



DOSSIER E-BANKING IN KOOPERATION MIT ASPECTRA

Sicherheit hängt von Mitarbeitern ab, die sich darum kümmern

rmo. In ihrer neusten Studie «IT-Sicherheit in Deutschland» hat IDC gut 200 Unternehmen mit mehr als 100 Mitarbeitenden befragt. Dabei ist herausgekommen, dass die Abwehr neuer Angriffsszenarien, die Cloud-Security und die Sicherheit mobiler Endgeräte als die drei wichtigsten Herausforderungen eingestuft werden. Als wichtigste Hindernisse stehen das mangelnde Risikobewusstsein der Mitarbeitenden, die Budgetsituation und die steigende Komplexität weit oben auf der Liste. Klar, Deutschland ist nicht die Schweiz. Aber tendenziell dürften sich die hiesigen Firmen mit sehr ähnlichen Problemen herumschlagen. Das lässt sich zumindest anhand dessen vermuten, was man in Gesprächen mit Fachleuten zu hören bekommt. Zurück zur Studie: In ihrer Mischung könnten die dort identifizierten Teilprobleme ziemlich giftige Rückkopplungsmechanismen auslösen. Ungenügende Budgets dünnen ja nicht nur

Ressourcen und Investitionen aus, sondern sorgen auch für unzufriedene Mitarbeiter. Unzufriedene Mitarbeiter wiederum wandern ab und damit verschwindet Know-how. Dies wäre aber dringend nötig, um den rasch wechselnden Bedrohungsszenarien zu begegnen.

Unter solchen Umständen könnte die Auslagerung von Sicherheitsaufgaben etwas entlasten. Wird das Thema richtig angegangen, dann ermöglichen externe Dienstleister plötzlich Massnahmen, für die die eigene IT bisher weder Zeit noch Geld hatte. Aber damit das gelingt, braucht es jemanden, der die eigenen Systeme und Prozesse im Detail versteht. Es braucht jemanden, der die Auslagerung korrekt aufsetzen, begleiten und steuern kann. In diesem Sinne lohnt es sich, wie Hannes Lubich im Interview auf Seite 29 empfiehlt, gerade während Sparübungen die guten Leute unbedingt zu halten.

- > **Seite 28**
Das E-Banking ist sicher. Was ist mit dem Rest?
- > **Seite 29**
Hannes Lubich, Fachhochschule Nordwestschweiz: «Der wesentliche Angriffspunkt ist das Endgerät des Kunden»

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 möglichst schnell auf allen denkbaren Geräten verfügbar sein sollen. Damit stellt sich schnell die Frage, ob die Sicherheit der sensiblen Daten noch gewährleistet ist. Kaspar Geiser

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.



Kaspar Geiser ist Managing Director und Inhaber der Aspectra AG.

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 fordert Know-how, über das die IT-Abteilung nur in Ausnahmefällen verfügt. 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 Prüfvorgehen, 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. <

«Der wesentliche Angriffspunkt ist das Endgerät des Kunden»

Hannes Lubich, Dozent für ICT System Management an der FHNW, erläutert, wo es mit der Sicherheit in der Banken-IT hapert, wo die Risiken bei E-Banking liegen und was getan werden müsste. Interview: René Mosbacher

Herr Lubich, wo liegen heute die grossen Baustellen bei der IT-Sicherheit in der Finanzbranche?

Die grösste ist der Druck auf die Fixkosten der IT. IT-Sicherheit ist personalgetrieben, und das verursacht eben Fixkosten. Die zweite Baustelle ist die Auslagerung von IT-Betrieben an externe Anbieter. Hier fragt sich, unter welchen Bedingungen das für die hochregulierte und sicherheitssensitive Bankenbranche möglich ist. Als Nächstes fällt mir die steigende Komplexität auf, die mit der zunehmenden Virtualisierung einhergeht und zusätzliche Risiken mit sich bringt. Ein weiteres Problem sind die intelligenten Endgeräte, auf die sehr viele Funktionen ausgelagert werden. Egal, ob Sie sie für die Fernwartung oder fürs Telebanking einsetzen – sie bergen Risiken. Der letzte Punkt schliesslich ist, dass die Integration der IT-Sicherheit in das übergelagerte Risiko- und Compliance-Management nicht so einfach ist, wie oft angenommen wird. Die IT-Sicherheit denkt ab und zu noch stark in technischen Silos, während das Risiko- und Compliance-Management eher abstrakte Servicemodelle einsetzt.

Man kann also sagen, dass sich die IT-Sicherheit verschlechtert hat, weil die Budgets gekürzt wurden?

