

Ein Spiel mit dem Feuer

Den PC oder das Smartphone einschalten, anstatt die Bankfiliale aufzusuchen – das ist für Internetnutzer mittlerweile ganz normal. Online-Banking – sowohl privat als auch geschäftlich – entwickelt sich zur Selbstverständlichkeit. Weniger selbstverständlich scheint es für die User zu sein, notwendige Schutzmaßnahmen zu treffen.

Am Schalter anstehen ist passé. Eine ständig wachsende Zahl von Deutschen erledigt ihre Bankgeschäfte online. Eine aktuelle BITKOM-Umfrage auf Basis von Erhebungen der europäischen Statistikbehörde Eurostat geht von 26 Millionen Online-Bankern hierzulande aus – das sind fast zehn Prozent mehr als noch im vergangenen Jahr. Altersgrenzen gibt es nicht, Online-Banking gehört für 41 Prozent aller Bundesbürger im Alter von 16 bis 74 Jahren zum üblichen Prozedere. Keine Wartezeiten, zeitliche Unabhängigkeit und die 24-Stunden-Verfügbarkeit sind für die meisten Nutzer die wichtigsten Beweggründe.

Bei sensiblen Finanzdaten stehen Datenschutz und -sicherheit ganz oben auf der Anforderungsliste der User, trotzdem sind immer weniger Nutzer bereit, selbst Schutzmaßnahmen zu ergreifen. Sie verlassen sich auf die Bankinstitute und deren IT-Experten und setzen das Thema „Sicherheit“ zunehmend als selbstverständlich voraus. Ein gefährlicher Irrglaube, wie eine Umfrage von Kaspersky Lab belegt. Diese hat das Sicherheitsbewusstsein von Endanwendern bei der Nutzung von Computern und mobilen Geräten wie Smartphones und Handys untersucht. Das Ergebnis: Viele deutsche Computernutzer sind bereits Hackerattacken auf dem eigenen Computer zum Opfer gefallen.

ATTACKE AUS DEM NETZ

Bei der internationalen Studie wurden insgesamt 2.027 Anwender aus Deutschland, Dänemark, Spanien, Portugal, Italien und Israel befragt. 63,6 Prozent davon haben in den vergangenen beiden Jahren mindestens einmal eine Cyberattacke auf den eigenen Com-

puter erlebt – bei den deutschen Befragten waren es sogar 75,1 Prozent. Davon haben 8,3 Prozent durch Attacken bereits Daten wie Musik, Fotos, Filme oder andere Dokumente verloren. Erhebungen bestätigen außerdem, dass Nutzer des weitverbreiteten Bezahl-dienstes PayPal massiven Angriffen ausgesetzt sind. Fast täglich werden Phishing-Mails, die vermeintlich von PayPal stammen, in Umlauf gebracht, um Daten abzugreifen. Der User wird zum Anklicken eines Links und zur Eingabe seiner Zugangsdaten aufgefordert – diese landen dann geradewegs in den Händen des Cyberkriminellen.

Phishing stellt vor allem deshalb eine Gefahr dar, weil die Angriffe billig und gegen eine große Anzahl von Opfern durchführbar sind. Eine E-Mail kostet nichts, und die Programmierung einer gefälschten Bankenwebseite ist ebenfalls für wenig Geld möglich. Doch normalerweise sollte sich kein Anwender ohne aktuelle und umfassende Sicherheitssoftware im Internet tummeln. Gängige Sicherheitssoftware wie beispielsweise Internet Security 2011 von Kaspersky Lab leistet einen Schutz gegen solche Attacken. E-Mails mit gefährlichen Anhängen werden gefiltert, Links zu fragwürdigen Webseiten blockiert oder zumindest nur nach Warnhinweisen freigegeben.

