Zahlungsverkehr

Wirksamer Schutz für Online-Banking

Das Angriffsziel von Cyberkriminellen sind längst nicht mehr nur Grossunternehmen, sondern vermehrt auch kleine und mittlere Unternehmen. Vor allem das Online-Banking haben die Angreifer im Visier. Damit KMU ihre Infrastruktur angemessen schützen können, sind grundlegende Verhaltensregeln zu beachten.

› Oliver Hirschi

Zwei jüngst veröffentlichte Medienberichte sprechen eine deutliche Sprache: Im Januar wurde bekannt, dass Hacker ein Freiburger Unternehmen um eine Million Franken erleichtert haben sollen. Und im Februar meldete die Schweizerische Melde- und Analysestelle Informationssicherung (Melani), dass spezielle E-Banking-Trojaner immer stärker auch Schweizer KMU angreifen. Unternehmen sind also gut beraten, sich angemessen zu schützen. Eine Anleitung dazu bietet das Informationssicherheitshandbuch für die Praxis (SiHB); die komplett überarbeitete und aktualisierte Auflage ist soeben erschienen (siehe Box). Exklusiv für das «KMU-Magazin» wird an dieser Stelle das Kapitel «Sicherer Zahlungsverkehr (Online-Banking)» daraus publiziert.

Die Ausgangslage

Der elektronische Zahlungsverkehr, sprich das Online-Banking ist wohl aus keinem Unternehmen mehr wegzudenken. Zu bequem und komfortabel ist der zeitunabhängige und direkte Zugriff auf die unternehmenseigenen Finanzen. Aufgrund seiner direkten Bereicherungsmöglichkeit stellt das Online-Banking aber auch für Angreifer ein begehrtes Ziel dar. Von Phishing-Angriffen über Social-Engineering-Attacken bis hin zu spezifisch programmierter Online-Banking-Schadsoftware sind die Angriffsvektoren vielfältig. Die Finanzinstitute selbst schützen die Daten und Finanzen ihrer Kunden umfassend mit modernen und neuen Sicherheitssystemen.

kurz & bündig

- Die Adresse der Webseite für das Online-Banking des Finanzinstituts sollte immer manuell in die Adresszeile des Browsers eingegeben werden. Dafür sollte niemals ein Link verwendet werden.
- Es muss sichergestellt werden, dass das Online-Banking immer über eine sichere Verbindung verwendet wird (dazu gehören die Bezeichnung «https» und das Schlosssymbol in der Adresszeile).
- Nach jeder Abmeldung der Online-Banking-Sitzung sollte zwingend der Browser-Cache geleert werden.

Sichere Datenaufbewahrung

Schweizer Finanzinstitute verfügen im internationalen Vergleich über einen sehr hohen Sicherheitsstandard. Geschützte Rechenzentren und Sicherheitssysteme gewährleisten, dass die Daten und Finanzen der Kunden sicher aufbewahrt werden. Externe Kontrollstellen wie beispielsweise die Eidgenössische Finanzmarktaufsicht Finma beaufsichtigen und kontrollieren alle Bereiche des Finanzwesens. Darüber hinaus garantieren ISO-Normen (unter anderem ISO 27002) die Standardisierung.

Geschützter Datenzugriff

Mit mehrstufigen Anmeldeverfahren gewährleisten die Finanzinstitute beim Login grösstmögliche Sicherheit. Angreifer müssten jede dieser Sicherheitshürden erfolgreich überwinden, um an die Daten und Finanzen der Kunden zu gelangen. Die von den Finanzinstituten angebotenen Anmeldeverfahren unterscheiden sich in der Art und Weise, wie sie implementiert sind und die Sicherheit gewährleisten, was einen Vorteil darstellt – Angriffsversuche sind nicht eins zu eins vom einen auf das andere Online-Banking-System übertragbar. Finanzinstitute bie-

ten den Kunden in der Regel die Wahl zwischen verschiedenen Anmeldeverfahren, dies oft aufgrund der Historie oder verschiedenen Kundenanforderungen.

Sichere Datenübermittlung
Die Daten werden verschlüsselt von den Computern der Kunden zu den Servern der Finanzinstitute übertragen und können somit von Dritten nicht eingesehen werden.

Transaktionsüberwachung
Alle vom Kunden eingegebenen Transaktionen durchlaufen ein spezielles Regelwerk von Prüfroutinen, bevor die Zahlungen effektiv ausgeführt werden. Unübliche Transaktionen und beispielsweise Auslandszahlungen werden vor der Ausführung speziell geprüft.

