Ständige **Wachsamkeit** aller Beteiligten **erforderlich**

Von Stefan Schlemmer

Der Schwachpunkt in der Online-Kommunikation zwischen Kunde und Bank bleiben die vom Kunden eingesetzten PC-Systeme und der sorgfältige Umgang mit Zugangsdaten, so Stefan Schlemmer. Sein Institut stellt derzeit von der i-TAN auf mobile TAN und HBCI-Chipkarte um. Schon vor drei Jahren wurde der Verfügungsrahmen bei privaten Kunden mit i-TAN-Zugängen auf 1 000 Euro pro Tag reduziert. Entscheidender Faktor für die Sicherheit des Systemes sei aber die Sensibilisierung und Aufklärung der Kunden. Red.

Die Sicherheit der Daten wird von vielen Seiten bedroht. Ziele der Betrüger und Kriminellen sind dabei weniger Rechenzentren und Banken, sondern Selbstbedienungsgeräte oder PC und Transaktionen von Bankkunden. Denn gerade Bankkunden sind als schwächstes Glied in der Kette dem Angriff von Phishern oder Hakkern ausgesetzt. Deshalb sind gemeinsame Anstrengungen von IT-Dienstleistern, Banken und Bankkunden nötig, um die steigende Anzahl der Attacken auf Daten und Konten abzuwehren.

Bei der Sicherheit der Bankdaten vertraut die VR Bank Hessen-Land auf ihren IT-Dienstleister Fiducia IT AG. Auf die Sicherheit der von den Bankkunden eingesetzten Systeme und auf den sorgfältigen Umgang mit den Onlinebanking-Zugangsdaten hat die Bank jedoch keinen direkten Einfluss. Genau hier setzen jedoch hauptsächlich die Angreifer an: am schwächsten Glied der Kette.

Bankkunden für Angriffsszenarien sensibilisieren

Unerfahrenheit, leider mitunter auch Gleichgültigkeit, sind die Ursachen für die oft unzureichende Sicherheitsausstattung der Anwender-PC. Zudem werden die Angriffsvarianten der Onlinebetrüger immer eleganter. Die Zeiten von Phishing-E-Mails in holprigem Deutsch sind lange vorbei. Banken müssen deshalb den Gefahren durch Fehlverhalten oder virenverseuchte PCs der Anwender begegnen und ihre Kunden so gut wie möglich schützen.

Sichere, aber trotzdem noch bedienbare Onlinebanking-Verfahren sind gefragt. Aktuell sind dies das mobile-TAN- und das smart-TAN-plus-Verfahren. Sie werden den Banken von ihrem IT-Dienstleister zur Verfügung gestellt. Zugangsverfahren, die den heutigen Anforderungen an sicheres Onlinebanking nicht mehr gerecht werden, wie die i-TAN mit den Transaktionsnummern auf einem Papierbogen, werden von den meisten IT-Dienstleistern zum Jahresende abgeschaltet. Bereits zum 30. September sperrt die VR Bank Hessen-Land die letzten noch verbleibenden i-TAN-Bögen. Den Kunden wird der Umstieg auf mobile TAN, smart-TAN-plus oder auf die HBCI-Chipkarte angeboten.

Zusätzlich ist es wichtig, Bankkunden ständig durch Informationen über mögliche Angriffszenarien für die Bedrohung zu sensibilisieren. Denn auch bei den aktuell sichersten Verfahren muss der Nutzer immer wachsam bleiben, um mögliche Manipulationsversuche zu erkennen und abzuwehren.