PERFIDE METHODEN

Doch es gibt zahlreiche weitere Angriffsvarianten für Informationen, die sich auf dem Computer des Benutzers befinden. Eine der perfidesten Methoden ist die Installation eines Keyloggers, der die Eingaben der Tastatur aufzeichnet und verdeckt an den Angreifer sendet. Damit erhält der Cyberkriminelle eine lückenlose Historie aller Benutzernamen, Passwörter und anderer wichtiger persönlicher Daten. Die Sicherheitsspezialisten von Kaspersky Lab haben deshalb in ihren Schutzprogrammen eine virtuelle Tastatur integriert, die das Tastatenfeld auf dem Bildschirm einblendet. Darauf können Anmeldedaten für Online-Shops oder -Banken gefahrlos per Mausclick eingegeben werden. Ist ein Keylogger auf dem Rechner installiert, sieht der Angreifer nicht, was hier eingegeben wurde. Die virtuelle Tastatur lässt sich auch in Office-Anwendungen zur Texteingabe einsetzen.

Auch mobile Endgeräte rücken verstärkt in den Nutzerfokus und werden damit für Angreifer als Ziel interessant. So sind Smartphones mittlerweile die meistverkaufte Geräteklasse in Deutschland. Für viele Anwender sind sie zum Allround-Talent avanciert und ersetzen den PC bereits komplett. Damit sind sie aber auch zum beliebten Ziel für Angreifer mutiert. Schutzsoftware ist hier bei Weitem nicht so verbreitet wie bei Notebooks oder stationären PCs.

Die Kaspersky-Sicherheitsumfrage zeigt, dass über 24 Prozent der deutschen Befragten mit einem mobilen Endgerät wie Tablet-PC oder Smartphone im Internet surfen. Lediglich fünf Prozent nutzen dabei eine Antivirensoftware. Der Großteil der befragten Smartphone-Nutzer – nämlich 75,3 Prozent – setzt keine Sicherheitslösungen für seine mobilen Endgeräte ein. Noch besorgniserregender: Über 60 Prozent beabsichtigen, auch in Zukunft keine Antivirenlösung für ihr Smartphone anzuschaffen.

Dennoch gaben die Befragten an, sie hätten insbesondere Angst, auf dem Handy gespeicherte Daten durch Diebstahl oder Verlust des Geräts preiszugeben. Dabei ist das Bedrohungsgefühl durchaus vorhanden: Die deutschen Umfrageteilnehmer wännen sich am wenigsten auf sozialen Netzwerken und am meisten beim Empfangen von E-Mails in Sicherheit. Online-Banking und -Shopping werden als sicherer empfunden als soziale Netzwerke. Passende Schutzsoftware wie Kaspersky Mobile Security 9 hilft auch auf mobilen Endgeräten dabei, die üblichen Einfallstore für Angreifer zu schließen. Gleichzeitig schützt es alle auf dem Smartphone gespeicherten Daten im Falle eines Verlusts oder Diebstahl des Geräts: Per SMS können vertrauliche Daten blockiert oder gelöscht werden. Zudem ist es möglich, Handys mit GPS-Funktion wiederzufinden.

Da sich auch Banken, Politik und Wirtschaft der Gefahren und der oft fehlenden Schutzmaßnahmen durch die Bürger bewusst

sind, soll der elektronische Personalausweis bald für mehr Sicherheit bei solchen Transaktionen sorgen. Er wurde am 1. November 2010 eingeführt und funktioniert mit einem integrierten Chip, der einen elektronischen Identitätsnachweis ermöglicht. Durch den digitalen Personalausweis sind sowohl User als auch Anbieter von Online-Services in der Lage, sich



GEFAHR VERKANNT: Beim Online-Banking via PC oder mobilem Endgerät verhalten sich User oftmals beängstigt-leichtsinnig.

auszuweisen; zusätzlich haben Verbraucher die Möglichkeit, eine sogenannte digitale Signatur auf dem Chip zu speichern. Laut einer BITKOM-Umfrage beabsichtigen fast 40 Prozent der Internetnutzer, den Ausweis beim Online-Banking einzusetzen.

Die Notwendigkeit der Sicherheit beim Online-Banking steht außer Frage. Datendiebe phishen in fremden Gewässern, solange sie keine Grenzen aufgezeigt bekommen. Trotzdem unterschätzen Anwender die Gefahren nach wie vor und nutzen zu selten effektive Schutzsoftware. Und auch der Gesetzgeber trifft Maßnahmen zum Schutz der Anwender. Es liegt also an den Benutzern, die Möglichkeiten zu ergreifen und ihre Bankgeschäfte online sicher abwickeln zu können. (dam) ■