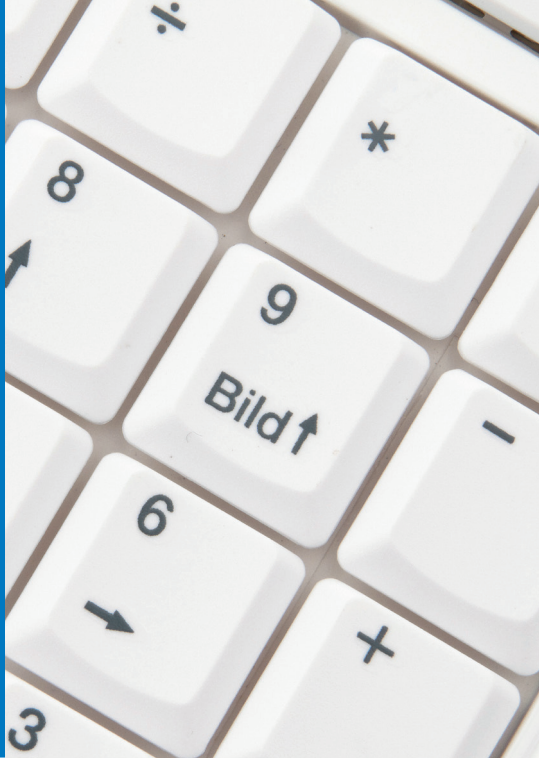
IT-Sicherheit: nicht nur eine Frage der Technik



Von Daniel Hamburg

Organisationen der Finanzbranche können sich keine Schwachstellen in ihren Netzwerken und Applikationen leisten. Neben den technischen müssen sie organisatorische und prozessuale Maßnahmen in alle Geschäftsbereiche integrieren. Anhand eines Informationssicherheitskonzepts zeigt Daniel Hamburg auf, wie ein solcher Prozess in sechs Schritten in das Unternehmen implementiert werden kann. Zudem stellt der Autor ein neues Konzept zur Freigabe von Bankgeschäften im Internet vor: Der USB-Stick arbeitet auf Basis einer digitalen Signatur, kommt jedoch ohne TAN aus. Red.

Schneller noch als die interne und externe Vernetzung von Unternehmen und Organisationen ist das Bedrohungspotenzial gewachsen: Mit immer neuen Methoden und Technologien wird versucht, die IT anzugreifen. Banken und Finanzdienstleister sind extrem gefährdet, denn dem erfolgreichen Angreifer winkt fette Beute. Auf der anderen Seite müssen gerade Banken ihre Daten zuverlässig vor unbefugtem Zugriff, Ausspähen, Manipulation und Verlust schützen, denn Bankgeschäfte sind Vertrauenssache: Kunden verlassen sich darauf, dass ihre Daten bei ihrem Institut sicher aufgehoben sind. Mit einer nachgewiesenen und zertifizierten Prüfung der Sicherheitskonzepte und -maßnahmen können Finanzinstitute das Vertrauen ihrer Kunden stärken.

In Deutschland sind die Vorgaben verschiedener Gremien für die IT-Sicherheitsstruktur von Banken hoch: Neben der Bankenaufsicht, die sich nach den Regeln des Kreditwesengesetzes (KWG) richtet, gibt es Vorschriften von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), der Bundesbank, der Europäischen Zentralbank EZB, des DK Die Deutsche Kreditwirtschaft (ehemals ZKA), der Bank für Internationalen Zahlungsausgleich BIZ, dem Baseler Ausschuss für Bankenaufsicht und dem Bundesamt für Sicherheit in der Informationstechnik BSI. Wie sieht die Bedrohungslage für Kreditinstitute aus und welche Vorsorge müssen und können sie in Form von Sicherheitskonzepten und technischen, organisatorischen sowie prozessualen Maßnahmen treffen?

Sicherheit im Onlinebanking

43 Prozent aller Bundesbürger im Alter von 16 bis 74 Jahren nutzen Onlinebanking. Das sind mehr als 27 Millionen Deutsche, etwa eine Million mehr als im Jahr 2010. Im Jahr 2003 waren es erst 21 Prozent. Mittelfristig wird sich Onlinebanking in Deutschland wie in anderen Ländern in der ganzen Bevölkerung durchsetzen. Nach Angaben der Deutschen Bundesbank gibt es in Deutschland 40 Millionen online geführte Konten unter den 93 Millionen Girokonten.

