schwertun, könnte der pragmatische Mittelweg eine sinnvolle Lösung sein: ein Teilkapitalbezug von beispielsweise 25 Prozent oder 50 Prozent. Damit lassen sich die Vorteile einer garantierten lebenslänglichen Rente mit dem Reiz eines frei verfügbaren Kapitals kombinieren.

Wer sich für einen Kapitalbezug entschieden hat, steht nun vor der Herausforderung, das Kapital ertragreich, flexibel und steuergünstig anzulegen. Hilfreich ist dazu ein Etappenplan (siehe Box unten).

In den seltensten Fällen macht es Sinn, das wegfallende Renteneinkommen der Pensionskasse durch eine Leibrente zu ersetzen. Der angepriesene Vorteil der Prämienrückgewähr wird teuer bezahlt: Die lebenslänglich garantierte Rente ist für dasselbe Vorsorgekapital wesentlich tiefer als bei der Pensionskasse.

Umgekehrt sind hohe Sicherheit, garantierte Mindestverzinsung und Steuerprivileg die Trümpfe einer mit Einmalprämie finanzierten Leibrente. Der Hauptvorteil liegt darin, dass der Ertrag unter bestimmten Bedingungen nicht als Einkommen versteuert werden muss. Diese sind: Vertragsabschluss vor dem 66. Altersjahr, Vertragsdauer mindestens fünf Jahre, Auszahlung nach dem 60. Altersjahr. Der Versicherungsnehmer muss mit der versicherten Person identisch sein. ■

Argumente

Argumente für den Kapitalbezug: Finanzielle Flexibilität, Chance auf höhere Renditen durch Anlagemöglichkeit, Möglichkeit, Erbvorbezüge auszurichten, Restkapital bleibt den Erben erhalten, (Teil-) Amortisation der Hypothek ist möglich. Gut zu wissen: Gestaffelter Bezug bringt Steuervorteile. Für den Satz der Kapitalsteuer ist die Höhe der Auszahlung und der Wohnort zum Zeitpunkt der Auszahlung massgebend. Anmeldefrist für die Kapitaloption nicht verpassen (siehe Reglement der Pensionskasse). Dort ist auch die maximale Höhe des Kapitalbezugs geregelt. Der Ehepartner muss den Vertrag mit unterzeichnen. **Argumente für die Rente:** Regelmässiges Einkommen bis ans Lebensende, Langzeitprofit, Hinterlassenenrenten (Witwen-, Witwer- und Waisenrenten für die Hinterbliebenen).

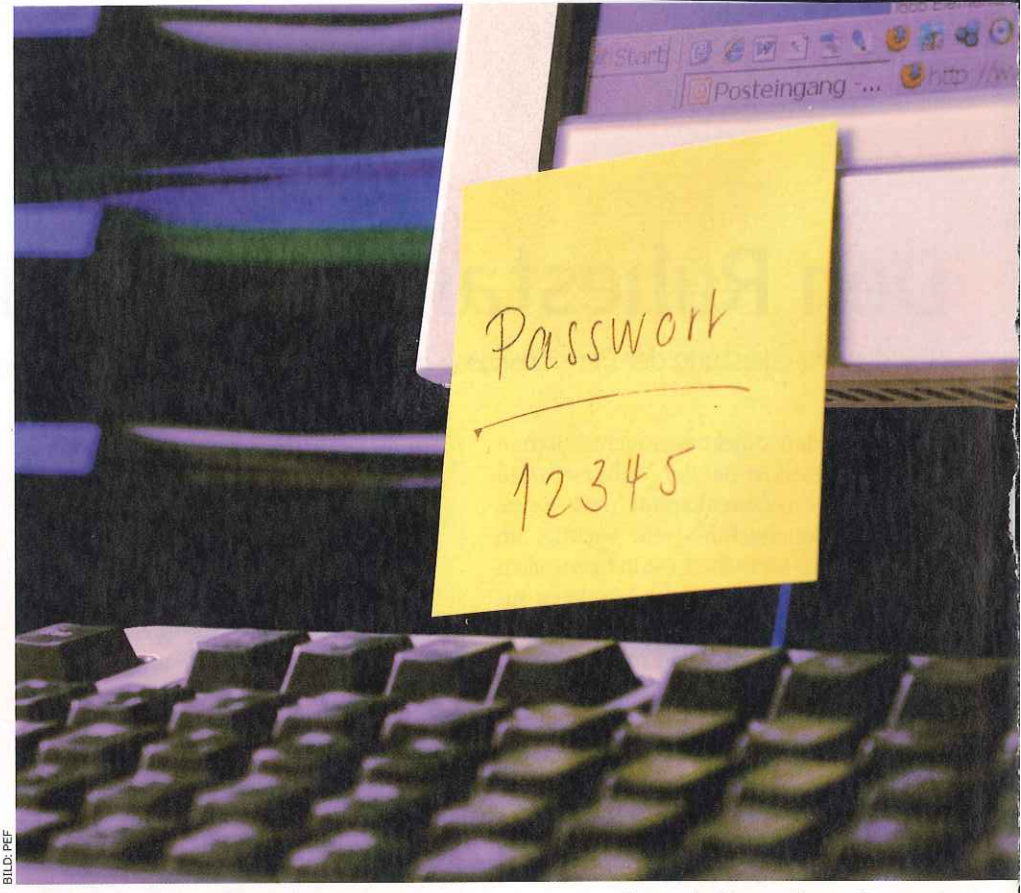

BILD: PEF

Gefahrenstufe Passwörter und sonstige E-Banking-Unterlagen sollten nicht beim PC herumliegen.