Des Weiteren ist es von grosser Wichtigkeit, dass auch die Bankkunden sowohl ihre Computer sowie auch ihre Infrastruktur angemessen schützen und grundlegende Verhaltensregeln beachten.

Das Konzept

Um Online-Banking sicher zu betreiben, sind beim Ein- und Ausloggen folgende wichtigen Punkte zu beachten.

Einloggen

- **Sichere Navigation zum Finanzinstitut**
  Die Adresse zum Online-Banking des Finanzinstituts sollte immer manuell in der Adresszeile des Browsers eingegeben werden. Niemals sollte ein Link verwendet werden, schon gar nicht, wenn er zum Beispiel per E-Mail zugestellt wurde! Ausserdem sollte Online-Banking nur von einem bekannten und sicheren Computer aus benutzt werden (das heisst nicht in Internet-Cafés, öffentlichen Hotel-Computern etc.).

- **Keine anderen Seiten offen**
  Beim Verbindungsaufbau zum Online-Banking und während dessen Benutzung sollten keine anderen Internetseiten und keine E-Mails geöffnet werden.

- **Überprüfen der sicheren Verbindung**
  Es muss darauf geachtet werden, dass ausschliesslich über eine «sichere» Verbindung («https» und Schlosssymbol in der Adresszeile) auf das Online-Banking zugegriffen wird und dass das Zertifikat echt und gültig ist (vergleiche Abschnitt «Zertifikatsprüfung»).

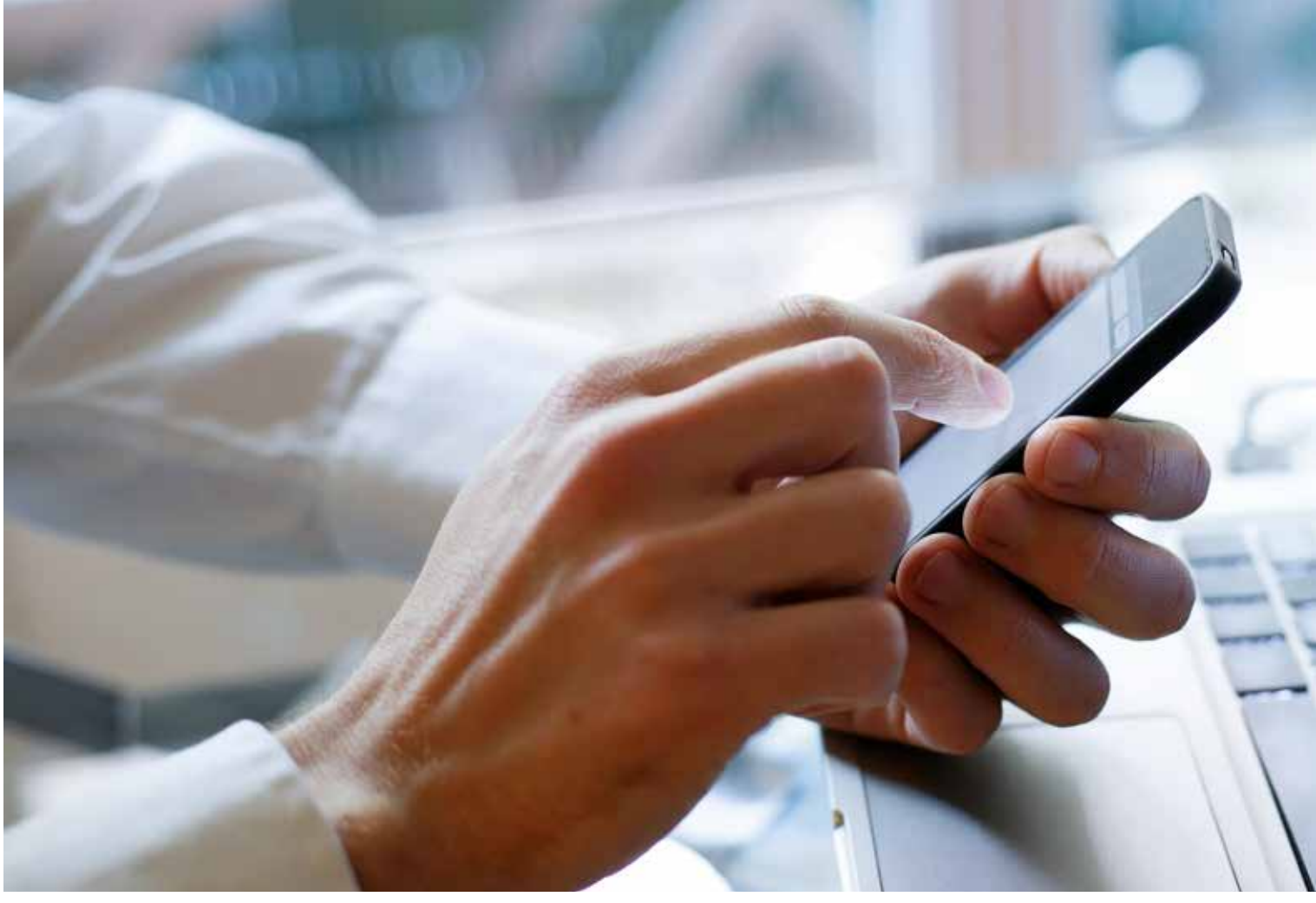
- **Vorsicht bei Systemunterbruch oder ungewöhnlichen Fehlermeldungen**
  Kommt es während dem Online-Banking zu einem Systemunterbruch (zum Beispiel plötzlich auftretender weisser Bildschirm) oder treten vor allem während dem Login ungewöhnliche Fehlermeldungen auf (zum Beispiel «Das System ist derzeit überlastet. Bitte haben Sie etwas Geduld und probieren Sie es später noch einmal»), sollte die Verbindung sofort beendet und die Spezialisten des Finanzinstituts benachrichtigt werden.