Ja. Ich denke, dass wir eine erhöhte Bedrohungslage aufgrund mangelnder IT-Security-Budgets haben. Es sind aber noch wenige Schadensfälle bekannt, die man direkt darauf zurückführen könnte. Das erschwert die Argumentation.

Welchen Stellenwert hat das IT-Risiko im Vergleich zu den übrigen Risiken in der Finanzbranche?

Im Verhältnis zu den übrigen Risiken spielt die IT-Sicherheit bei den Banken derzeit noch keine grosse Rolle. Die Schäden durch klassischen Betrug oder Systemausfall sind sicher noch um einiges höher. Bezüglich Schadenpotenzial hingegen steufe ich die IT-Sicherheit eher hoch ein.

Wo sind heute die typischen Einfallstore für Cyberkriminelle?



Hannes Lubich ist Dozent für ICT System Management an der Fachhochschule Nordwestschweiz

«Besonders interessant ist Managed Security für mittelgrosse Unternehmen.»

Der wesentliche Angriffspunkt heute ist das Endgerät des Kunden. Hier liegt vieles im Argen – es soll ja Leute geben, die Geldgeschäfte nicht einmal an ihrem eigenen, sondern von einem Rechner im Internetcafé aus betreiben. Ein zweites Tor sind Mitarbeiter, die über Mobil- oder Heimarbeitsplätze auf die Bankeninfrastruktur zugreifen. Hierzu gehören auch unvorsichtige Mitarbeiter, die vielleicht am Telefon Auskünfte geben, die ▶

► sie nicht geben sollten. Ein drittes Tor ist die Lieferkette der IT. Sie bietet viele Möglichkeiten, sich unlegitimiert Zugang zur Banken-IT zu verschaffen. Denken Sie etwa an Schadsoftware auf ausgelieferten PCs oder auf Software-CDs. Wenn Sie 10 000 PCs bestellen, schauen Sie nicht in jedes einzelne Gerät hinein. Aber auch bei der Entsorgung von alten Geräten wird nicht immer sauber gearbeitet.

Und was spielt das E-Banking für eine Rolle?

Hier liegt die grösste Gefährdung beim Kunden, und sie steigt rapide. Das hängt unter anderem damit zusammen, dass das Verhältnis von Gewinnspanne zu Risiko für die Cyberkriminellen sehr positiv aussieht. Der Kunde müsste sich eigenverantwortlich durch entsprechende Massnahmen und angemessenes Verhalten schützen, was bekanntlich nicht immer funktioniert. Für die Banken ist das Risiko durch Internetbanking hingegen noch relativ klein. Das liegt auch daran, dass ihre Telebanking-Systeme in der Regel mehrstufig geschützt sind.

«Die IT-Sicherheit denkt ab und zu noch stark in technischen Silos.»

Wie betreibt man denn ein Telebanking heute im Rahmen der Banken-IT?

Es läuft in der Regel auf separaten Systemen, die keine persistente Datenhaltung haben. Solche Frontsysteme sind mit sehr selektiven und gut geschützten Schnittstellen ausgestattet. Und sie werden auch gut überwacht.

Es gäbe mittlerweile ja Konzepte, mit denen auch die Kunden viel besser geschützt werden könnten ...

Dass die nur zögerlich eingesetzt werden, dürfte einerseits mit dem Schutz von bereits getätigten Investitionen und andererseits mit der Angst vor den Kosten einer Transition zusammenhängen. Hinzu kommt, dass Banken grundsätzlich skeptisch sind, wenn neue Schutzverfahren das E-Banking für die Kunden komplizierter machen. Banken stehen im Wettbewerb, und ein Kunde, dem das E-Banking zu kompliziert wird, kann locker zur Konkurrenz wechseln. Ich glaube, dass die Toleranz der Kundschaft gegenüber aufwendigen Sicherheitsverfahren relativ klein ist, zumal das Restrisiko gemäss AGB am Ende ja doch wieder bei ihm landet.

Was beschert uns das Mobile Banking?

Die grösste Aufgabe beim Mobile Banking wird sein, die Endgeräte genügend zu schützen. Die Kommunikation zwischen Endgerät und Bank halte ich für weniger problematisch. Die mobilen Endgeräte haben wenig Rechenleistung, kleine Speicher und kurze Produktzyklen. Unter solchen Umständen ist es schwierig, wirksame und bezahlbare Schutzsoftware zu entwickeln. Dazu kommt, dass der Nutzer seine einmal installierte Sicherheitstechnik möglichst einfach von einem Gerät aufs nächste migrieren möchte. Doch das geht bei der bisher schlechten Rückwärtskompatibilität von Handybetriebssystemen nicht ohne Weiteres. Deshalb wird sich Mobile Banking vorderhand wohl auf eine technikaffine Bevölkerungsgruppe beschränken, die sich mit solchen Fragen beschäftigen mag. Damit bleibt das Gesamtrisiko für das System aber auch relativ niedrig.

