

«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 stuft 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. <