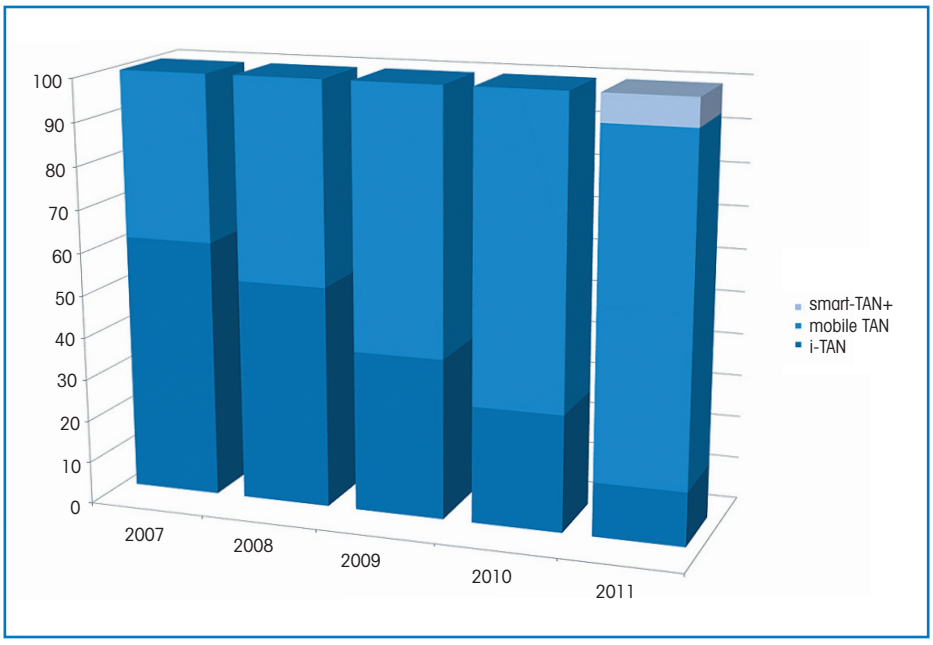
Umstellung auf die mobile TAN

Sicherheit beim Onlinebanking hat für die VR Bank Hessen-Land seit Jahren höchsten Stellenwert. Mit der Einführung der mobile TAN im Jahre 2007 begann die aktive Kundenansprache und Bewerbung des neuen, sicheren Verfahrens. Bereits Ende des gleichen Jahres nutzten rund 35 Prozent der Onlinebanking-Kunden das neue Verfahren. Da die Bank die mobile TAN kostenlos anbietet, fiel die Entscheidung der Kunden zugunsten der höheren Sicherheit leicht.

Zum Autor

Stefan Schlemmer ist Leiter Internetvertrieb bei der VR Bank HessenLand eG, Alsfeld.

Nutzung der verschiedenen TAN-Verfahren (Angaben in Prozent)



Zudem erhalten seit dieser Zeit Kunden der Bank neue Onlinebanking-Zugänge grundsätzlich nur noch in Verbindung mit dem mobile-TAN-Verfahren oder mit HBCI-Signatur/Chipkarte. Das gilt sowohl für Privat- als auch für Firmenkunden. Ausgenommen hiervon waren Kunden, die die mobile TAN definitiv nicht nutzen konnten. Kunden ohne Mobiltelefon gab es zwar kaum, wohl aber eine Anzahl Menschen, die in der heimischen Wohnung oder am Arbeitsplatz keine Netzabdeckung haben.

Das Geheimnis des Erfolgs war nicht zuletzt die frühzeitige Einbeziehung der Mitarbeiterinnen und Mitarbeiter. Bevor die mobile TAN im Kundenbereich eingeführt wurde, stellten alle Bankmitarbeiter ihre eigenen Zugänge auf das neue Verfahren um und lernten den Umgang mit der mobile TAN kennen. Die Argumentation beim Kunden fiel leichter, da die Mitarbeiter aus eigener Erfahrung sprachen (siehe Abbildung). Um das Risiko für die verbliebenen Nutzer des i-TAN-Verfahrens zu senken, reduzierte die Bank im Sommer 2008 den Verfügungsrahmen der i-TAN-Zugänge auf 1 000 Euro pro Tag. Für Firmenkunden gilt seither ein maximaler Verfügungsrahmen von 10 000 Euro.

Auch die für 2011 anstehende Abschaltung der letzten i-TAN-Bögen ging die Bank engagiert und offensiv an. Zunächst informierte sie ihre Kunden auf den Internetseiten und im Internetbanking. Über die Bildschirme der SB-Geräte wurde mit aufmerksamkeitsstarken Motiven auf die Veränderung hingewiesen. Die Bilder zeigen, wie TAN-Bögen zerrissen und durch den Schredder gelassen werden oder als Papierflieger „den Abflug machen".

Sicherheit nur unter Einbindung und mit Hilfe der Kunden

Zehn Wochen vor dem Abschalttermin wurden alle Kunden, die noch einen i-TAN-Bogen nutzen, angeschrieben. Dem Schreiben lag eine vorgefertigte Rückantwort bei. Hier konnte der Kunde direkt ein anderes Onlinebanking-Verfahren ankreuzen oder um einen Rückruf bitten. Seit Anfang August erscheint zusätzlich bei jeder Transaktion, die im Internetbanking mit einer i-TAN bestätigt wird, der Hinweis auf den Abschalttermin.