Wie wirkt sich der Trend zu Standardpaketen auf die Sicherheit aus?

Ich befürchte, dass diese Standardpakete oft insofern missverstanden werden, als man meint, man erwerbe damit eine vollständige Banksoftware. Dabei kauft man in der Regel nur einen stark konfigurierbaren und konfigurationsbedürftigen Bausatz, aus dem man sich die Bankenlösung zusammenstellt. Diese Baukästen enthalten natürlich auch Sicherheitselemente, doch ob und wie man sie braucht, entscheidet das Customizing. Und selbst wenn sie ordentlich konfiguriert sind, reichen die Möglichkeiten solcher Baukästen nicht, um die notwendige End-zu-End-Sicherheit herzustellen. Das ist aber kein Argument, auf standardisierte Software zu verzichten. Man muss sich nur im Klaren sein, dass sie einen nicht davon entheben, ein eigenes Sicherheitsdispositiv zu entwickeln und umzusetzen.

Das dürfte so ähnlich wohl auch für das Cloud Computing gelten.

Hier kommt noch hinzu, dass manche vergessen, ihre IT aufzuräumen, bevor sie in die Cloud wechseln. Früher, beim klassischen Outsourcing, wurden ganze Prozesse an einen externen Dienstleister übergeben. Von ihm erhoffte man sich, dass er das Ganze dann günstiger, aber gleich sicher betreibt wie die eigene IT zuvor. Bei der Cloud geht das natürlich nicht. Dort muss ich vorher bei meiner eigenen IT standardisieren. Ich muss proprietäre Lösungen, die nicht in die Cloud passen, ablösen, bevor ich migriere. Das ist ausgesprochen sicherheitsrelevant und kann besser oder schlechter gelöst werden. Beim Cloud Computing kommt noch die Frage hinzu, wie weit ich überhaupt die

Kontrolle über meine Daten habe. Sie kennen ja die Probleme mit dem US-amerikanischen Datenschutz. Das liesse sich zwar beispielsweise durch eine gemeinsam betriebene Schweizer Banken-Cloud lösen. Wenn man aber sieht, wie sehr die Banken schon mit der Schaffung einer gemeinsamen Wertschriften-transaktionsplattform gescheitert sind, wird eine gemeinsame Cloud wohl eher unwahrscheinlich.

Wie beurteilen Sie die Auslagerung von Sicherheitsaufgaben an Managed-Security-Dienstleister?

Ich glaube, hier hat ein Umdenken bei den Sicherheitsfachleuten stattgefunden. Man hat gemerkt, dass einem die Komplexität des Betriebs oft gar keine andere Wahl lässt, als einzelne Tasks einer Fremdfirma zu übergeben. Allerdings muss man dabei entscheiden, ob der Betrieb als Ganzes oder nur die Überwachung übergeben werden soll. Heute gibt es für beide Versionen Anbieter, die dies können. Besonders interessant ist Managed Security für mittelgrosse Unternehmen, denn

«Die grösste Aufgabe beim Mobile Banking wird sein, die Endgeräte genügend zu schützen.»

die haben oft nur die Wahl zwischen etwas gar nicht zu machen oder es auszulagern. Bewährt hat sich meiner Meinung nach, solche Aufgaben über einen mehrstufigen Prozess auszulagern, währenddem man langsam Vertrauen aufbauen kann. Die Kunst wird hier sein, den richtigen Anbieter auszuwählen und das Ergebnis zu bewerten.

Und was haben Sie für Tipps für die Bankencios?

Das Wichtigste: Sie sollten einen gewissen Widerstand leisten gegen die nächste und die übernächste Sparrunde. Irgendwann werden die Ressourcen so ausgedünnt, dass man stabil nein sagen muss. Das Zweite, was mir auffällt: Es geht darum, die guten Mitarbeiter zu halten und falls nötig auch zu entlasten – egal, wie stark man eine IT schrumpfen muss. Man sollte sich auch auf den Druck vorbereiten, den die Geschäftsleitung künftig in Richtung Cloud Computing aufbauen wird. Und zum Schluss denke ich, dass der CIO heute eine ganz entscheidende Marketingfunktion wahrnehmen muss. Er muss die Leistungen der IT gut verkaufen und ihre Verdienste ins rechte Licht rücken. <