Unter Onlinebanking versteht man den direkten Zugriff auf den Bankrechner über Internet oder Direkteinwahl bei der Bank per Datenfernübertragung. Aktuell gibt es mehrere Verfahren: Zum einen das Onlinebanking über einen Internetbrowser, der auf die Website der Bank zugreift und für die Datenübertragung meist mit Secure Socket Layer (SSL) gesichert ist. Eine andere Methode arbeitet mit einem Client-Programm, wobei die Transaktion (offline) vorbereitet und anschließend eine Netzverbindung für die Übertragung aufgebaut wird. Zunehmender Beliebtheit erfreuen sich mobile Zugriffe von Smartphones, Tablets und Handys über Apps.

Alle Onlinebanking-Anwendungen können angegriffen und gehackt werden, wenn die Banken keine Vorsorge treffen. Zu den prophylaktischen Maßnahmen gehört es etwa, Benutzerdaten nur verschlüsselt abzulegen und den Zugriff zu reglementieren sowie alle Anwendungen auf Lücken abzuklopfen. Dies kann durch eine Sicherheitsanalyse geschehen, bei der Experten Angriffe simulieren.

Zum Autor

Dr.-Ing. Daniel Hamburg ist Head of Security Engineering bei der TÜV Rheinland i-sec GmbH, Köln.

Typischerweise läuft eine solche Sicherheitsanalyse zur Schaffung von Sicherheit und Qualität in sechs Schritten ab: Konzept für Qualität und Sicherheit, Umsetzung und Betriebsunterstützung, Security-Analyse und Tests, Prüfung von Usability und Performance sowie Zertifizierung oder Testat.

Ein Sicherheitskonzept für das Onlinebanking: Zunächst wird ein Sicherheitskonzept für die Infrastruktur, die Online-Applikation und die datenschutzrelevanten Prozesse erstellt beziehungsweise das bestehende Konzept geprüft. Das Ziel ist, potenzielle Gefahren zu identifizieren und entsprechende Gegenmaßnahmen zu planen. So hilft Verschlüsselung gegen den unbefugten Zugriff und die Manipulation von Kundendaten. Authentifizierungsmechanismen sorgen dafür, dass Angreifer keinen Zugriff auf Kundendaten erhalten und Kunden nur ihre eigenen Daten sehen können.

Häufig vernachlässigt wird die Sicherheit bei der Entwicklung neuer Onlinebanking-Anwendungen. Dabei ist es doppelt vorteilhaft, Sicherheitsaspekte bereits beim Erstellen des Software-Designs und während seiner Implementierung zu berücksichtigen: Das erspart nämlich eine oft kostspielige nachträgliche Beseitigung von Sicherheitslücken in der Software und gleichzeitig steigt die Wahrscheinlichkeit, dass die Applikation nicht nur heutigen, sondern auch zukünftigen Angriffen standhält.

Das Sicherheitskonzept wird an die Sicherheitsvorgaben (Security Policy) der Bank angepasst und in das Informationssicherheitsmanagementsystem ISMS integriert.

Umsetzung und Betriebsunterstützung: Im zweiten Schritt wird das Sicherheitskonzept umgesetzt. Dabei wählen die Experten geeignete Maßnahmen aus, um die Sicherheit der Kundendaten zu gewährleisten. So hilft der Einsatz von Firewalls oder die Härtung von Server-Systemen, die Angriffsfläche der Online-Anwendungen zu verringern.

Nicht jeder Onlinebanking-Anbieter muss sich zum Sicherheitsspezialisten weiterbilden, sondern er kann auf Managed Services zurückgreifen. Das ist eine Art Rundum-Sorglos-Paket, bei dem externe Fachleute aus dem Technical Assistance Center die Konfiguration und den Betrieb der Sicherheitskomponenten übernehmen. Im Falle des Falles tauschen sie sicherheitsrelevante Hardware durch Ersatzgeräte aus und übernehmen das Lizenzmanagement ebenso wie die Laufzeitkonsolidierung. Der TÜV Rheinland bietet beispielsweise Managed Services an, bei denen ein Onlinebanking-Anbieter sich passende Stufen von Service Level Agreements (SLA) auswählen kann.

Sicherheitsanalyse und Praxistests: Die Sicherheitsanalyse deckt Risiken auf, die in der Onlinebanking-Applikation selbst und in den Diensten liegen, und schlägt Maßnahmen vor, diese zu eliminieren oder zu reduzieren. Die Vorschläge orientieren sich beispielsweise an den Vorgaben der Standards ISO 27001, IT Grundschutz nach BSI und Open Web Application Security Project (OWASP). Das aktuelle Sicherheitsniveau der Onlinebanking-Anwendung wird in drei Stufen analysiert: Bei Angriffen auf die zugrunde liegende Infrastruktur sowie bei Angriffen auf die Anwendung mit und ohne Authentifizierung. Ziel ist die Überprüfung der Wirksamkeit von bereits implementierten IT Sicherheitsmaßnahmen und eine Steigerung der Sicherheit.