Online-Geldgeschäfte? Aber sicher!

Mit einem optimierten Anmeldeverfahren wollen E-Banking-Anbieter dieses Jahr die **Bedrohung durch Hacker** vermindern. VON MICHEL BENEDETTI

Rechnungen zu zahlen macht niemandem Freude. Aber es muss gemacht werden. Viele Bankkunden erledigen diese Pflicht mit wenigen Klicks an ihrem Heim-PC. Allein die drei Grossbanken Credit Suisse, UBS und Zürcher Kantonalbank sowie die Raiffeisengruppe hatten Ende 2008 über zwei Millionen E-Banking-Anwender unter Vertrag. Die PostFinance ist mit aktuell 985 000 Kunden die Nummer 1 im schweizerischen E-Banking und hat im vergangenen Jahr 125 000 Neuanmeldungen für ihre Anwendung E-Finance registriert.

Wer seinen Kontostand am PC abruft oder die Miete begleicht, ist ähnlich wie bei virtuellen Kreditkartenzahlungen einem erheblichen Gefahrenrisiko ausgesetzt. «Sicherheitsrisiken existieren sowohl im klassischen Zahlungsverkehr als auch im Online-Banking», sagt Urs Ackermann, Pressesprecher der Zürcher Kantonalbank. «Im Online-Banking zielen die betrügerischen Angriffe hauptsächlich auf den Computer der Anwender ab.»

Eine dieser Attacken besteht im sogenannten Phishing. Dabei verschicken Kriminelle E-Mails, die angeblich von der Hausbank stammen. Wer auf den Link klickt und seine Benutzerkennung offenlegt, öffnet dem Hacker den Zugang zum eigenen Bankkonto. Bei der «Man-in-the-Middle-Attacke» handelt es sich um eine andere böswillige Kreativität der Hackergemeinde. Der «böse Mann in der Mitte» kontrolliert per Schadprogramm den Datenverkehr zwischen seinem Opfer und dessen Bank. Und schliesslich treibt das seit Jahren berüchtigte «Trojanische Pferd» auch in der E-Banking-Welt sein Unwesen. Dabei schleicht sich eine Software ein, die sich getarnt auf dem PC installiert und den Anwender ausschnüffelt oder seine Internetverbindung manipuliert.

Informationen über erfolgreiche Hackerangriffe gibt es kaum, denn die meisten

Banken halten sich bedeckt. Flannery Fiona, Mediensprecherin der Credit Suisse, spricht von «ganz vereinzelten Kunden, die von Angriffen betroffen waren». ZKB-Mediensprecher Urs Ackermann hingegen sagt, «dass bei der ZKB-Onlinebank bisher noch kein Kunde zu Schaden gekommen ist». Die Melde- und Analysestelle zur Informationssicherung des Bundes (Melani) sieht ebenfalls kein Schreckensszenario: «Es ist von einer verhältnismässig geringen Schadenssumme auszugehen», meint Marc Henauer, Sektionschef von Melani. Dem Schweizer Bankenombudsman Hanspeter Häni schliesslich sind keine Fälle bekannt, «in denen es gelungen wäre, ohne Kenntnis der Identifikationsmerkmale ins System einzudringen».

> Bisher zeigte sich die UBS bei Schäden recht kulant.

Wie sich die Banken bei Schäden oder Missbrauch schadlos halten, erfährt jeder neue E-Banking-Kunde im Kleingedruckten des Anwendervertrags. So muss beispielsweise ein Kunde der Raiffeisen-Gruppe «die Risiken tragen, welche sich aus Manipulationen an seinem Computer durch Unbefugte ergeben». Die Zürcher Kantonalbank schreibt, sie wolle keine Haftung übernehmen «für das Endgerät des Benutzers»; das könnte sich bei virenverseuchten PC als fatal erweisen.

Allerdings: Die meisten E-Banking-Anbieter beharren nicht auf den Paragraphen und geben sich bei effektiv entstandenem Schaden dem Kunden gegenüber grosszügig. «Bisher hat sich die UBS kulant gezeigt, wenn einem Kunden aufgrund einer Hacker-Attacke auf dessen PC tatsächlich ein Schaden entstanden ist», bestätigt UBS-Mediensprecher Dominique Gerster. Ähnlich klingt es bei PostFinance.

