

Das E-Banking ist sicher. Was ist mit dem Rest?

Die meisten Finanzinstitute haben das E-Banking via PC im Griff. Die Kunden und das Business verlangen aber immer neue Anwendungen, die auf allen denkbaren Geräten verfügbar sein sollen. Damit stellt sich schnell die Frage nach der Sicherheit. Kaspar Geiser



Kaspar Geiser
ist Managing Director und
Inhaber der Aspectra AG.
kaspar.geiser@aspectra.ch

Finanzinstitute nutzen das Internet für unterschiedliche Zwecke. Einerseits erbringen sie immer mehr Dienstleistungen für ihre Kunden online. Andererseits sind aber auch für Banken die Onlinemedien immer wichtigere Instrumente für die Marketingkommunikation. Wie auch immer eine Bank das Internet einsetzt, ob für E-Banking, die Corporate Website, Mobile-Apps oder bloss kleine und kurzfristige Webauftritte und Anwendungen: Alle Applikationen müssen professionell betrieben werden. Andernfalls besteht die Gefahr, dass sie als Tor für Attacken missbraucht werden.

Das Internet ist für Finanzinstitute zu einem wichtigen Kommunikationskanal geworden. Immer mehr Dienstleistungen, Marketingaktivitäten und Informationen werden via Internet Interessierten angeboten. Der Aufbau der Corporate Website oder des E-Banking wird im Idealfall durch eine Projektorganisation begleitet, über eine gewisse Zeit entwickelt, getestet und in Betrieb genommen. Dabei wird den Sicherheitsrisiken die nötige Aufmerksamkeit gewidmet, und es werden die entsprechenden Massnahmen umgesetzt. Dies ist allerdings 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. Kommt dazu, dass viele Trends ausgesprochen schnelllebig sind und gerade die Kommunikationsabteilungen zu schnellem Handeln gezwungen sind. So werden beispielsweise Internetseiten für einzelne Events gebaut, die bloss einige Wochen in Betrieb sind. Oder es werden Versuche in den Social Media durchgeführt oder gar die Nutzung einer kompletten Anwendung irgendwo in die Cloud verschoben. Der jüngste Trend sind Mobile-Apps, die eine Mischung aus Marktinformationen und persönlichen Daten verwenden.



Sicherheit hat sehr viel mit Sensibilisierung und Ausbildung zu tun. Daher gehört es zu den wichtigsten Aufgaben, sämtliche Business Owners hinsichtlich der Gefahren zu schulen und die Datenschutzrichtlinien zu kommunizieren. Bildquelle: Fotolia

All dies hat zur Folge, dass unter Umständen sensible Personendaten oder Daten, die aus Sicht eines Angreifers interessant sind, auf irgendwelchen Systemen ausserhalb einer Banken-IT auftauchen. Eine weitere Herausforderung sind die eingesetzten Anwendungen. Heute werden im Markt zum Beispiel fixfertige Redaktionssysteme als komplette Software angeboten. Diese sind schnell in Betrieb genommen und einfach zu bedienen. Eine interne Redaktion publiziert dann nur noch die Inhalte auf diesen Systemen. Die Zugriffsmechanismen auf solche Systeme, beispielsweise via ein Single Sign-on, oder wie die Sicherheit der Daten gewährleistet ist, lässt sich kaum nachvollziehen. Dies führt dazu, dass sich die markt- und kundenorientierten Abteilungen einem Zielkonflikt ausgesetzt sehen: Einerseits sollen sie schnell und flexibel auf die Bedürfnisse der Kunden und die Entwicklungen im Markt eingehen. Andererseits müssen sie bei der Zusammenarbeit mit der internen IT sehr restriktive Anforderungen an die Sicherheit erfüllen. Das Resultat ist, dass sie sich an externe Dienstleister wenden und der internen IT die Kontrolle entgleitet. Das muss nicht zu einem Problem werden, setzt aber voraus, dass der externe Partner dieselben oder höhere Ansprüche an die Sicherheit erfüllt wie die eigene IT.

Herausforderungen für das Finanzinstitut

Sicherheit bedeutet Aufwand. Einerseits sind bei der Planung und Realisierung von Applikationen und Infrastrukturen höhere Anforderungen zu erfüllen und strengere Restriktionen zu berücksichtigen. Andererseits ist im Betrieb die Nutzung sowohl für den Anbieter als auch die Kunden aufwendiger: Strichlisten, Matrixkarten oder Secure ID

Tokens müssen produziert, versandt und ersetzt werden. Bei jedem Log-in müssen die Kunden User-ID, Passwort und eine TAN eingeben.