Das Portal „datenleck" listet Pannen auf, in denen es um Finanzdaten geht, und wird jeden Monat mindestens einmal fündig: www.datenleck.net

In Nordamerika haben sich beispielsweise Kriminelle durch URL-Manipulationen Zugriff auf die persönlichen Daten hunderttausender Kunden einer Großbank verschafft und von 3 400 Konten insgesamt 2,7 Millionen Dollar abgehoben. Üblicherweise werden Identifikationsnummern entweder direkt am Bankterminal oder beim Onlinebanking abgegriffen, da sie in allen anderen Situationen verschlüsselt sein sollten. In diesem Fall war es den Hackern jedoch gelungen, die PINs direkt aus dem Geldautomatennetz der Bank im Klartext auszulesen.

Zunächst werden die IP-Adressen der Anwendung auf Netzwerk- und Dienste-Ebene auf Schwachstellen untersucht. So werden sicherheitsrelevante Schwachstellen in der Firewall-Konfiguration und den erreichbaren Diensten identifiziert. Ferner wird festgestellt, ob das bestehende Patch-Management greift und die Serversysteme hinreichend gehärtet wurden.

In der zweiten Stufe wird versucht, die Applikation anzugreifen. Kann ein Angreifer den Login-Mechanismus bei administrativen Schnittstellen überwinden, zum Beispiel durch gezielte Brute-Force-Angriffe (Ausprobieren von Standard- und Trivialpasswörten)? Wie verhält sich die Anwendung bei Parameter-Veränderungen? Werden Fehlermeldungen ausgegeben, die auf potenzielle Schwachstellen hindeuten? Was passiert bei einer Änderung an Session-Variablen und Cookies, bei Datenbankangriffen wie SQL-Injection oder anderen Manipulationen? Wie reagiert die Applikation auf Cross-Site-Scripting und Code- und Command-Injection-Angriffe? Weitere Angriffsvarianten hängen von der jeweiligen Programmiersprache und Technologie der Anwendung ab.

Zuletzt wird die Anwendung von einem authentifizierten Benutzer angegriffen. Dies simuliert einen Angreifer, der Zugriff auf die Login-Daten eines Benutzers hat. Ein solcher authentifizierter Angreifer hat viel mehr Möglichkeiten, als ein Angreifer ohne Benutzerrechte: Kann er etwa auf die Daten anderer Benutzer zugreifen? Kann er Kontrolle über die Applikation oder sogar über andere Systeme erhalten? Untersucht werden die Reaktion der Applikation auf Änderungen an Session-Variablen und Cookies sowie die Zuverlässigkeit

beziehungsweise Nicht-Vorhersagbarkeit der Session. Zusätzlich wird geprüft, ob nicht-öffentliche Teile der Applikation ohne vorherige Authentifizierung erreichbar sind.

Usability und Performance: Neben den Sicherheitsaspekten spielen beim Onlinebanking auch die Benutzerfreundlichkeit und die Schnelligkeit der Applikation eine Rolle. Sind die Daten der Benutzer vielleicht so sicher, dass nicht einmal der Benutzer sie einsehen kann? Verzweifelt ein Benutzer, weil er nicht das findet, was er sucht? Experten untersuchen die Usability der Applikationen und helfen, sie so zu gestalten, dass der Benutzer sich wohl fühlt und mit möglichst wenigen Klicks zum gewünschten Ziel kommt.

Muss ein Benutzer zu lange auf eine Antwort warten, wenn viele Benutzer gleichzeitig zugreifen? Last- und Performance-Tests simulieren typisches Anwenderverhalten und typische Aktionen. Sie messen die Reaktion der Applikation und ihre Antwortzeiten. Durch die Usability-Optimierung wird die Akzeptanz der Anwendung bei den Benutzern erhöht.

Zertifikat: Ein Zertifikat für die Onlinebanking-Anwendung bedeutet geprüfte Sicherheit und schafft eine breite Vertrauensbasis für die Anbieter, die sie sich sonst in jahrelanger Arbeit aufbauen müssten. Finanzunternehmen festigen und bestätigen mit einem Zeugnis das bestehende Vertrauen ihrer Kunden.