Doch mit der Technik alleine ist es nicht getan. Es gilt, den Anwender für die Gefahren des Internet zu sensibilisieren. Daher erhält jeder Kunde, der sich bei der VR Bank Hessen-Land zum Internetbanking anmeldet, zusammen mit seinen Zugangsdaten Informationsmaterial zum Thema Sicherheit. Seit 2007 sensibilisiert die Bank stetig ihre Kunden für Online-Sicherheit. In Zusammenarbeit mit externen Dienstleistern werden Hacking und Phishing in unterhaltsamen, aber dennoch informativen Vorträgen live vorgeführt.

Selbstverständlich erhalten die Besucher der Veranstaltung auch zahlreiche Tipps, wie sie sich schützen können. 2010 wurde die Veranstaltung um Informationen zu Spaß und Risiken von Social Media und den Gefahren des Cybermobbings ergänzt. Sechs gut besuchte Veranstaltungen in Schulen in der Region zeigten, wie aktuell das Thema auch bei jüngeren Zielgruppen ist.

Nach den Kundenveranstaltungen registrieren die Mitarbeiter der electronic-banking-Hotline vermehrt Anfragen nach empfehlenswerten Sicherheitslösungen für den heimischen PC. Auf ihren Internetseiten hat die Bank deshalb entsprechende Informationen zur Verfügung gestellt und über externe Partner auch eine direkte Bestellmöglichkeit geschaffen.

Mit regionalen IT-Dienstleistern wurden Kooperationsvereinbarungen getroffen. Die Kooperationspartner wurden auf den Internetseiten aufgelistet und bei entsprechender Anfrage kommuniziert. Somit konnte die Bank ihren Kunden regionale, qualifizierte Ansprechpartner nennen. Seit 2010 bietet die VR Bank Hessen-Land ihren Mitgliedern zusätzlich die Jahreslizenz des Sicherheitspakets „F-Secure Internet-Security" zu einem besonders günstigen Preis an.

Aktuelle Phishing-Methoden thematisiert

Für November plant die VR Bank Hessen-Land drei weitere Kundenveranstaltungen

zum sicheren Onlinebanking. Das Angebot richtet sich dieses Mal in erster Linie an Senioren, aber es sind selbstverständlich alle Altersgruppen willkommen. Ein wichtiger Programmpunkt in diesen Veranstaltungen werden die aktuellen Phishing-Methoden sein. Die Angreifer haben erkannt, dass die Manipulation der neuen TAN-Verfahren zu aufwändig ist. Stattdessen versuchen sie, den Anwender zu manipulieren und beispielsweise zu Testüberweisungen ins Ausland zu verleiten.

Der beste Schutz der Kunden vor diesen Angriffen ist eine offene und ehrliche Kommunikation. Onlinebanking-Anwender, die die verschiedenen Phishing-Szenarien kennen, lassen sich durch manipulierte Internetseiten nicht so leicht täuschen. Auch hier sind die Mitarbeiterinnen und Mitarbeiter wieder der Schlüssel zum Erfolg. Sie sprechen ihre Kunden gezielt zum Thema Sicherheit an.

Skimming: manipulierte Geldautomaten

Voraussetzung hierzu ist, dass die Beraterinnen und Berater mit den Grundlagen der Onlinebanking-Sicherheit vertraut sind. Sie erhalten regelmäßig aktuelle Informationen über das bankeigene Informationssystem. Außerdem bietet die Bank Inhouse-Schulungen zur Auffrischung der Kenntnisse an. Bereits auf dem Schulungsplan der Auszubildenden ist das Thema Onlinebanking und Sicherheit vertreten.

Doch nicht nur am heimischen PC gilt es, ein Auge auf die Sicherheit zu haben. Auch bei der Bargeldversorgung am Automaten kann es inzwischen durch Manipulationen zu finanziellem Schaden kommen. Trickbetrüger versuchen die Kartendaten oder PIN auszulesen.

Dazu bringen sie häufig vor dem Kartenschlitz einen Magnetstreifenleser an. Alternativ überwachen sie die Tastatur des Automaten mit einer winzigen Kamera, um die PIN-Eingabe auszuspähen. Die Geldautomatenhersteller haben zwischenzeitlich auf diese sogenannten Skimming-Angriffe reagiert und ihre Geräte angepasst. Als zusätzlicher Schutz werden neuralgische Punkte mit Siegelaufklebern für den Kunden augenfällig gekennzeichnet.