Ausloggen

- **Korrektes Beenden der Online-Banking-Sitzung**
  Die Online-Banking-Sitzung sollte immer korrekt über die dafür vorgesehene Funktion (meist mit «Abmelden», «Logout» oder «Beenden» gekennzeichnet) beendet werden.

- **Leeren des Browser-Cache**
  Nach jeder Abmeldung der Online-Banking-Sitzung sollte der Browser-Cache geleert werden.

Auf der Webseite www.ebankingabersicher.ch sind weitere praxisnahe und aktuelle Informationen zu notwendigen Massnahmen und Verhaltensregeln für



eine sichere Anwendung von Online-Banking-Applikationen zu finden.

Zertifikatsprüfung

Jeder Browser verifiziert beim Aufbau einer verschlüsselten Verbindung (SSL, TLS) die Zertifikatseigenschaften «Vertrauenswürdigkeit des Ausstellers des Zertifikats», «Gültigkeit des Zertifikats» und «Adresse des Webservers». Wenn diese drei Überprüfungen erfolgreich durchgeführt werden konnten, zeigt der Browser beim Aufbau der SSL-Verbindung keine Fehlermeldungen an. Eine korrekt aufgebaute SSL-Verbindung, die auf einem echten und gültigen Zertifikat basiert, lässt sich anhand von eindeutigen Browser-Merkmalen erkennen:

- Anfangs Adresszeile steht https://
- Am Anfang oder am Ende der Adresszeile ist ein Schloss sichtbar
- Die Adresszeile oder der Name des Finanzinstituts ist abhängig vom verwendeten Zertifikatstyp grün oder weiss hinterlegt (grün bei Extended Validation Zertifikaten)

Die Echtheit des der Verbindung zugrunde liegenden Zertifikates kann auch manuell überprüft werden. Dazu wird der Fingerabdruck des Zertifikats verifiziert. Der Fingerabdruck ist eine Zeichenfolge, bestehend aus den Buchstaben A bis F (wobei nicht zwischen Gross- und Kleinbuchstaben unterschieden wird) und den Ziffern 0 bis 9. Die Verifikation des Fingerabdrucks erfolgt durch einen Vergleich dieser Zeichenfolge mit einer Referenzfolge, die der Benutzer vom Finanzinstitut erhalten hat. Stimmt die aus dem Zertifikat herausgelesene Zeichenfolge mit der vom Finanzinstitut erhaltenen Zeichenfolge überein, ist das Zertifikat echt.