- Das Zertifikat „Datenschutz und Datensicherheit" des TÜV Rheinland etwa bestätigt dem Anwender, dass die organisatorischen, administrativen und datenschutzrelevanten Prozesse des Onlinebankings mit technischen Sicherheitsanalysen untersucht wurden.

- Das Zertifikat „Geprüfter IT-Testprozess" des TÜV Rheinland bescheinigt die Auditierung des Software-Qualitätssicherungsprozesses bereits während der Entwicklung.

- Das Zertifikat „Usability nach der ISO 9241" bescheinigt die Gebrauchstauglichkeit der Applikation.

Testat: Ein Testat für eine i-Phone-App oder eine Android-App wird für die App in der geprüften Version ausgestellt. Entscheidend ist dabei die sichere Entwicklung der App. Es gilt, Sicherheitslücken von Anfang an zu vermeiden. In diesem Bereich der Sicherheitsanalysen sieht der TÜV Rheinland aktuelle Schwerpunkte.

Authentifizierung beim Onlinebanking

Für Online-Transaktionen haben sich in Deutschland verschiedene Verfahren etabliert. Privatanwender nutzen das PIN-/TAN-Verfahren, dessen einfachste Form eine TAN-Liste auf dem Papier ist. Inzwischen sind auch TAN-Generatoren (Lesegeräte) oder SMS-TANs verbreitet. Beim Homebanking Computer Interface (HBCI) oder Financial Transaction Services (FinTS) legitimiert der Anwender sich per Chipkarte oder Schlüsseldiskette.

Angreifer können versuchen, durch Schadprogramme wie Viren, Keylogger oder Trojaner auf den Computer des Bankkunden zuzugreifen und ihn fernzusteuern. Phishing ist eine Methode, direkt an die PIN und TAN zu gelangen. Mit DNS-Spoofing versuchen Hacker, das Domain Name System zu manipulieren und die URL einer Onlinebanking-Seite auf die eigene IP-Adresse umzulenken. Ein sehr aufwendiger Angriff auf Onlinebanking ist der Man-in-the-middle-Angriff, bei dem sich der Angreifer zwischen Nutzer und Bank schaltet. Dafür muss er den Datenverkehr in Echtzeit entschlüsseln und verfolgen.

Verfahren wie die mobile TAN (m-TAN) und chip-TAN versprechen Schutz gegen solche Angriffe, ebenso eine Überprüfung des digitalen Zertifikats der SSL-Verschlüsselung.

Für Bankanwendungen im Geschäfts- und Privatkundenbereich hat TÜV Rheinland für die Postbank ein neues Signaturverfahren zur Freigabe von Bankgeschäften im Internet zertifiziert. Für ihren umfangreichen Zahlungsverkehr benötigen vor allem Firmenkunden ein Verfahren, mit dem sie sicher, einfach und schnell viele Transaktionen im Onlinebanking freigeben können.

Neues Signaturverfahren mit USB-Stick

Das innovative und von TÜV Rheinland geprüfte Verfahren „Best Sign" arbeitet auf Basis der digitalen Signatur, kommt aber ohne Transaktionsnummer (TAN) aus. Der Bankkunde braucht nur seine Kontonummer und Online-PIN sowie ein kleines, handliches USB-Gerät. Nach Eingabe der Transaktionsdaten sendet die Bank diese auf den an den Kunden-PC angeschlossenen USB-Stick zurück. Dieser zeigt die Daten im Display an und der Kunde gibt sie durch manuelle Bestätigung am USB-Gerät frei. Der Knopfdruck erzeugt auf dem Chip im USB-Stick eine digitale Signatur.

Wie bei allen Signaturverfahren erfolgt der Datenaustausch zwischen Stick und Bank vollständig verschlüsselt. Weil der PC lediglich als „Stromspender" und Zugang zum Onlinebanking dient, ist das Verfahren sehr flexibel, denn es kann an jedem freigeschalteten USB-Port genutzt werden. Jeder Mitarbeiter hat seinen eigenen Stick, den er hüten muss wie eine TAN-Liste.

Wie aktuell viele Branchen, sind auch die Finanzinstitute sehr engagiert, Schwachstellen in ihren Netzwerken und Applikationen auszuschalten. Dabei müssen alle Anwendungen – vom Onlinebanking bis hin zu den Apps auf mobilen Geräten – in das Sicherheitskonzept einbezogen werden.

Ein mehrstufiges IT-Sicherheitskonzept bietet große Vorteile: Während isolierte Maßnahmen leichter angreifbar sind, schaffen Banken mit einer integrierten Lösung für Informationssicherheit mittel- und langfristige Sicherheit, die auch eine solide Grundlage für zukünftige Anforderungen bietet. ■