Zu mehr Sicherheit trägt seit diesem Jahr ein optimiertes Log-in-Verfahren der E-Banking-Anbieter bei, das den Hackern ein Schnippchen schlagen soll. Im klassischen Anmeldeverfahren hat der Anwender bisher seine Vertragsnummer und ein eigens definiertes Passwort in den PC getippt. Für das dritte Element, eine Zufallszahl, haben die Zürcher Kantonalbank und die Raiffeisen-Gruppe ihren Kunden noch im vergangenen Jahr sogenannte Streichlisten zugeschickt. Sie galten bisher als grösste Sicherheitslücke, denn neben den virtuellen Dieben sind solche Unterlagen auch für reale Eindringlinge interessant. So gibt es laut dem Fachmagazin PC-Tipp «Einbrecher, die bei ihren Raubzügen in Wohnungen gezielt nach E-Banking-Material Ausschau halten».

Doch ab diesem Jahr dürfte die Streichliste für die meisten E-Anwender Geschichte sein. Bereits seit 2008 erhalten Kunden der ZKB beim neuen «mTAN-Verfahren» ihre Zufallszahl über das Handy. «Das neue Sicherheitsverfahren mTAN bietet zusätzlichen Schutz, weil zwei verschiedene Übermittlungskanäle, nämlich Internet und Handynetz, zum Einsatz kommen», erklärt Urs Ackermann. Bei anderen Anbietern, wie UBS oder PostFinance, ist das Verfahren ähnlich, doch hier erhalten die Kunden für das Log-in eine persönliche Chipkarte und ein Kartenlesegerät. Bei PostFinance geht es so: Auf der Website tippt der Anwender seine Vertragsnummer und sein Passwort ein. Danach schiebt er seine Chipkarte in das Kartenlesegerät und erhält über dieses nach ein paar weiteren Eingaben seine Zufallszahl ausgeliefert.

Können E-Anwender nun ruhiger schlafen oder besteht noch ein Restrisiko? «ZKB mTAN bietet hervorragenden Schutz vor den heute bekannten Angriffsmustern», beteuert ZKB-Sprecher Urs Ackermann natürlich. Dennoch rechne die ZKB auch in Zukunft damit, dass sie die Sicherheitsmassnahmen optimieren müsse, um den Angreifern «auch in Zukunft zwei Schritte voraus zu sein». ■

Sicherheitstipps

Fünf Gebote für E-Banking-Anwender

Aktuelle Software Regelmässige Updates des Betriebssystems sowie der installierten Software sind unverzichtbar. Auf keinen Fall sollten Sie E-Banking auf einem fremden PC durchführen, wenn Sie nicht absolut sicher sind, dass diese gut gewartet werden.

Virenfrei Halten Sie Ihren PC frei von Schädlingen aller Art. Nutzen Sie Antiviren-Software und mindestens die in Windows eingebaute Firewall. Damit alle Viren erkannt werden, sollte der Virenscanner permanent aktualisiert werden.

Liste und Karten Lassen Sie Ihre Passwörter und sonstigen E-Banking-Unterlagen nicht beim PC herumliegen. Verstauen Sie diese jeweils getrennt vom Computer.

Sicheres Abmelden: Beginnen Sie Ihre E-Banking-Sitzung sofort nach dem Aufstarten des PC. Öffnen Sie daneben keine anderen Anwendungen oder Webseiten. Sobald Sie mit dem E-Banking fertig sind, loggen Sie sich aus der Anwendung aus. Leeren Sie danach den Browsercache.

Seite und Zertifikat prüfen: Prüfen Sie jeweils, ob Sie auf einer echten E-Banking-Seite gelandet sind. In der Version 3 des Browsers erscheint bei einer seriösen Website der linke Teil der Adresszeile in Grün. Klicken Sie darauf, zeigt der Webbrowser die Sicherheitsinformationen an. Dort befinden sich auch Informationen über das verwendete Zertifikat. Bei anderen Webbrowsern prüfen Sie das Zertifikat, indem Sie auf das kleine gelbe Vorhängeschloss am unteren Bildrand klicken.

Weitere Tipps: Erhalten Sie bei der jeweiligen Hotline Ihres Anbieters.

Quelle: www.pctipp.ch

E-Banking-Anbieter im Vergleich

	Zürcher Kantonalbank	Credit Suisse	UBS	Raiffeisen	PostFinance
Log-in (3. Stufe)	mTAN	mTAN	Chipkarte und Kartenlesegerät	mTAN	Chipkarte und Kartenlesegerät
Anwenderfreundlichkeit	☺☺☺	☺☺☺	☺☺☺	☺☺☺	☺☺☺
Sicherheitstipps bei Demoversion	☺	☺☺	☺	☺☺☺	☺
Verfügbarkeit Hotline	☺☺	☺☺☺	☺☺☺	☺	☺☺

Bewertung: ☺☺☺ = gut ☺☺ = mittel ☺ = schwach

Quelle: Stocks