Anmeldeverfahren /Authentisierungsmittel

Für die Anmeldung für das Online-Banking kommen verschiedene Anmeldever-

Literatur

Informationssicherheitshandbuch für die Praxis – Speziell für Sicherheitsverantwortliche und Geschäftsführer von KMU

Das praxisnahe Sicherheitshandbuch richtet sich an Personen, die sich nicht ausführlich mit dem Thema Informationssicherheit befassen (können), den Schutzbedarf aber erkannt haben und die Sicherheit entsprechend optimieren wollen. Anerkannte Schweizer Sicherheitsexperten beschreiben verständlich, wie die Informationssicherheit in Unternehmen umgesetzt und kontrolliert werden kann (Themen Management, Recht, Organisation und Technik). Die komplett überarbeitete und aktualisierte Auflage 8/2015 ist soeben erschienen.

Weitere Informationen und Online-Bestellung: www.sihb.ch.

fahren und Technologien zum Einsatz. Mittlerweile ist die Zwei-Faktor-Authentifizierung Standard, bei der zusätzlich zur Vertragsnummer und zum Passwort (Erster Faktor «Wissen») meist auf einem zweiten Gerät (Token) oder einer Smartcard (Zweiter Faktor «Haben») ein einmaliger Zugangsschlüssel bereitgestellt wird.

Transaktionsbestätigung / Transaktionssignierung

Für den Schutz vor unbeabsichtigten Zahlungen wird oft die sogenannte Transaktionsbestätigung (auch Zahlungsbestätigung oder Transaktionssignierung genannt) eingesetzt. Dabei müssen gewisse ausgehende Zahlungen vor der Überweisung durch den Benutzer zusätzlich überprüft und explizit zur Ausführung freigegeben werden. Die Prüfung kann Elemente wie Währung, Betrag sowie Teile der Kontonummer des Zahlungsempfängers umfassen.

Offline-Zahlungssoftware

Mit einer Offline-Zahlungssoftware können Zahlungen ohne Internetverbindung erfasst und dann gesammelt im standardisierten DTA-Format an das Finanzinstitut übermittelt werden. Des Weiteren bieten diese Programme oft auch Schnittstellen zu verschiedenen Buchhaltungsprogrammen und Finanzinstituten, was die Arbeit in dieser Hinsicht erheblich erleichtert und weniger fehleranfällig macht.

Die Umsetzung

Die Infrastruktur, welche für das Online-Banking benutzt wird, muss angemessen geschützt sein. Der Benutzerkreis für das Online-Banking muss so weit wie möglich eingeschränkt und die Verantwortlichkeiten klar geregelt sowie dokumentiert werden. Zudem müssen die Benutzer von Online-Banking für den sicheren Umgang geschult werden. Ein besonderes Augenmerk sollte dabei auf den Anmeldeprozess und die Handhabung des damit verbundenen Authentisierungsmittels gelegt werden.

Nach Möglichkeit sollte für jeden Benutzer ein eigener Online-Banking-Zugang eingerichtet werden – Gruppen-Accounts oder gemeinsam genutzte Zugänge sind zu vermeiden. Die Einführung und Verwendung einer Offline-Zahlungssoftware ist zu prüfen.

Die Kontrolle

Folgende Fragestellungen sind zu berücksichtigen:

- Wird für das Online-Banking angemessen geschützte Infrastruktur verwendet?
- Ist der Benutzerkreis so weit wie möglich eingeschränkt, die Verantwortlichkeiten klar geregelt und dokumentiert?
- Ist das den Anforderungen entsprechend sicherste Verfahren zur Anmeldung (Authentisierungsmittel) eingesetzt?
- Sind die Online-Banking-Benutzer geschult und werden die Verhaltensregeln für das Ein- und Ausloggen beim Online-Banking konsequent angewendet?
- Werden die benötigten Authentisierungsmittel (Token, Smartcard etc.) sicher angewendet und aufbewahrt?
- Falls vom Finanzinstitut angeboten: Ist die Transaktionsbestätigung aktiviert?
- Wurde die Einführung bzw. die Verwendung einer Offline-Zahlungssoftware geprüft? «

Links

www.sihb.ch
www.ebankingabersicher.ch
www.2-fa.info
www.finma.ch

Porträt

Oliver Hirschi
Dozent

Oliver Hirschi ist seit sechs Jahren an der Hochschule Luzern – Wirtschaft tätig. Er ist Dozent und Projektleiter für Informationssicherheit am Institut für Wirtschaftsinformatik IWI. Er hat die Dienstleistung «eBanking – aber sicher!» mitaufgebaut und leitet diese seit über sechs Jahren. Ausserdem ist er Mitautor der 8. Auflage des «Informationssicherheitshandbuch für die Praxis».

Kontakt

oliver.hirschi@hslu.ch, www.hslu.ch/iwi, www.sihb.ch