ZEITUNG FÜR KOMMUNALE WIRTSCHAFT

Verlag: Sigillum GmbH München/Berlin
Redaktion: Neumarkter Straße 87 · 81673 München

Ausgabe 04/12, Seite 24

Datensicherheit nur konsequent

CHEFSACHE Schutz empfindlicher Unternehmensinformationen ist überlebenswichtig. Schäden grassieren

Von **KAY SCHLÜPMAN,** ComCode GmbH, Gröbenzell

Versorger besitzen und verarbeiten viele Informationen, die nicht in unbefugte Hände geraten sollen, die korrekt sein müssen, und die dann zur Verfügung zu stehen haben, wenn sie gebraucht werden. Dazu zählen Informationen über Kunden, Lieferanten, Verbräuche, Geschäftspläne, Strategien, Forschungen, usw. Alle sind in IT abgelegt. Diebstahl oder eine Manipulation von Unternehmensdaten kann mitunter gravierende Folgen nach sich ziehen.

Die Liste möglicher Angreifer ist lang: Vom fahrlässigen oder verärgerten Mitarbeiter über den Hacker, die Konkurrenz bis hin zu Organisationen fremder Staaten oder gar Terroristen – sie alle stellen realistische Bedrohungen dar. Sicherheit ist nicht Selbstzweck. Sie soll dazu beitragen, dass die Geschäftsprozesse der Unternehmen funktionieren und dass Geld verdient wird. Eine sichere IT ist dafür unabdingbar, aber das sichere Funktionieren der Geschäftsprozesse hängt nicht nur von sicherer IT ab.

Wenn wichtige Informationen verfälscht werden oder ungewollt das Unternehmen verlassen, wenn geplante Umsätze nicht gemacht werden können, weil Prozesse nicht laufen, dann ist es egal, ob fehlerhafte IT-Sicherheit oder andere Gründe dazu geführt haben. Der Schaden für das Unternehmen ist unabhängig vom Warum.

Technik allein genügt nicht | Zur ganzheitlichen Absicherung von Informationen und Prozessen reicht technische (IT-)Sicherheit allein nicht aus. Adäquate Sicherheit wird erst erreicht, wenn ein unternehmensweites Sicherheitskonzept neben der Technik auch die Dimensionen Organisation und Personal betrachtet und absichert. Sicherheit funktioniert top-down, der effiziente Ansatz zur Schaffung von ganzheitlicher Unternehmenssicherheit beginnt mit den Fragen: „Womit verdient unser Unternehmen das Geld?“ und „Was sind unsere Kronjuwelen?“ Die Antworten, die die Unternehmensleitung auf diese Fragen gibt, definieren unmittelbar, welche Prozesse und Werte am dringlichsten zu schützen sind.

Nun wird das weitere Vorgehen an einen entsprechend positionierten Experten übergeben, der unternehmensweit und ganzheitlich die erforderlichen Maßnahmen plant, mit der Leitung abstimmt, umsetzt und überwacht. Er arbeitet von den Haupt-Geschäftsprozessen und wertvollsten Assets auf oberster Ebene sukzessive ins Detail und sichert alle beteiligten und unterstützenden Prozesse, Systeme und Werte so, dass der Schutzbedarf der obersten Ebene erreicht werden kann. Dabei folgt er bei der Bewertung von Bedrohungen und Maßnahmen einer definierten Risikostrategie des Unternehmens. Die Maßnahmen umfassen Technik, Organisation und Personal und sichern gemeinsam die Fitness und die Zukunft des Unternehmens.

„Es wird schon nichts passieren“ | Die heutige Realität in vielen Firmen ist aber, dass Sicherheitsmaßnahmen von der IT-Abteilung, von einzelnen Führungskräften oder Mitarbeitern für ihren Bereich umgesetzt werden. Damit werden zwar einige durchaus prominente Aspekte der Sicherheit abgearbeitet, aber ein strategisch abgestimmter und das ganze Unternehmen ausgewogen und wirtschaftlich schützender Weg ist damit nicht beschritten. Die Verantwortung für Sicherheit liegt bei der Geschäftsleitung. Sie wird zum Nachteil der Unternehmen teilweise nicht richtig wahrgenommen. Oft wird davon ausgegangen, die Erfüllung von Compliance-Anforderungen sei hinreichend, Sicherheit sei „natürlich“ gegeben, und es werde schon nichts passieren.

Die Informationen des Verfassungsschutzes, des BSI, die einschlägigen Blogs und Tweets von „Aktivisten“ und nicht zuletzt immer mehr die Berichte in den Medien belegen anderes: Schäden grassieren. Es sind nicht mehr nur Hacker, die für „Ruhm und Ehre“ in der Szene Schwachstellen publizieren und damit Firmen öffentlich blamieren. Es sind Profis, die sich auf das Ausspähen von Geheimnissen und auf Sabotage spezialisiert haben, und die ihr Geschäft verstehen. Daher der Appell an alle Chefs: Machen Sie ganzheitliche Unternehmenssicherheit zu Ihrem Thema. Beauftragen Sie Experten und lassen Sie sie direkt an Sie berichten. Statten Sie sie mit Einfluss und Ressourcen aus. Schaffen Sie Bewusstsein für Sicherheit bei Ihren Mitarbeitern auf allen Ebenen. Und leben Sie Sicherheit konsequent vor!