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 betreffend Datenschutz zu kommunizieren. Nur so können diese einigermassen dezentralisiert und ohne bremsenden Flaschenhals agieren, ohne die Sicherheit zu kompromittieren.

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. Grund dafür sind nicht nur die hohen Sicherheitsanforderungen. Auch die Palette der verschiedenen Clients, Applikationen und Kanäle hat zugenommen. Früher genügte eine Website, die über einen PC-Browser angesteuert wurde. Das höchste der Gefühle war, wenn man über die Website Zugriff auf das Portfolio und das E-Banking hatte und die Bank regelmässig eine Newsmeldung publizierte. Heute wollen die Kunden nicht nur über den PC, sondern auch über Tablets und Mobiltelefone Bankgeschäfte erledigen. Zusätzlich müssen externe Anwendungen wie Facebook und Twitter sowie Datenfeeds wie Bloomberg eingebunden werden.

Diese zunehmende Komplexität erfordert Know-how, über das die IT-Abteilung nur in Ausnahmefällen verfügt. ►

«Die zunehmende Komplexität erfordert Know-how, über das die IT-Abteilung nur in Ausnahmefällen verfügt.»



Sicherheit bedeutet Aufwand, es sind höhere Anforderungen zu erfüllen und strengere Restriktionen zu berücksichtigen. Bildquelle: Fotolia

Es empfiehlt sich daher, nicht bloss System- und Entwicklungsspezialisten in den eigenen Reihen zu halten, sondern auch die Rolle des Architekten oder der Sicherheitsbeauftragten zu stärken. Diese können auch ohne grossen Aufwand Lösungsvorschläge von zum Beispiel Marketingagenturen und Webentwicklern beurteilen.

Zusammenarbeit mit Externen

Um interne wie externe Anwendungen mit der nötigen Sicherheit und ohne Überschreitung von Kosten und Terminen zu realisieren, empfiehlt es sich, einen Teil dieser Anwendungen bei spezialisierten Unternehmen entwickeln und betreiben zu lassen. 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 bei der Evaluation einen Anbieter zu erkennen, der bestmögliche Sicherheit und Qualität anbietet, empfiehlt es sich, insbesondere die Organisation beziehungsweise die Rollentrennung eines solchen Dienstleisters zu durchleuchten. Sinnvollerweise sind mindestens folgende Aufgaben verschiedenen Rollen zugeordnet: (1) Physische Sicherheit, das heisst der Zutritt zum Rechenzentrum und der physische Zugriff auf die Systeme; (2) Netzwerksicherheit, das heisst die Verantwortung für Firewalls, Paketfilter und Reverse Proxies; (3) Verantwortung für die Server und deren Betriebssystem; (4) 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.

Wichtig ist bei der Wahl des Dritten auch die Kompatibilität. Einerseits sollten die Grössenverhältnisse nicht zu stark divergieren: Wenn zum Beispiel ein kleines oder mittleres Unternehmen eine Grossfirma als externen Partner beauftragt, läuft es Gefahr, spätestens nach Abschluss der Projektphase an Priorität zu verlieren. Andererseits sollten die Ansprechpartner auf beiden Seiten ähnlich ticken. Am besten ist es, wenn sie sich kennen und keine hohe Fluktuationsrate haben. Probleme lassen sich unter diesen Voraussetzungen viel schneller und effizienter lösen.

Transparenz und Kontrollen

Auch wenn es sich um kleine oder auf den ersten Blick 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 die internen IT- und Sicherheitsverantwortlichen. Auch ist dank solcher Tools eine sichere Kommunikation zwischen Finanzinstitut und dem IT-Dienstleister erst möglich. Online-Echtzeit-Systeme sind dabei dem monatlichen Bericht in schriftlicher oder mündlicher Form vorzuziehen.

Testate über externe Zertifizierungen (z.B. ISO 27001) oder besser Prüfverfahren, die von Kreditkartenfirmen (z.B. PCI DSS) oder Aufsichtsbehörden (z.B. FINMA) gefordert werden, können vom IT-Dienstleister ebenfalls gefordert werden. Solche Zertifizierungen geben einen Hinweis auf die Professionalität des Anbieters. Sie entbinden aber nicht von der Pflicht, diesen zusätzlich kritisch zu hinterfragen. ■