysteme wie die SIEM-Systeme müssen auch Cloud-Aktivitäten prüfen können.
- **Mitgebrachte Geräte** Immer mehr Mitarbeiter bringen ihre privaten Geräte mit ins Büro, verknüpfen private und berufliche Accounts. Diese Geräte werden von vielen Sicherheitskonzepten gar nicht berücksichtigt.
- **Unklare Definitionen** In vielen Firmen besteht Unklarheit darüber, welche Inhalte im Unternehmen schützenswert sind und welche nicht. Hier müssen sensible Inhalte klar definiert werden.