

Das schwächste Glied in der Kette

Das Internet ist für Finanzinstitute ein wichtiger Kommunikationskanal geworden. Dabei wird der Sicherheit nicht bei allen Projekten die nötige Aufmerksamkeit geschenkt. Doch Webauftritte und Anwendungen müssen professionell betrieben werden. Kaspar Geiser

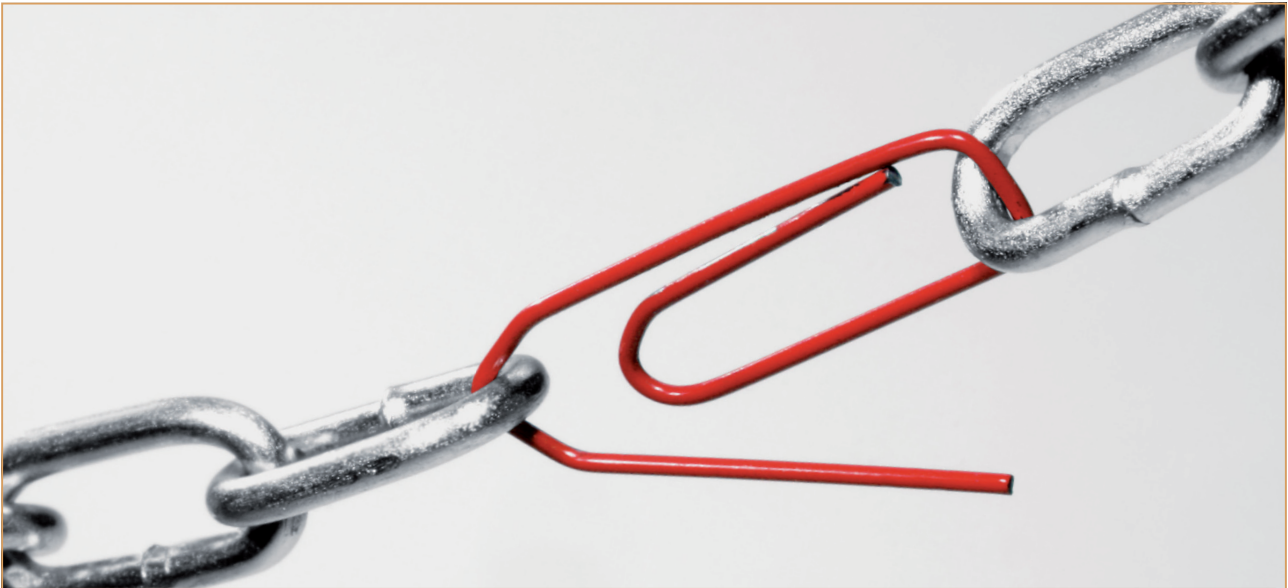


Kaspar Geiser

ist Geschäftsführer und
Mitinhaber der Aspectra AG.
kaspar.geiser@aspectra.ch

Finanzinstitute nutzen das Internet, um ihre Dienstleistungen zu erbringen und für die (Marketing-)Kommunikation. Egal ob E-Banking, Corporate Website oder bloss kleine und kurzfristige Webauftritte und Anwendungen – sie müssen professionell betrieben werden. Andernfalls besteht die Gefahr, dass sie als schwächstes Glied in der Kette als Tor für Angriffe missbraucht werden.

Das Internet ist für Finanzinstitute zu einem wichtigen Kommunikationskanal geworden. Immer mehr Dienstleistungen, Marketingaktivitäten und Informationen werden via Internet Interessierten angeboten. Die Corporate Website sowie ein E-Banking werden meist durch eine Projektorganisation begleitet und über eine lange Zeit entwickelt, getestet und in Betrieb genommen. Dabei werden den Sicherheitsrisiken die nötige Aufmerksamkeit geschenkt und die entsprechenden Massnahmen umgesetzt. Dies ist aber nicht bei allen Projekten der Fall: Mit immer neuen Anwendungen und Anforderungen aus dem Markt verlagern sich immer mehr Bedürfnisse beziehungsweise deren Lösung ins Internet. So werden beispielsweise Internetseiten für einzelne Events gebaut, die nur einige Wochen in Betrieb sind. Auch werden Versuche in den «Social Media» gewagt oder gar die Nutzung einer kompletten Anwendung irgendwo in der «Cloud». Und natürlich besteht dabei auch der Wunsch, dass sich Kunden oder Mitarbeiter auf diesen Anwendungen einloggen können und Zugriff auf eigene Daten in diesen Anwendungen haben. Dies impliziert, dass unter Umständen vertrauliche Daten oder Daten, die aus Sicht eines Angreifers interessant sind, auf irgendwelchen Systemen ausserhalb einer Bank-IT auftauchen. Eine weitere Herausforderung sind die eingesetzten Anwendungen. Heute sind im Markt zum Beispiel fixfertige Redaktionssysteme als komplette Software vorhanden. Diese sind schnell in Betrieb und einfach bedienbar. Das heisst, eine interne Redaktion publiziert



