

IT-SECURITY | 2/2009, S. 13

„Neue Technologien brauchen Sicherheit“



Worin sehen Sie die derzeit wichtigsten Entwicklungen in der IT-Sicherheit?

Wir können für die Zukunft eine rasant ansteigende Komplexität der IT-Systeme erwarten. Diese Komplexität bietet in vielfältiger Weise An-

griffstellen. Neue Technologien werden sich aber nur dann durchsetzen, wenn Vertrauen in ihre Sicherheit besteht. Besonders beim Cloud Computing ist dies ersichtlich. Die Auslagerung und der vernetzte Zugriff auf kritische Unternehmensdaten lässt Bedenken entstehen, die nur mit überzeugenden Lösungen ausgeräumt werden können. Insgesamt denke ich, dass der Stellenwert der IT-Security bei den Unternehmen angekommen ist, denn auch in der Wirtschaftskrise hat sich der Security-Markt als robust erwiesen.

Zunächst ist das fachliche Know-how qualifizierter Mitarbeiter gefragt, die auf dem neuesten Stand der Technik sind und die kriminellen Aktivitäten beispielsweise in Form von Computerviren, schädlichen Links und PDFs, SQL-Injection- und Phishing-Attacks oder Trojanern intensiv verfolgen, um entsprechende Abwehrmaßnahmen präventiv vorzunehmen. Ein guter IT-Sicherheitsleiter wird aber gleichzeitig nicht nur rein technische Lösungen entwickeln, sondern das Unternehmen insgesamt in den Blick nehmen und ein Informationssicherheitsmanagement entwickeln.

Was sind Ihrer Meinung nach die besten Abwehrmaßnahmen gegen IT-Angriffe?

Hierzu gehört beispielsweise die Klassifikation von Daten gemäß ihrer Wichtigkeit oder die verbindliche Festlegung von Sicherheitsregeln. Diese müssen dann allerdings auch den Mitarbeitern in Schulungen vermittelt werden. In der Hitze des geschäftlichen Alltags werden Sicherheitsregeln gerne vernachlässigt, ohne dass eine böswillige Absicht besteht. Die spektakulären Fälle von illegalem Datenhandel und Datenklau zeigen, dass die Daten nicht mit aufwendigen technischen Systemen entwendet wurden, sondern mittels USB-Stick oder CD-Rom.

Was gehört zu einem solchen Management dazu?

Hierzu gehört beispielsweise die Klassifikation von Daten gemäß ihrer Wichtigkeit oder die verbindliche Festlegung von Sicherheitsregeln. Diese müssen dann allerdings auch den Mitarbeitern in Schulungen vermittelt werden. In der Hitze des geschäftlichen Alltags werden Sicherheitsregeln gerne vernachlässigt, ohne dass eine böswillige Absicht besteht. Die spektakulären Fälle von illegalem Datenhandel und Datenklau zeigen, dass die Daten nicht mit aufwendigen technischen Systemen entwendet wurden, sondern mittels USB-Stick oder CD-Rom.

Was können Sie als IT-Mittelstandsverband für eine sichere IT leisten?

Wir können zum Beispiel aus mittelständischer Sicht darauf hinweisen, dass auf politischer Ebene die Standardisierung von elektronischen Systemen und Sicherheitsbestimmungen international vorangetrieben werden muss, um die Komplexität zu beherrschen und besonders neuralgische Punkte wie die beispielsweise die webbasierten Zahlungssysteme zu schützen. Damit bieten wir mittelständischen Unternehmen die Möglichkeit, ihr Gesicht zu zeigen und sich Gehör zu verschaffen – nicht gegenüber der Politik, sondern auch gegenüber den IT-Konzernen.