SparkassenZeitung

12. Februar 2016 - 11:52 | Interview

Lage hat sich verschärft

Existenzielle Geschäftsprozesse in den Sparkassen basieren auf IT. Entsprechend sind Sicherheitslösungen von entscheidender Bedeutung für die Funktionsfähigkeit der IT. Die Sparkassenzeitung sprach mit Benno Rieger, Geschäftsführer der SIZ GmbH, über sicherheitsrelevante Aspekte.

Benno Rieger, SIZ-Geschäftsführer.

(SIZ)

DSZ: Vor welchen Herausforderungen stehen heute die IT-Abteilungen der Sparkassen gerade in puncto IT-Sicherheit ?

Rieger: Ich möchte hier auf drei zentrale Herausforderungen eingehen: Erstens befindet sich der Bankenmarkt nach wie vor in einer wachsenden Digitalisierung - man denke nur an das Browser- und Mobile-Banking. Um diesen Bewegungen gerade auch in der IT zu begegnen, sind rasche Anpassungen und Veränderungen wichtig. Durch die elektronischen Kanäle gewinnen neue Bedrohungen an Bedeutung, die zusätzlich besonders agile Angreifer versuchen auszunutzen. Zweitens sind in den vergangenen Jahren die regulatorischen Anforderungen an die Banken-IT stark gewachsen, sowohl in Hinsicht auf Prüfungen als auch auf Meldepflichten. Beides findet zu großem Teil Niederschlag in der IT-Sicherheit. Drittens stehen alle Banken unter einem erheblichen Margendruck. Steigende Budgets zur Erarbeitung von IT-Sicherheitslösungen passen nur schlecht dazu.

DSZ: Viele Sparkassen stehen vor der Aufgabe, auch in der IT immer mehr Einsparungspotenzial zu generieren. Ist dies überhaupt möglich, ohne die IT-Sicherheit zu gefährden ?

Rieger: Grundsätzlich ja, wenngleich es nicht immer ganz einfach ist. Zunächst bietet es sich an, beim Einsatz von IT jeweils zu prüfen, ob nicht geeignete Dienstleister zur Verfügung stehen, die mit Ihrem Spezialwissen in der IT bzw. mit ihren Anwendungen für ein den Anforderungen entsprechendes Sicherheitsniveau sorgen können. Beim Institut verbleiben dann die Steuerungs- und Überwachungsaufgaben im Rahmen der Dienstleistersteuerung. Hierfür ist Sicherheits-Know-how notwendig. Viele Institute

kaufen dieses Know-how ergänzend in Form von langfristig angelegten Unterstützungen bei Sicherheitsdienstleistern wie der SIZ GmbH zusätzlich ein. Bei Prüfern findet dieses Modell Anerkennung.

DSZ: Die Angriffe auf die IT-Systeme auch der Sparkassen nehmen zu. Ist die Sparkassen-Finanzgruppe jeweils auf dem gleichen Stand der Dinge wie die Angreifer, oder hinkt man hinterher ?
Rieger: Ja, es lässt sich feststellen, dass sich die Bedrohungslage verschärft hat. Aber nicht nur für die Sparkassen # dies gilt für alle Branchen. Traditionell hat das Thema Informationssicherheit in der Finanzbranche aber eine zentrale Bedeutung. So sind heute umfassende technische und organisatorische Sicherheitsmaßnahmen Standard. In der Sparkassen-Finanzgruppe zeigt sich dies etwa in den dezentralen Maßnahmen in den Instituten sowie in zentralen Maßnahmen der IT-Dienstleister. Um aber auch künftig auf Ballhöhe mit den Angreifern zu bleiben, hat der DSGV schon im Jahr 2014 einen übergreifenden Lage- und Reaktionsmechanismus als Reaktion auf die aufkommenden Cyber-Attacken etabliert. Dieser Mechanismus besteht unter anderem in einem Betrugsabwehrteam, das bei der Finanz Informatik angesiedelt ist. Weitere zentrale Komponente ist ein sogenanntes Cyber-Abwehrteam, das operativ vom S-Cert (Computer-Notfallteam der Sparkassen-Finanzgruppe) unseres Hauses betrieben wird. Die Experten dieses Teams setzen sich schon seit vielen Jahren mit Bedrohungen und Angriffen auseinander. Durch die tägliche Abwehr unterschiedlichster Angriffe ist dort schon seit vielen Jahre großes Expertenwissen hinsichtlich Angreifergruppen und deren Methoden vorhanden. Ständig arbeiten unsere S-Cert-Experten auch daran, neue Angriffsmethoden früh zu erkennen und zu verstehen sowie geeignete Gegenmaßnahmen zu erkennen und zu kommunizieren. Eine Aufgabe, die in Zukunft noch an Bedeutung gewinnen wird.

DSZ: Zur Absicherung der Kerngeschäftsprozesse bietet das SIZ Dienstleistungen zu Business-Continuity-Management an. Sind damit auch sicherheitsrelevante Szenarien abgedeckt ?
Rieger: Die Antwort lautet. Ja! Beim Business Continuity Management geht es darum, die wichtigsten Geschäftsprozesse des Unternehmens auch in Notfallsituationen aufrechterhalten zu können. Szenarien, die zu Notfällen führen können, umfassen dabei neben der IT auch alle anderen wichtigen Ressourcen wie etwa Mitarbeiter, Räume oder die relevanten Dienstleister. Wie Sie sehen, wird hier „Sicherheit“ weit gefasst und abgedeckt.

DSZ: Das Produkt "Sicherer IT-Betrieb" dient den Sparkassen dazu, die Integrität, Verfügbarkeit und Vertraulichkeit ihrer Informationen zu gewährleisten. Gilt dies auch für den menschlichen Faktor?
Rieger: „Sicherer IT-Betrieb“ dient dazu, ein Informationssicherheits-Managementsystem aufzubauen, das ganzheitlich die Anforderungen an die von Ihnen beschriebenen Anforderungen an die Sicherheit behandelt - so wird das ja auch von der einschlägigen Bankenregulierung wie etwa den MaRisk gefordert. Im Unterschied zur reinen IT-Sicherheit werden hierbei natürlich auch die menschlichen Faktoren wie etwa Vorgaben für die Kommunikation in der Öffentlichkeit oder den Umgang mit Passwörtern berücksichtigt. Die notwendigen Sensibilisierungen der Mitarbeiter und Externen müssen dann vor Ort erfolgen.

Das Gespräch führte Thomas Volk.