

➤ Ein Kommentar von Wilfried Pruschak, Raiffeisen Informatik.

Durchdachte Sicherheit

Daten und IT-Services müssen zu 100 % geschützt werden. Nur wer umfassende Securitymaßnahmen im Repertoire hat, sollte IT-Leistungen in der Wirtschaft anbieten.

Informationen sind ein integraler Bestandteil unserer Gesellschaft. Sie durchdringen das private und vor allem das berufliche Umfeld jedes Einzelnen. Zur Verarbeitung von Informationsdaten wird hauptsächlich die IT herangezogen, die sich somit zusehends zum Lebensnerv der Unternehmen entwickelt. Denn kaum mehr ein Unternehmen kann von sich behaupten, unabhängig von IT zu sein. Kommt es zu IT-Ausfällen, kann dies zu Problemen im Geschäftsablauf führen. IT hat sich somit zur kritischen Komponente beziehungsweise zum Rückgrat der Unternehmen entwickelt, welches es gilt, entsprechend zu schützen. Vor allem in Rechenzentren, wo die IT von vielen Unternehmen verwaltet wird, ist es besonders wichtig, durchdachte Sicherheitskonzepte zu erstellen.

Dabei tragen sowohl der physische als auch der virtuelle Schutz zur umfassenden Informationssicherheit bei. Physisch umfasst der Schutz vor allem Gebäude- und Zutrittskontrollen. Angefangen von Videoüberwachung, Bewegungsmeldern, Zutrittsberechtigungen in verschiedenen Sicherheitszonen bis hin zum Mehraugenprinzip in hochsensiblen Bereichen erstreckt sich die breite Palette der möglichen Sicherheitsmaßnahmen. Auch sind Vorkehrungen zum Schutz vor höherer Gewalt wie Wassereinbruch oder Brand zu treffen. Obligatorische Schutzübungen, um im tatsächlichen Notfall einen koordinierten und effektiven Einsatz zu ermöglichen, sind hier jedoch nicht ausreichend. Es müssen auf jeden Fall auch Notfallpläne zur Aufrechterhaltung der wesentlichen Geschäftsprozesse existieren.

Aber auch virtuell müssen Daten vor Verlust, Diebstahl und Missbrauch geschützt werden. Vor allem der Zugang zu unter-



Wilfried Pruschak, Raiffeisen Informatik, prägte den Slogan »IT muss so sicher sein, wie Strom aus der Steckdose«.

nehmenskritischen Informationen muss gut kontrolliert und gesichert sein, um die Informationen vor unbefugtem Zugriff – beispielsweise durch Hackerangriffe – zu schützen. Hier bedarf es einer intensiven Beschäftigung mit dem Thema Security, um die ständig wachsenden Herausforderungen effektiv meistern zu können. Der Zusammenschluss in Netzwerken, wie beispielsweise dem österreichweit agierenden und international vernetzten »Computer Emergency Response Team (CERT)«, ist eine gute Möglichkeit für Sicherheitsexperten, einen deutlichen Informations- und somit auch Handlungsspielraum durch den Austausch von Wissen und Erfahrung zu erlangen. Weiters hilft ein wasserdichtes Berechtigungssystem im Bereich »Identity und Access Management (IAM)« bei der

“IT hat sich zur kritischen Komponente bzw. zum Rückgrat der Unternehmen entwickelt.”

Identifikation sowohl von Benutzern, die auf Daten zugreifen, als auch von Infrastruktur, auf der sich die Daten befinden. Solche Systeme sind essentiell, denn viele Unternehmen managen ihre Benutzer-Accounts und Zugriffsberechtigungen noch sehr undurchgängig. Das Resultat sind ineffiziente Prozesse mit hohem manuellen und materiellen Aufwand, vielen Fehlerquellen und großen Sicherheitsrisiken.

Sämtliche Maßnahmen zur Informationssicherheit können durch periodische Schulungen, Business-Continuity-Tests und Disaster-Recovery-Pläne wirkungsvoll unterstützt werden. Auch ein durchdachtes Risikomanagement und in Zusammenhang mit Sicherheitsthemen ermittelte Kennzahlen, welche in periodischen Reviews erhoben werden, bieten hier eine gute Möglichkeit, potenziellen Abweichungen in der Sicherheitskonzeption zeitgerecht entgegenzuwirken. □

ZUM AUTOR

➤ **Mag. Wilfried Pruschak** ist seit 1996 Geschäftsführer des größten österreichischen IT-Anbieters Raiffeisen Informatik und seit 2009 Aufsichtsratsvorsitzender der Konzerntochter Comparex AG. Der Raiffeisen Informatik Konzern wird in 2012 mit rund 2.800 Mitarbeitern an 100 Standorten in 30 Ländern einen Umsatz von rund 1,5 Milliarden Euro erzielen.