Webauftritte und Anwendungen müssen professionell betrieben werden. Andernfalls besteht die Gefahr, dass sie als schwächstes Glied in der Kette als Tor für Angriffe missbraucht werden. Bildquelle: Fotolia

nur noch die Inhalte auf diesen Systemen. Die Zugriffsmechanismen in solche Systeme, beispielsweise via ein Single-Sign-on, oder die Vertraulichkeit der erfassten Artikel sind für den Anwender oft nicht durchschaubar.

Anforderung an das Finanzinstitut

Sicherheit bedeutet Aufwand. Sicherheit hat aber auch sehr viel mit Sensibilisierung und Ausbildung zu tun. Daher ist wohl eine der wichtigsten Aufgaben eines Unternehmens, sämtliche Business Owners zu schulen, wo die Gefahren liegen und die eigenen Richtlinien bezüglich des Datenschutzes zu kommunizieren. Was die Technik angeht, so wäre es natürlich wunderbar, wenn die unternehmenseigene IT sämtliche Anwendungen und Internetauftritte selbst entwickeln und betreiben könnte. Dies hat bestimmt schon manches Unternehmen versucht, mit dem Resultat, dass es sehr lange dauert, bis eine Anwendung in Betrieb geht oder die Kosten für die technische Umsetzung nicht mehr im Verhältnis zum Nutzen stehen. Die Anforderung, alles in den eigenen vier Wänden zu produzieren, wird mit den Social Media wie Facebook oder Twitter beinahe unmöglich. Es empfiehlt sich also, nicht bloss System- und Entwicklungsspezialisten in seinen Reihen zu halten, sondern auch die Rolle des Architekten oder der Sicherheitsbeauftragten zu stärken. Diesen Mitarbeitern ist es möglich, auch ohne grossen Aufwand Lösungsvorschläge von zum Beispiel Marketingagenturen und Webentwicklern zu beurteilen.

Zusammenarbeit mit Dritten

Um interne wie externe Anwendungen mit der nötigen Sicherheit sowie ohne Überschreitung von Kosten und Terminen zu realisieren, empfiehlt es sich, einen Teil dieser Anwen-

dungen bei spezialisierten Unternehmen zu betreiben. Die Anforderungen an einen solchen Partner entsprechen denselben, die an die interne IT-Organisation gestellt werden. Doch da sich ein solcher Partner «nur» auf den Betrieb konzentriert, kann er dies dank spezialisiertem Personal und der nötigen Technik sicher und kostengünstig anbieten. Um die bestmögliche Sicherheit und Qualität zu erlangen, empfiehlt es sich, insbesondere die Organisation beziehungsweise die Rollentrennung eines solchen Dienstleisters zu durchleuchten. Sinnvollerweise sind mindestens folgende Aufgaben verschiedenen Rollen zugeordnet: physische Sicherheit, Netzwerksicherheit, Verantwortung für die Server und deren Betriebssystem sowie Verantwortung für die Applikation. Sind

diese Rollen nicht klar voneinander getrennt, und wird zum Beispiel die Netzwerksicherheit durch dieselben Personen verantwortet, die

beispielsweise auch das Betriebssystem eines Servers unterhalten, kann dies die Sicherheit beeinträchtigen.

Transparenz und Kontrollen

Auch wenn es sich um kleine oder im ersten Moment unwichtige Anwendungen handelt, muss der Überwachung beziehungsweise dem Reporting durch einen Drittanbieter Aufmerksamkeit geschenkt werden. Management-Cockpits, die über die Verfügbarkeit und Performance Auskunft geben, sind wertvolle Instrumente für die Auftraggeber und Finanzinstitute und deren interne IT- und Sicherheitsverantwortliche. Auch ist dank solcher Tools eine sichere Kommunikation zwischen Finanzinstitut und dem IT-Dienstleister erst möglich. Testate über externe Zertifizierungen oder besser Prüfverfahren, die zum Beispiel von Kreditkartenfirmen (PCI DSS) oder Finanzinstituten (PS 402, FINMA) gefordert werden, können von IT-Dienstleistern ebenfalls gefordert werden. ■

«Sicherheit bedeutet Aufwand. Sicherheit hat aber auch sehr viel mit Sensibilisierung und Ausbildung zu tun.»